COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW

SCHMITT & O'DONNELL

U.S. NAVAL WAR COLLEGE

INTERNATIONAL LAW STUDIES

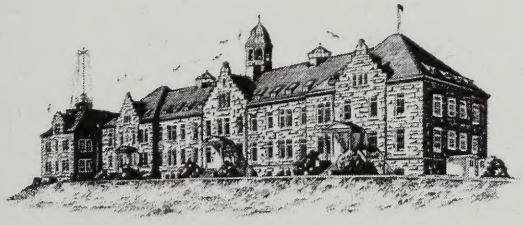
VOLUME 76

INTERNATIONAL LAW STUDIES

Volume 76

Computer Network Attack and International Law

Michael N. Schmitt & Brian T. O'Donnell
Editors



Naval War College
Newport, Rhode Island
2002

INTERNATIONAL LAW STUDIES

Volume 76

Library of Congress Cataloging-in-Publication Data

Symposium on Computer Network Attack and International Law (1999 : Naval War College)
Computer network attack and international law / Michael N. Schmitt & Brian T. O'Donnell, editors.
p. cm. -- (International law studies ; v. 76)
ISBN 1-884733-22-0
1. Information warfare (International law) 2. War (International law) 3. Computer networks --Security measures. I. Schmitt, Michael N. II. O'Donnell, Brian T., 1964– III. Title. IV. Series.

JX1295. U4 vol. 76
[KZ6718]
341.7′577--dc21

2002002063

Contents

Foreword

The International Law Studies "Blue Book" series was initiated by the Naval War College in 1901 to publish essays, treatises, and articles that contribute to the broader understanding of international law. This, the seventy-sixth volume of the series, consists of papers written for the Naval War College's Symposium on Computer Network Attack and International Law.

Participants in the Symposium represented a broad range of expertise in the rapidly developing field of information operations. Included were government officials, operational commanders, international law scholars, technical experts, and military and civilian lawyers. They were brought together to examine the expanding capabilities created for military planners by the technological revolution that today permits means and methods of attack beyond the contemplation of warfighters of the past. This Symposium focused on one of those—computer network attack. Although its full potential is still unrealized, it will certainly become an integral part of the way warfare is waged. Because of its unique nature, computer network attack presents difficult challenges to the law. Yet, if it is to be useful to the operational commander, these challenges must be addressed and the issues surrounding when and how it may be used resolved. Although much work remains to be done, this Symposium has that process well underway.

While the opinions expressed in this volume are those of the individual writers and not necessarily those of the United States Navy or the Naval War College, their insightful analyses make a valuable contribution to the study and development of the law applicable to computer network attack. On behalf of the Secretary of the Navy, the Chief of Naval Operations, and the Commandant of the Marine Corps, I extend to all the contributing authors our thanks and gratitude, with a special note of appreciation to Professor Michael N. Schmitt and Lieutenant Commander Brian T. O'Donnell, who not only contributed individual papers, but provided invaluable service as the editors of this important publication.

RODNEY P. REMPT
Rear Admiral, U.S. Navy
President, Naval War College

Introduction

The 1990's produced a worldwide, technological explosion in computers, information processing, communication systems, and the use of the Internet. The global reach of these vast and complex networks pervades almost every aspect of modern civilization. The Naval War College conducted a Symposium on Computer Network Attack and International Law in June 1999, to address such advanced technology's impact in the area of warfare directed through and against computer networks. The Symposium is documented in this volume of the International Law Studies (the "Blue Book") series.

The Symposium was made possible with the support of the Honorable Arthur L. Money, Assistant Secretary of Defense (Command, Control, Communication, and Intelligence) and the Pell Center for International Relations and Public Policy of Salve Regina University, Newport, Rhode Island. Their assistance is greatly appreciated.

Professor Michael N. Schmitt, George C. Marshall European Center for Security Studies and Lieutenant Commander Brian T. O'Donnell, JAGC, US Navy, Navy Warfare Development Command, collaborated as editors for this volume. Mike was a member of the Oceans Law and Policy Department, (now the International Law Department) before retiring from the US Air Force. Brian was also a member of our Department prior to his transfer to the Navy Warfare Development Command. Their dedication and perseverance are responsible for seeing this project to completion.

A special thank you is necessary to Dr. Robert S. Wood, the former Dean of the Center for Naval Warfare Studies, and Dr. Alberto Coll, the current Dean, for their leadership and support in the planning and conduct of the Symposium, and the funding for the printing of this book.

The "Blue Book" series is published by the Naval War College and distributed throughout the world to academic institutions, libraries, and both US and foreign military commands. This volume is a fitting and necessary addition to the series as it begins its second century of publication.

DENNIS MANDSAGER
Professor of Law
Chairman, International
Law Department

Preface

This volume of the International Law Studies series ("Blue Books") completes work begun in June of 1999 during the United States Naval War College's Symposium on Computer Network Attack and International Law. Gathering international legal scholars, judge advocates, warfighters, and computer experts under the auspices of the Oceans Law and Policy (now International Law) Department, the symposium comprehensively considered an emerging *means*, the computer, and *method*, computer network attack, of warfare.

At the time, numerous countries, most notably the United States, were beginning to develop computer network attack (CNA) capabilities. Simultaneously, there was a growing global sense of vulnerability to computer network attack, not only from State actors, but also terrorists, criminals, and cybervandals. Unfortunately, thinking on the technical possibilities of CNA was far outpacing that on the legal limitations to which such methods and means were (or should be) subject. Narrowing this gap was the symposium's purpose, and that of this volume. By bringing operators, technicians, and lawyers together, a fertile environment was created in which those responsible for designing and conducting CNA could acquire a more sophisticated understanding of the normative limits on their activities, while those tasked with considering prescriptive constraints became better equipped to grasp the context in which the law is to be applied. Simply put, the intent of both the symposium and this book was to relate the possible to the permissible.

In 1999 the nature of international law's applicability to computer network attack was quite uncertain. Despite the increasing attention paid to the issue since then, much uncertainty remains. This volume addresses the most pressing issues. It begins with contributions describing the operational milieu in which the law applies, including its technical possibilities and strategic significance. The focus then shifts to the law. Most significant is the legal analysis of the *jus ad bellum*, that aspect of international law governing when a State may resort to force as an instrument of national policy. Does a computer network attack violate the prohibition on the use of force found in Article 2(4) of the United Nations Charter, and, if so, when? Can it fall within one of the two exceptions to that proscription—use pursuant to Security Council authorization in accordance with Chapter VII of the Charter and use in self-defense, based either on Charter

Article 51 or the customary right thereto? If a State conducts a CNA against another State, can the target respond with classic kinetic force? If so, under what circumstances?

Equally challenging are the *jus in bello* issues, i.e., those that surround the conduct of hostilities. When does the law of armed conflict (LOAC) apply to CNA operations? Is it implicated in all cases of computer network attack or do some fall outside its purview? Does it present difficulties for the application of core LOAC principles like discrimination and proportionality or pose particular risks to protected persons and objects? Do lacunae exist in a normative architecture intended to shield non-participants from the effects of conflict? Might CNA, by contrast, offer possibilities for enhancing their protection?

Complex questions regarding computer network attack extend beyond the confines of the *jus ad bellum* and *jus in bello*. This "Blue Book" explores the key ones. Specific attention is devoted, for instance, to the topics of neutrality, space operations, intelligence gathering, and terrorism. Additionally, both the suitability of existing treaty law and application of rules of engagement are considered.

Given the uncertainty surrounding the precise legal limitations on computer network attack, considerable interpretive play exists. Paradoxically, those States most capable of integrating computer network attack, or more broadly information warfare, into their operational capabilities, are those with the greatest vulnerability to CNA. Thus, they find themselves on the horns of a dilemma—resist constraints on the technology and thereby heighten opportunity *and* threat, or normatively impede it and forfeit asymmetrical advantage out of concern over asymmetrical risk. Conversely, those States most defenseless against computer network attack might well find developing a CNA capability attractive because doing so is relatively inexpensive compared to acquiring the conventional military capabilities necessary to challenge those who are currently dominant militarily. How States resolve these policy Catch-22s will determine much of the face of future conflict and its legal infrastructure.

Many thanks are due in any major publishing project, a fact especially true in this one. First and foremost are those earned by the contributors to the volume. Aside from the insightful analysis for which readers are in their debt, they were paragons of patience and cooperation during the unfortunate delays that accompanied completion of the project. Secondly, Captain Ralph Thomas (USN, retired) selflessly gave of his own time to editing this work. His name would have appeared on the title page, but for his excessive modesty. Professor Emeritus Jack Grunawalt also contributed substantial time editing and reviewing the chapters for their content. Lieutenant Colonel James Meyen, USMC, assisted in editing and brought his past experience in bringing this volume to print. Particular

gratitude is due to Professor Dennis Mandsager and the entire staff of the College's International Law Department, Ms. Pat Goodrich of the Naval War College Press, who served as the Press' project editor, as well as Mr. Samuel O. Johnson, Mr. Jeremiah Lenihan, Ms. Susan Meyer, and Ms. Joan Vredenburgh for desktop publishing and proofreading support.

Hopefully, this collection of articles will assist in elucidating the intricacies of applying international law to computer network attack. Perhaps as important is the desire to have it assist in the process of determining appropriate normative vectors as the relevant law evolves to meet these new capabilities. CNA offers both promise and peril. Understanding it, and the legal environment in which it operates, is essential if computer network attack is to contribute to international stability and humanitarian protection. Regardless of the allure of CNA for those starstruck by its possibilities, ultimately the objective of operators and attorney must be to further such ends.

Michael N. Schmitt
Professor of Law
George C. Marshall European
Center for Security Studies
Garmisch-Partenkirchen, Germany

Brian T. O'Donnell
LCDR, JAGC, USN
Legal Advisor
Navy Warfare Development Command
Newport, Rhode Island

I

CNE and CNA in the Network-Centric Battlespace: Challenges for Operators and Lawyers

Arthur K. Cebrowski

IT 21 and Network-Centric Warfare

As President of the Naval War College, I am charged with examining advances in technology and asking the question: "what are the implications for the Navy and its activities in the next century?" Admiral Jay Johnson, former Chief of Naval Operations, has described the future as being shaped by three growing—and irreversible—trends: networking, greater globalization and economic interdependence, and technology assimilation. Critical to our understanding is a recognition that these trends operate synergistically. Using the Internet, intranets, and extranets, networking has rapidly become a powerful force for global organization, one that fosters an interdependency unprecedented in human history. The phenomenon is the result of extraordinary leaps in technological possibilities. Within the next twenty years, for instance, constellations of satellites will blanket the earth providing television, telephone, Internet access, and business opportunities to all but the furthest reaches of the world.

Complicating the difficulties of coherent planning and systems development in this environment of continual flux is the fact that technology is being assimilated at

an ever-increasing rate. It took nearly three generations for electric power to become an everyday part of people's lives. It took radio and television about a generation and a half. The Internet will achieve that status within a single generation.

Obviously, these trends have enormous implications for the armed forces. We are now in the midst of a revolution in military affairs unlike any seen since the Napoleonic Age. In that period, the practice of maintaining small professional armies to fight wars was replaced by the mobilization of citizen armies composed of much of a nation's adult population. Henceforth, societies as a whole would, perhaps tragically, become intricately vested in warfare. The character of armed conflict had changed fundamentally.

Today we are witnessing an analogous change in the character of war and warfare—an information revolution that enables a shift from what we call platform-centric warfare to Network-Centric Warfare. Understanding of these new operations remains nascent; no great body of collated wisdom has emerged to explain how this revolution will alter national and international security dynamics. That is one of the challenges with which I charge readers, to identify and explore the operational and legal issues associated with the new way in which wars of the next millennium will be waged.

Perhaps most notably, Network-Centric Warfare enables a shift from attrition based warfare to a much faster and effects-based war fighting style, one characterized not only by operating inside an opponent's decision loop by speed of command, but by an ability to change the warfare context or ecosystem. At least in theory, the result may well be decisional paralysis.

How might this be achieved? The approach is premised on achieving three objectives:

(1) The force achieves information superiority in terms of accuracy, relevance, and timeliness, thereby having a dramatically better awareness or understanding of the battlespace.

(2) Forces acting with speed, precision, and the ability to reach out long distances with their weapons achieve the massing of effects versus the massing of the forces themselves.

(3) The results that follow are the rapid reduction of the enemy's options and the shock of rapid and closely coupled effects on his forces. This disrupts the enemy's strategy and, it is hoped, forecloses the options available to him.

Underlying this ability is an alteration in the dynamics of command and control. Traditionally, military commanders engaged in top-down direction to achieve the required level of forces and weapons at the point of contact with the

enemy. However, top-down coordination inevitably results in delays and errors in force disposition. It is an unwieldy process that denies flexibility to subordinate commands. Combat power is needlessly reduced and opportunities present themselves to one's enemy. In contrast, bottom-up execution permits combat to move to a high-speed continuum in which the enemy is denied operational pause to regroup and redeploy.

The key to this possibility is the ability to provide information access to those force levels that most need it. In a sense, the middle-man is cut out. Allow me to offer one illustration.

Three years ago, the Navy launched an effort called Information Technology for the 21st Century, or "IT-21." It reflected the Navy's understanding that 21st Century combat power must come from warriors and platforms operating in a networked environment. What is required is linkage between systems that accurately provide the necessary levels of understanding of the battlespace (the sensors) and systems that link the ships and aircraft (the shooters). Therefore, overlying these two systems, or grids as they are referred to, must be high-performance information links—a complex and responsive information grid that empowers real-time C4ISR processes (command, control, communications, computers, intelligence, surveillance, and reconnaissance). Although the full integration of the three grids—sensor, engagement, and information—remains incomplete, and new technologies must be developed to optimize Network-Centric Warfare, this vision is clearly the future of United States war fighting.

Challenges

One indispensable need in building our Network-Centric Warfare capability is adequately defending the information grids that support our capabilities. We know all too well that our enemies recognize the vulnerabilities posed by our network dependent systems. Because information and the network will be valued, it will become a target. Therefore, a core strategic goal must be to design, build, and operate secure IT systems resistant to computer network exploitation (CNE) and computer network attack (CNA). Disruption or corruption of these systems could have devastating strategic effects. Think, for example, where we would be today if the Yugoslav intelligence agencies had through CNA caused Allied Forces to "inadvertently" bomb the Russian Embassy in Belgrade . . . or a hospital . . . or a school. Information assurance is the *sine qua non* of effective, reliable Network-Centric Warfare. Assurance need not be absolute . . . nothing is in war. But some aspects require higher levels of assurance.

A troubling reality we must deal with is that most military systems obtain and process information from civilian systems over which the Department of Defense has a lesser—or no—degree of control. These civilian systems are likely to be much more vulnerable to CNE and CNA than military systems because of public access, and may have fewer resources dedicated to their security. Along the same lines, our military infrastructure is dependent upon the domestic civilian infrastructure. Military supply, logistics, and routine communications systems rely extensively on the public telecommunications grid, the domestic electric grid, and domestic transportation systems. Each is itself dependent on potentially vulnerable computer networks.

The threats cannot be overestimated because the value cannot be overestimated. Some are new; others are merely new forms of existing threats. CNA is certain to be used in conjunction with traditional warfare by those who are otherwise unable to match the United States' military wherewithal. In particular, it is guaranteed to appeal to terrorists and rogue States. Further, we may expect to see computer network exploitation as a new form of an age-old threat—espionage.

In facing such threats, the United States and its allies should strive for, but should never presume, technological dominance. When people say CNE and CNA technologies are warfare on the cheap, I think of the National Security Agency budget. But formidable capabilities can be developed and obtained relatively inexpensively. The critical capital in this industry is brainpower and computing power. With only a fraction of the world's population, and given the widespread nature of computing power, it may become difficult for us to maintain our present advantage. Though defensive mechanisms will constantly improve, so too will the offensive abilities of potential adversaries. The environment will be hostile and dynamic. It may be impossible to determine who has the advantage at any time. In the conventional world of land forces, ships, planes, and submarines, US intelligence agencies have a fair ability to determine the enemy's order of battle; that luxury disappears in the world of cyberspace.

The face of war is truly changing. In particular, we in the United States face a different reality in the effort to shape international law than faced in the past. In the post-Cold War era, attacks on the territory of the United States by conventional forces have not been a great concern. On the North American continent, separated from potential adversaries by the Atlantic and Pacific oceans, we were relatively protected. With CNE and CNA, those large expanses of ocean only serve to provide a false sense of security. Today, the homeland threat is from any country, terrorist organization, or hacker behind a computer anywhere in the world.

During future crises, the United States must expect significant CNE and CNA activity against both our military *and civilian* infrastructures. Though our forward-deployed battle systems should be impenetrable, the support systems reaching back to and in the United States will be far less secure. This new reality, of the United States homeland as a viable target, will inevitably influence our approach to international law. The Department of Defense's interest in the shaping of international law in the recent past has arguably been driven by the desire to further our offensive interest—our interests as a shooter rather than as a target. Today, with the homeland at risk, a new balance between our offensive and defensive interests must be achieved.

Many questions are presented by this new paradigm. Particular attention must be paid to the following:

- Does international law require us to wait until lives are lost or property destroyed before we may engage in acts of self-defense?
- What is the new context of rules of engagement? Proportional response? Precision? Perfidious act?
- How is targeting affected by the fact that military systems are networked to civilian IT systems controlling communications, energy, finance, and transportation?
- Are legal consequences of international law triggered upon the perpetrator gaining *access* to our IT systems, or do they depend upon the *effects* or tangible consequences of access?
- Are there differing perspectives on the desired direction in which the law should develop among US Government agencies and among different nations?

Framework of the Law

The Hague and Geneva Conventions, and other sources of international law, both *ad bellum* and *in bello*, provide guidance for future conflicts. Consider the critical principles that regulate the conduct of nations during armed conflict:

(1) Only military objectives may be attacked.

(2) It is prohibited to launch attacks against civilians.

(3) The loss of civilian life and damage to civilian objects must not be excessive in relation to the military advantage anticipated.

No reasonable person would disagree with these norms; but their application in cyberspace attacks will place stress on commanders, targeteers, and their

lawyers. There will be considerable difficulty in identifying sources and locations of threats in cyberspace. Dual-use technology will render the ability to distinguish between a military and civilian target elusive. And determining second and third order effects from information attacks will be a complex task indeed.

Despite the difficulties in application, I am persuaded that we will be well served by applying the core principles of international law to information age warfare. We cannot, in our zest for tactical mission success, lose sight of our goals as a nation—to protect life and liberty, in our country and throughout the world. Adherence can be difficult, but our commitment to protecting the innocent, the noncombatant, reflects our national values. One commentator stated it with precision: "Adherence to the law reflects who we are as a nation, and separates the good guys from the bad guys." Therefore, the warfighters, IT professionals, and lawyers must all ask what steps need to be taken so the cyberwarriors of tomorrow can remain the good guys.

Finally, I would caution that we should not rush to place undue controls on information operations before we understand the implications of such control. The law of armed conflict developed over centuries as nations determined what restrictions on their war fighting capability they were willing to accept. Time and experience are the brick and mortar of international law. As our understanding of the technology increases, so too will the ability of nations to best determine the desired international norms. We must be cautious not to advocate new law regarding information warfare without understanding its moral, legal, and practical implications.

II

Technology and Law: The Evolution of Digital Warfare

David Tubbs, Perry G. Luzwick, Walter Gary Sharp, Sr.

Introduction

Technology began shaping the conduct of war when the first warrior picked up a stone to increase his killing power during hand-to-hand combat.[1] Ever since, new technologies have increasingly affected the balance of power by:

- leveraging existing strategies or efforts of either the attacker or the defender;
- enabling new and unexpected strategic uses of existing weapons technology;
- providing new weapons of increased destructive force;
- neutralizing or mitigating the effects of enemy weaponry or strategy; and
- providing or denying the element of surprise.

Telecommunications and information-related technological advances, however, have perhaps been the most fundamental in shaping warfare. Telecommunications enables command and control by providing rapid, accurate, and secure communications among friendly forces. Without communications, the Strategic Air Command Commander-in-Chief, General Tommy Powers, once

observed, "all I would command is my desk, and that's not a very lethal weapon." Telecommunications has allowed the battlespace to grow from a grassy field to encompass outer space, the atmosphere, the earth's surface, and under the seas. Table 1 demonstrates how telecommunications has reduced by several orders of magnitude the time needed for command and control.

Circa	Methodology	Time
1775	Message from Boston via horse and courier to a ship, which then sails to London and taken by horse and courier to the King - and return reply	Months
1850	Message from New York to San Francisco via telegraph and the Pony Express	Weeks
1925	Message from Washington, DC to Tokyo via high frequency radio	Days
2000	Message from Washington, DC to Tokyo	Seconds

Telecommunications today give fighting forces incredible capabilities to be proactive and adaptive, and to take meaningful response. Today's warfighters expect and demand reliable, fast, interoperable, and protected communications. Telecommunications also enables the acquisition of information concerning the disposition, objectives, and vulnerabilities of the enemy to gain a strategic advantage, creating warfighting disciplines such as Communications Intelligence (COMINT), Electronic Warfare (EW), Electronics Intelligence (ELINT), Foreign Instrumentation Signals Intelligence (FISINT), Imagery Intelligence (IMINT), Open Source Intelligence (OSINT), and Signals Intelligence (SIGINT). High-speed communications cannot occur, however, without computers, and the pervasive use of computers in almost every device inextricably link telecommunications, computers, and the warfighting capability of any modern military force.

Information Operations (IO) and Information Warfare (IW) compose the modern construct that embodies and demonstrates the dependency of modern warfare on telecommunications and computers. Fundamentally, IO and IW include any activity that influences the production, modification, falsification, distribution, availability, or security of information relative to any aspect of the pursuit of war. These activities may be wide-ranging, even low technology, as long as they influence the gathering, analysis, distribution, or implementation of useful warfighting information. Sabotage, bombing of communications infrastructure, radio frequency jamming, High Energy Radio Frequency (HERF) weapons, and electromagnetic pulse generation are all examples of relevant, modern IW.

Offensive and defensive IW implications of new technologies must constantly be assessed by the professional warfighter. Specifically, computer networking technologies are becoming ever more integrated into modern commerce and communications; consequently, attacks on these computer networks must be integrated into offensive and defensive warfare strategies. Relevant IW computer technologies include the full networking spectrum—from small, hardened, independent Local Area Networks (LANs) and regionally distributed Wide Area Networks (WANs) to the use of the global, publicly-supported Internet.

Enter the Internet

Although the impact of telecommunications on warfare has been dramatic, the invention of the Internet has been profound. Because of its pervasive integration into modern technology infrastructures, the Internet will very likely be used as either the primary or a collateral medium for any computer network attack. The commercial interests of developed nations, and even many unclassified military functions of these same nations, are now dependent on the availability and reliability of Internet communications. Exploitation, elimination, or compromise of this vulnerable asset will often be the primary component of a nation's IO campaign.

The Internet began in 1969 as the ARPANET.[2] Originally the ARPANET was simply an experiment in highly reliable information networking. The experiment connected the Department of Defense with military research companies and specified universities who had military research contracts.[3] High reliability was achieved through the development of a new set of technologies, collectively named "packet switching."

In 1990, the ARPANET shut down, and was replaced by the NSFNET.[4] At the same time, non-DoD related commercial enterprises started to recognize the value of such a pervasive, distributed communication medium and they began connecting their previously private computer networks to the Internet, supplying new paths for all transmissions. These commercial entities brought commercial employees, suppliers, and customers to the Internet for the first time. They also began making a profit selling Internet access to the public. As commercial connections and traffic burgeoned, the NFSNET backbone handled less and less of the total traffic volume. While the NSFNET is not completely gone, the process of replacing the government's Internet infrastructure with commercial equivalents is well under way.

The essential, high reliability concept of packet switching used by the ARPANET, NSFNET, and now the Internet, is the elimination of a central,

single-point-of-failure, control and switching center. Packet switching first divides an electronic communication into pieces, known as packets. A header then prefixes each packet with identifying data such as:

- the sender of the message;
- the intended recipient of the message;
- the subject of the communication (for e-mail);
- the date and time of the transmission; and
- the position of this packet in the series of packets for this message.

Each packet is then independently routed to a computer that forms part of the backbone of the Internet (an Internet node). Each Internet node passes packets on to any computer on the network that is "nearer" to the destination identified in the header information than the present location. Recognize, however, since Internet node routing considers existing network traffic loads, and the definition of "nearer" is an estimate of total travel time rather than physical distance, the node to which a packet is routed may be physically farther away from the destination. Packets often travel quite circuitous routes to their destination. In fact, the various packets of a message may travel very different routes to the destination and will almost certainly arrive at different times. The header information allows the packets to be reassembled in proper order at the destination computer.

Internet Vulnerabilities

For many reasons, however, these commercial and governmental initiatives seldom considered security as a part of the infrastructure. The main reasons for not implementing greater security were capability, cost, and schedule. Security uses system resources and thus slows the system down or, worse from a user's perspective, does not permit certain features. Security is costly in terms of time, money, and people. It adds to the cost of the delivered capability. Security also lengthens delivery schedules because it takes longer to write a computer program without the flaws which make it vulnerable.

Perhaps the overarching reason for not implementing security is that the public, industry, and government did not perceive a threat sufficient to warrant the extra cost to embed security into hardware and software. For example, not realizing that a mountainside switch was on the rail line that the US Army uses to transport its main battle tanks to a seaport during hostilities, a Conrail railroad employee might ask, "Why would anyone want to attack a switch?" Not only is security expensive, it is prohibitively costly if it is considered after the fact. One

IBM study stated that it would cost ten times more to retrofit security into a system than it would if it was considered from the beginning.

Potential vulnerabilities are also frequently overlooked by the government in its use of commercial-off-the-shelf (COTS) products. The rationale for their use is two-fold. First, COTS provides strong capabilities at reasonable cost. Not only do these strong capabilities enable businesses to make a profit, but in addition the government does not bear the long-term costs of the resources to develop the products. Second, COTS upgrades and new products are more timely. However, the typical software product, portions of which are developed overseas in countries that either are or may be US competitors, contains several million lines of code. Determining whether such software contains any malicious code is economically infeasible and practically impossible. To do so would require a line-by-line code check as well as an understanding of how the lines of code interact. There is no artificial intelligence program that does this. It requires skilled people and time; indeed, more people and time than it takes to write the software in the first place.

Complexity is a hallmark of modern software. There are at least 300 security features in Windows NT, for example, that can be turned on and off. Adversaries constantly probe for weaknesses. It takes just one weakness not detected and resolved in one system to make all users connected to it vulnerable to exploitation and attack. Because of the trusted relationship between systems and networks in our highly interconnected infrastructure, achieving and maintaining control over our environment is very difficult.

The distributed routing design of the Internet means that there is no central point of control and thus no single-point-of-failure. This creates a highly reliable telecommunications system because an enemy or accident must disable every Internet node to disrupt traffic. Paradoxically, this high reliability carries with it an associated security vulnerability—every participating Internet node computer is a decision-maker, with full routing information and authority and access to the information stream. Accordingly, access to any Internet node will give a hostile or criminal element access to Internet traffic.

Also, with no centralized control, Internet entities do not naturally make use of information correlated from diverse sources to evaluate the intentions of their traffic—hostile traffic that conducts a distributed computer network attack is not recognized as such and thus allowed unimpeded passage. In direct analogy to covert, spread spectrum communications that spread wireless information over a number of radio frequencies to disguise transmissions, distributed Internet attacks use coordinated connections and communications from disparate locations to disguise the activity or objectives of the attack. These distributed attacks

ultimately make use of flaws in the operating system or applications software, just as with any other computer "hack." Often, however, the distributed exploit is not obvious because individual steps are taken by different remote computers and each step is, in and of itself, relatively innocuous.

Methods of Computer Network Attack

Perhaps the greatest vulnerability of any computer system is the human element. Most people still use family names or other easy-to-remember passwords, or use more difficult passwords but write them down in an easily accessible location near the computer. While some hackers may attack only by the Internet, a sophisticated and persistent threat dedicated to compromising a computer system will attempt to surveil the system physically and electronically. Information gathered from conventional forms of surveillance and analysis is very effective in determining which type of intrusion will be the most successful. Insiders, of course, are the greatest threat to any computer system—they have authorized access.

If physical access is obtained, both information gathering and actual system compromise are significantly easier. Hackers may gain physical access to a company's computers through employment as a janitor or temporary secretary—or they may simply be a client or customer who is left alone near a computer momentarily. Once they gain physical access to a computer, hackers can immediately download or corrupt information, or install sniffer software to collect it. A sniffer is a program that runs in the background of the target machine, collecting information, such as passwords or credit card numbers, during normal operations. It generally requires a return visit to retrieve the collected information, but these programs may be quite small and difficult to detect.

Physical access also allows hackers to plant conventional recording devices that will collect information. For example, an audio recording of an impact printer may allow the printed characters to be recreated. Similarly, devices planted in nearby offices can record an entire document when it is transmitted by electronic bursts to a laser printer. Hackers may also learn relevant information by simply collecting trash from the curbside.

Finally, hackers may use social engineering techniques to learn information that compromise a computer system. Social engineering takes advantage of the fact that most people endeavor to be honest and helpful. Unless an enterprise has taken steps to educate its user base to the vulnerabilities represented by releasing seemingly innocuous information, social engineering gathers attack design information very effectively. Typically, a perpetrator will call on an over-worked employee, either in person or by telephone, invent a plausible need-to-know

excuse, and ask for relevant information. They may also offer a free magazine subscription in return for answering a few survey questions. Or, they may actually send free software (which contains malicious code) to try out on a computer. A trained practitioner in social engineering will usually obtain at least unclassified system details, but often passwords and sensitive information can also be obtained.

Seemingly innocuous information can also be very useful, leading to ease of access through system configuration details, personnel information, or guessed passwords. Public records, such as a company's website, or public business relationships allow a significant amount of information to be collated for use against the target. This information may point to a vulnerable electronic interface or an insecure business partner with full access. These elements of friendly information (EFI) may be insignificant in isolation, but can generate considerable weight when collected and pieced together.

Aside from the vulnerabilities exposed by a lack of discipline and compliance of the user base, computer network attacks ultimately rely upon flaws in software, and these type of attacks are greatly enhanced in an Internet environment because of the robust and flexible access and communications paths that the Internet represents. The incongruous truth is that, in spite of a carefully crafted public image of total control over others' information systems, the hacker is precisely limited to what the inadvertent holes the software design process leaves behind allow him or her to do.

Flaws in software design take many forms. Since large software packages contain many million lines of source code,[5] the law of averages guarantees many flaws in logical construction, reduction to source lines, typographical errors, and ill-defined interfaces between code developed by many different groups, at different times, and in different places. The hacker community lives to find and exploit these inevitable flaws and they are very good at doing so, but they cannot normally create holes *a priori* for their own use.[6]

Buffer overflows, for example, are a common vulnerability in all software. They require specific knowledge of the targeted operating system, but are powerful in that they allow arbitrary code (i.e., malicious programs) to be executed. Buffer overflows occur when data written to a pre-sized memory buffer exceeds the buffer's allocated space. The excess data then overwrites other memory areas. This can occur when a user response is longer than the software designer expected. Intentional buffer overflows attempt to write the perpetrator's code into the computer's instructions. Implementation of this exploit is routine; however, it must be precisely written, aligned, and sized so that it falls on a specific memory location.

The majority of flaws in any software package simply represent sand in the gears, disrupting or halting operation in generally unpredictable ways. A large percentage of these purely disruptive flaws are useful for Denial Of Service (DOS) attacks. The defining characteristic of a DOS attack flaw is the element of control. The DOS must be activated by an external action over which the perpetrator has control. As with any compromise of a computer system, access to exercise this control is crucial. Unfortunately, DOS flaws are legion, due to the pervasive instabilities in common operating system and application software packages.

In a DOS attack, triggering the flaw simply disables the target computer in some way, denying the services of that machine to the owner or intended user. Combined with extortion or other kinetic or IW attacks that the target computer was designed to monitor or prevent, DOS can be a useful component of many IW attacks. In the hacker community, which is largely a socially-based merit system, there are very few "brownie points" awarded for DOS attacks because they are so commonly available and easy to perpetrate.

One method for conducting a DOS attack is to transmit malformed data, which is data in a format that isn't expected by the target. For example, sending a negative value where the programmer assumed a positive value would always be received. Although the result of a malformed data packet is generally undetermined, the common result is to crash the target, thus denying service.

A small percentage of the inherent flaws in a software package are useful for more purposefully directed attacks. These include, in order of increasing severity: destruction of data (vandalism), viewing protected data (read capability), modifying data (read/write capability), and control of the system (administrative rights or root access). Of particular importance are exploits that allow a normal user to increase his assigned rights on the network to more powerful levels. These exploits allow a hacker who gains access to the network at any level to make himself an administrator, with full rights to every aspect of the system and data.

Hackers have the innate advantage, and they work together. The collegial, intellectual nature of the hacker community and of the Internet in general guarantees that many hundreds of hours are spent by malicious individuals to develop and improve existing, published exploits. Websites, chat rooms, private electronic bulletin board systems, and other services which cater to the malicious hacker number in the thousands. Hundreds of pre-designed exploits are categorically listed by operating system and software application on public electronic forums (e.g., see www.rootshell.com[7]). Many more exploits exist or are in development in private venues, though private exploits are published coincident with news of the first major attack using the exploit.

Defending Against Computer Network Attack

Effective computer security demands constant vigilance by all users, system administrators, and commanders—and depends upon an integrated security program that protects against hardware, software, and social engineering attacks. The cornerstone of all computer security programs is situational awareness, training, and education. "Security through obscurity," i.e., not worrying about flaws buried in millions of line of code, is a very poor choice for network defense. Unauthorized access must be prevented through an active, layered defense, erecting sequential electronic defenses, which include intrusion detection systems. This strategy allows the defender to detect intruders in the information-gathering stage that precedes every significant information attack. The Achilles' heel of this approach is that human operators must monitor intrusion detection systems for full effectiveness. This is a thankless task of reviewing scores of perfectly legitimate electronic transactions looking for the one obscure, innocent looking interchange that might indicate an attack. This time-consuming and boring task requires considerable technical skill and patience—a difficult combination.

The Application of International Law in Cyberspace

There has been no evolution of international law to govern or prohibit State activities in cyberspace such as computer network attack. Indeed, maintaining a credible ability to project military force in cyberspace is a lawful and fundamentally important aspect of deterrence and maintenance of international peace and security. Existing international law, however, does govern the conduct of computer network attack and other State activities in cyberspace. While these international law norms do not explicitly address information operations, information warfare, computer network attack, or other State activities in cyberspace, they do prohibit the entire range of State activities that causes certain effects. Accordingly, it is critically important that all State activities in cyberspace, especially those conducted by the military and the intelligence community, be reviewed by assigned government counsel.

Until a legal regime matures that comprehensively addresses State activities in cyberspace, which is highly unlikely anytime in the near future, legal advisers must principally conduct an effects-based analysis of international law to determine the lawfulness of State activities in cyberspace. State activities must comply with the law of conflict management and the international peacetime regime, and, during times of armed conflict, the law of war.

Under the law of conflict management, all State activities in cyberspace must comply with the Charter of the United Nations. Unless otherwise authorized by the Security Council under its Chapter VII authority, Article 2(4) of the Charter prohibits the threat or use of force by any State against the territorial integrity or political independence of another State except in individual or collective self-defense as authorized by international law and recognized by Article 51 of the Charter. Customary international law requires that all use of force authorized under the law of conflict management be necessary and proportional.

Although unlawful under the domestic law of most States, the peacetime regime of international law permits espionage, but the unique nature of computer network attack, which allows remote electronic access, undermines the deterrent value of national law. Of grave concern is that many forms of computer espionage may be considered a hostile act or a demonstration of hostile intent, thereby causing a State to use military force in response. There are many other peacetime norms that govern State activities in cyberspace. The 1982 United Nations Convention on the Law of the Sea, for example, prohibits any act conducted in the territorial sea aimed at collecting information to the prejudice of the defense or security of the coastal State; any act of propaganda aimed at affecting the defense or security of the coastal State; and any act aimed at interfering with any systems of communication or any other facilities or installations of the coastal State. Similarly, peacetime telecommunications treaties such as the 1982 Nairobi Convention prohibit harmful interference with radio navigation services, and the 1976 INMARSAT Convention requires that its telecommunications infrastructure be used only for peaceful purposes.

Law of war principles embodied in the Geneva and Hague conventions as well as customary international law apply to State activities in cyberspace during armed conflict. For example, the universally accepted general principle that the "right of belligerents to adopt means of injuring the enemy is not unlimited" certainly places many restraints on the conduct of cyber warfare. Similarly, the principles of military necessity, unnecessary suffering, proportionality, distinction, and collateral damage also apply.

More detailed analyses of these and many other applicable international norms are provided later in this volume by other authors who are noted experts in international law. There are a number of issues, however, which remain unclear under international law. For example, what State activities in cyberspace constitute a use of force prohibited by the law of conflict management? What are peaceful purposes? Can hostile military activities which are tantamount to a use of force conducted in self-defense as recognized by Article 51 of the Charter of the United Nations be peaceful within the meaning of the INMARSAT

Convention? In modern society, the military is heavily dependent upon the civilian infrastructure, especially the telecommunications infrastructure. To what extent is the civilian telecommunications infrastructure a lawful target because a military relies upon it in some way for command and control or computer network attack? What about the Internet nodes of a State that is not a party to a conflict; is its telecommunications infrastructure a lawful target? Is a cyberattack against the critical infrastructures of an "undefended" city prohibited by the Hague Convention even if no physical destruction ensues? How do we regulate computer espionage to avoid the appearance of a hostile act or a demonstration of hostile intent without outlawing espionage completely? A legal review of these and the many other unresolved issues must be conducted in the context of the fundamental principle of international law and sovereignty which provides "that which is not prohibited is permitted." Legal advisers must also understand and embrace the Internet technology of binary mathematics and electronic circuitry which forms the foundation of digital warfare.

The Future of Technology, Law, and Warfare

While the future of technology, law, and warfare is uncertain, it is very clear that technology will continue to drive profound changes in the nature and conduct of 21st century warfare, and that international law, by its very nature, will always lag behind. The international community does not yet understand, much less agree, on how existing international law applies to State activities in cyberspace. An international consensus on a comprehensive regulation of State activities in cyberspace is very unlikely, and States must continue to regulate these activities by their own domestic laws and rules of engagement. In crafting their domestic norms, States must remember, however, that State practice will shape the evolution of international law that will in turn permit or prohibit future activities in cyberspace by all States.

The unintended consequences of computer network attack are also uncertain. For most, the notions of computer network attack and digital warfare conjures up visions of precision warfare, but these visions are far from reality. Information systems are constructed from flawed building materials. All operating systems, software applications, and hardware architectures contain many flaws that can be exploited by computer network attack—and the variations on how they can be combined represent almost an infinite number of vulnerabilities and unintended responses to unauthorized intrusions. Unauthorized access, such as during a computer network attack, therefore, has a relatively high probability of inducing instability into the target system. Without a complete and

accurate modeling of the target system, the uncertainty in predicting the exact primary, secondary, and subsequent order effects of a computer network attack is large. Obviously estimates of distinction, proportionality, and collateral damage are very tenuous when predicated on uncertain estimates of effects.

An exact determination of the uncertainty of a computer network attack is calculable, given *complete* information about the information systems involved, but such a calculation would become quickly outdated due to the fast pace of software development. Reasonable estimates that account for incomplete information are also possible, but these estimates are even more difficult and short-lived since minor changes to a system configuration can have dramatic effects on the results of a particular attack. Estimating the effects of a computer network attack will continue to be risky and inaccurate until the operating systems and applications, for the attacker as well as the target, achieve a reasonable measure of stability. Scenarios where a computer network attack on a military information system disables a linked civilian system that controls water purification, for instance, are very plausible.

The Information Environment (IE) is the new battlespace of the 21st century. The IE is the interrelated set of information, information infrastructure, and information-based processes. Information is data, information, and knowledge—and the information infrastructure is the hardware, software, and transport media used during information-based processes created when storing, manipulating, and transferring information. Denying, degrading, or destroying a select subset of the IE can have significant repercussions in one or more critical infrastructures and can be more effective than physical destruction. Manipulation of the IE now offers the potential to obtain political and military objectives without the use of kinetic weapons. Indeed, control of the IE may be far more effective than physical attack, and may be able to prevent future hostilities.

States must develop a national strategy to defend their own IEs and affect the international IE to successfully attain political and military objectives. Such a strategy requires breaking with traditional organizing, equipping, training, and warfighting strategy. Political support, along with appropriate planning guidance, strategy, and force structure, must be developed. The philosophical insights and intellectual understanding of such a national IE strategy are in their nascent stages and need further development.

Existing information systems have not begun to scratch the surface of the capabilities for self-aware behavior. In ten years, these systems will make practical use of what we have learned in both neural networks and artificial intelligence to model human thinking more closely. This means both that our information systems will modify their own behavior in response to past experience and that the

larger the network, the more effective this behavior will be. They will be capable of detecting and correcting defects in their own hardware, minor imperfections in their own software codes, damage due to neglect, vandalism, or war, and obvious errors in the judgment of their operators.

For information warfare, the potential of self-aware behavior is overwhelming. We could, for example, teach a distributed information system to gather information from a target network *exactly* as a series of a certain number of legitimate users would use the system, i.e., their intrusion detection software will not be able to distinguish between the two events. Or the attack could model an attack on the enemy network from 600 saboteurs in 200 locations, causing the target network to disconnect vast subnets. This would exacerbate the degradation of the target network's self-aware functions, denying it the information it needs to discriminate further fictional attacks from real events (the speed and accuracy of a neural net is directly related to the size of the net).

On the battlefield, individual warfighters will be connected to vast information resources to enable effective decision-making and coordination of troops. Forward observers will be automated and equipped with sensors that dwarf a human's information collecting hardware. Indeed, humans may not need to inhabit the kinetic battlefield at all.

Defensive capabilities will reap similar advantages, at some point pitting their software and processing skill against ours. With rapid software and hardware development likely to continue, a quickly escalating arms race in technology weapons is possible. Lagging behind in this race might be as deadly as losing an arms race in kinetic weapons, but the time scales will be much, much shorter.

The United States currently enjoys a distinct technological advantage. The most likely scenario is that this will continue and technical developments will generally tend to open the disparity in capability between us and our enemies, to our favor. Commercial development pressures will drive this naturally, although military applications need to be carefully identified as new technologies present new offensive and defensive possibilities. This creative ruminating is not trivial and must not be cursory—the selection process that produces technologists ensures that they are creative. The weapons they design will exploit non-obvious niches in new technologies.

At present, however, the instability of present operating systems and our dependence upon them, paradoxically leaves us more vulnerable to information warfare and computer network attack than less technically developed nations. Malicious code, HERF weapons, EMP, and other less sophisticated attacks could wreak great havoc in our technological society. This "Blue Book," and the conference on which it is based, is a tremendous step toward an international

understanding of the implications of information technology on a State's national security, the information environment, and the underlying international legal issues.

Notes

1. STEPHEN BULL, AN HISTORICAL GUIDE TO ARMS & ARMOR 7 (1991).

2. Advanced Research Project Administration NETwork—later renamed DARPANET: Defense Advanced Research Project Administration NETwork, although ARPA had always been a Department of Defense entity with military objectives.

3. M.L. YOUNG AND J.R. LEVINE, INTERNET FAQs: ANSWERS TO THE MOST FREQUENTLY ASKED QUESTIONS 22–24 (1995).

4. National Science Foundation NETwork. The NSFNET was initiated to handle the increasing volume of traffic as the ARPANET became more and more popular. NSFNET also solved a number of technical headaches inherent in the original design of the ARPANET, and so eventually the ARPANET was phased out completely.

5. The Windows NT™ operating system, for instance, contains roughly fifty million lines of source code.

6. A notable exception is, of course, when the hacker works for a software development firm—a not infrequent case. Even in this case, inserting a "backdoor" providing access to the software after deployment is not trivial. The software development enterprise has layers of testing in place to catch such defects. While these layers of testing are far from foolproof, such a hacker has a slightly lower than even chance of success. Failure typically results in termination of employment, making repeated attempts statistically meaningless.

7. These sites are free and are extensively cross-referenced. The primary belief that motivates the maintainers of these sites is that full disclosure of all exploitable flaws is the only way for intelligent system administrators to ensure robust information systems security.

III

A Different Kettle of Fish: Computer Network Attack

Roger W. Barnett

The Information Age has dawned, and it is maturing rapidly. How remarkable the celerity and scope at which the entire world is becoming one far-flung network! As one pundit observed, "To a first approximation, all computers in the world are connected to each other." Indeed, when one connects to the Internet, he or she is linked globally to all other computers on the Internet. In 1999 there were nearly 200 million Internet users worldwide; by the year 2003, at least another 100 million are expected to be on line.

Some have suggested that, in terms of technological progress, these are revolutionary times. Yet, as long ago as the decade after the orbiting of Sputnik, Soviet authors wrote about a "Revolution in Military Affairs." The instrument that effected this particular revolution was the marriage of the intercontinental range ballistic missile with the nuclear weapon warhead. This combination meant that, for the first time in history, *strategic* attacks (attacks with the potential to alter the course and outcome of a *war*, as opposed to an attack with the potential to alter the course and outcome of, say, a *battle*, which would be at the *tactical* level) could be conducted at any time against any target in the world. This was genuinely revolutionary, and had to be addressed by developing a wholly new set of concepts, doctrines, and international rules. Today, the close-coupling of societies by information technologies is beginning to portend the same effect—potentially a

strategic effect—but without the necessity for nuclear weapons or long range missilery. Just as the Soviets noticed something revolutionary going on, this is also a major occurrence, but it is also a different kettle of fish.

While the Soviet "Revolution in Military Affairs" offered to produce strategic effects, the means to accomplish this end was centralized in the hands of the State. For good or ill, the power was concentrated, and it was a power that could be acquired only with significant technological effort and at great expense. Today, the potential for a *strategic information systems attack* has become a reality.[1]

What makes this so remarkably different is not only the effects that might be produced without the use of nuclear weapons, but also the diffuse availability of this power. The entry costs to conduct a strategic information attack are insignificant—an inexpensive computer, some easily obtainable software, and a simple connection to the Internet. In theory, anyone just about anywhere can gain access and mount an information attack that might bring about devastating results. Moreover, using this ubiquitous capability, strategic effects might be wrought with little physical damage and no loss of life. Conceivably all national infrastructural components could be vulnerable: telecommunications; food, water, oil, gas, and electrical distribution; health care; education; finance; industry; and also military facilities, networks, command and control, and personnel.

Even more disconcerting, such strategic attacks can be conducted anonymously. Heretofore, the concentrated power of long-range nuclear weapons was in the hands, and under the responsibility and accountability of, governmental officials. Military means, especially those with strategic consequences, were tightly and centrally controlled. Time, technology, and the change in the way in which societies create wealth have changed all that. Thomas Czerwinski has cautioned that "As the 'combat form' in any society follows the 'wealth creation form' of that society, the wars of the future will be predominantly, but not solely, 'Information Wars.' "[2]

Now nameless, faceless actors can potentially attain strategic objectives; and the possibility exists of not being able to identify the perpetrators and hold them accountable. Because of the diffusion of power, the anonymity and ease of access, the speed at which attacks can be mounted, and the paucity of observable preparation (resulting in little or no warning time), control or regulation of cyberspace attacks, as might be attempted by legal means, seems almost beyond comprehension. Yet, efforts must be made, for the stakes are high.

To ascertain at what points legal instruments might be effective either in preventing attacks or in mitigating their consequences, the ingredients of an attack can be factored into five parts for analysis.

- *Objectives to be sought.* These could range from overturning the ruling political power to the infliction of sheer pain.
- *Actors with motivation.* Motivations might be political, anarchic, criminal, monetary, or merely to vandalize.
- *Inexpensive, easy-to-use tools.* Low expense and ease of attaining powerful tools increase the potential for their use.
- *Access to a variety of targets* almost too numerous to count. A key route of access would be via the Internet.
- *Wide-ranging results*, from mere copying of information (no direct injury from the act) to contaminating the water supply of a large metropolitan area, to sparking economic chaos, to causing the release of a weapon of mass destruction.

Recognizing that these categories are interdependent, it is nevertheless useful to break each of them out for individual discussion.

Objectives

Access to information empowers. Someone who has the ability to review and change a pay schedule or an academic grade, for example, wields significant power. A person with access to private or classified information can use that information in a variety of ways, not all of which are beneficial or lawful. If the stakes are high enough, the temptation to copy, or alter, or pilfer information can be very strong.

Objectives for obtaining, altering, or obliterating information can vary, depending on the kind of information, its potential uses and value, and the ease in accessing it. Conceivably, governments could be toppled by a malefactor with the right information. The sheer volume of information flow—in the form of e-mail, financial transactions, and telephone calls, for example—means that if only a very small fraction is corrupted, intercepted, or stolen, enormous problems can ensue. Each day over a trillion dollars circulates electronically in the global currency market, and in excess of nine billion e-mail messages are sent in the United States alone. An error, loss, or siphoning rate in the currency market of only one one-hundredth of one percent (.0001) equates to more than $100,000,000. Numbers (and tolerances) such as these border on the incomprehensible. Consider the potential damage that could be wrought by an unauthorized person changing a bank's financial records by a simple instruction such as "change all sevens to ones." Or even more deviously, change every third seven to a one. Or, perhaps, change the first one thousand sevens to ones, change the

second two thousand fours to twos. Such instructions are trivial for someone with very modest computer literacy to compose, but the difficulty and cost to repair the damage could be significant.

Information has the special property that it can exist in more than one place at one time. This is at the same time an advantage and a disadvantage; for example, decision makers can view and act on the same information simultaneously, even though they are widely separated by distance. On the other hand, it can permit the compromise of valuable or sensitive information without its owner's knowledge.

Information also frequently has an element of timeliness; that is, information can be so perishable that it can have great value at one point in time and be worthless at a later—or conceivably even an earlier—time. Thus, the value of information depends on its availability, its integrity, and its confidentiality.

For those who would seek to attack the information of others, these would be the targets. Availability includes the loss of information, delay in its receipt, and the loss or delay of an information service. Integrity includes unauthorized changes in the information or the introduction of false data. Confidentiality means the unauthorized access to data or information that has some requirement for protection or privacy. In some cases, no damage to the data will result from exploitation. The data might be undisturbed, but its revelation could have severe repercussions.

An additional complication is presented by the medium of "cyberspace." Because cyberspace is viewed as a virtual realm, it carries an aura of unreality. From his bedroom, a young hacker connects to the Internet, travels thousands of miles in seconds, enters the computer system of a large corporation, and views the data contained on storage devices there. His unauthorized presence may or may not be detected. If he destroys data on the storage device, by a mere series of keystrokes on his keyboard, there is no fire, smoke, or noise. The information just disappears. The tactile experience, the physical environment in all its manifestations, the sense of personal danger, and the resultant damage from such an activity are unreal, truly virtual. They are far removed from an actual, corporal breaking and entering, but the transgression is the same.

Have any cyberspace events taken place to the extent that severe consequences, either monetary loss or damage to national security, resulted? To date, there is little evidence to support such a claim, but it is well within the realm of the possible. One might not know whether such attacks have taken place, in part, because if any institution suffers a loss, it has great incentives to suppress that fact. Confidence of investors or customers can be greatly undermined by such a revelation. Moreover, the fact that an institution was attacked and suffered losses can inspire additional attacks on other institutions. But central to the issue of

objectives, one must analyze what gain might accrue to the perpetrator of such acts. If the objective is sheer malice, or to inflict pain with no anticipation of gain, then protection is at the level of maximum difficulty. The same is true of terrorism, for example. If terrorists have an agenda or an objective, one seeks to deter them by withholding the objective. In effect, they are told, "You might be able to injure me, and to inflict great pain on me, but you cannot attain what you seek—so you might as well not even make the attempt." If, on the other hand, terrorists intend only to cause pain and suffering, and they place little or no value on their own lives or prospects, then they become exceedingly difficult to deter.[3]

If, rather than wanton damage, the objective is monetary gain, political change, or competitive advantage, it is helpful for the defender to try to anticipate or envision the objectives of the perpetrator. In that way, the defender can erect active or passive defenses to try to thwart an attack or to minimize or otherwise manage the consequences of a successful attack.

Actors

Closely coupled to the question of objectives is the issue of actors. In information attack it has become a simple matter for anyone, virtually anywhere, to gain unauthorized access to information. This means, literally, that any modestly literate person who has minimum capabilities in computing can be a participant in information attack or exploitation. From the lowest level (drawing moustaches on billboards or spray painting subway cars) to the highest (gaining unauthorized access to the information held by a large corporation or government), the difference in capability of the actor is remarkably small. This means that children can be recruited and taught the necessary skills; indeed many of the identified "hackers" have been minors.[4] The entry fee, in short, is low in terms of capability, and tends to be low in terms of age as well.

As a special commission reported to the President of the United States:

> Like any new tool in previous eras, computers can be used by those who prey on the innocent. International narcotics traffickers now routinely communicate with each other via computer messages. Hostile governments and even some transnational organizations are establishing cyber-warfare efforts, assigned the mission of crippling America's domestic infrastructure through computer attacks. Hackers destroy cyber-property by defacing homepages and maliciously manipulating private information. Pedophiles stalk unsuspecting children in computer chat rooms. Individuals post homepages with instructions to manufacture pipe bombs, chemical weapons, and even biological agents. Crooks

> break into business computers, either stealing funds directly or extorting payments from companies anxious to avoid more expensive disruption. Disgruntled employees, with valid access to their companies' system, can take steps to disrupt the business operations or steal proprietary, sensitive, and financial information. And our personal data is at risk of being unlawfully accessed and read by malicious individuals, without our knowledge, as it resides on or traverses communications and computer networks.[5]

No longer is espionage something undertaken exclusively—or, perhaps, even primarily—by professional spies in highly adversarial countries; the field is now open to rank amateurs on a global basis, with or without political, cultural, or religious axes to grind. No longer is sabotage reserved to anarchists, social activists, or well trained enemies of the State; the electronic environment of cyberspace makes it widely available for the doing. Actors may perform their activities in singular privacy, without personal mentoring and a modicum of instruction. Alternatively, they may be organized and scripted by anti-government groups, or as part of a government or industrial team. Accordingly, security forces guarding against electronic attack or exploitation will have great difficulty in "profiling" potential perpetrators.

State-supported acts are in a class of their own. As noted, however, they might well be indistinguishable from mere "hacking." The non-governmental culture that underwrites computer network attacks (CNA), however, knows no international boundaries, and it tends toward alienation and hostility. Here is an excerpt of the "Hacker's Manifesto," in which can be heard echoes of the ravings of the infamous Unabomber:

> This is our world now . . . the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt cheep [sic] if it wasn't run by profiteering gluttons, and you call us criminals. We explore . . . and you call us criminals. We exist without skin color, without nationality, without religious bias . . . and you call us criminals. You build atomic bombs, wage wars, murder, cheat, and lie to us and try to make us believe it is for our own good, yet we're the criminal. . . . Yes, I am a criminal. My crime is that of curiosity. . . . My crime is that of outsmarting you, something that you will never forgive me for. I am a hacker and this is my manifesto. You may stop this individual, but you can't stop us all . . . after all, we're all alike.[6]

Among the most feared and powerful of all actors in attacks on information are insiders. In part, this is because the strength and integrity of a network is

largely a matter of perception. From an outsider's point of view, a network might appear very robust. It has many nodes, many links, many alternatives to routing information, and good security. To an insider who knows the network, there might appear to be a substantial number of vulnerabilities. An outsider is reluctant to attack what seems to him to be a very difficult, very adaptive target. The insider, however, knows the system and its potential weaknesses. This is why the insider is of such high concern—he's inside the firewall, inside the security. His trustworthiness and reliability then ascend to the level of pivotal issues.

Motivation of actors must be viewed as a major variable in the process. For one who acts from the outside, the rewards might be monetary, political, religious, or perhaps just personal satisfaction. For an insider, the motivations might be much less consequential. Changes in workplace environment or relationships, revenge, malicious acts at the behest of an outsider, the challenge, sheer curiosity, or even a misguided good-faith effort to fix a problem can all stimulate an insider to action that could be exceedingly damaging and costly.

Because "cyberspace" has been so ill-defined, because it was initially commandeered by the youth of the world, because it is so easily accessible, and because it is global and instantaneous, almost anyone can become an actor within its confines.

Tools

On a daily basis, new tools for attacking networks are honed and made available via the Internet to anyone who wants them. Many are free merely for the downloading. According to Bruce Middleton, an expert on the subject, "The most popular of these tools fall into several categories: password crackers, port scanners, war dialers, general network vulnerability scanners, and intrusion detection systems."[7]

Because many firewalls and other security devices require a password to breach them, *password crackers* attempt to determine what the user's password might be. It is a well-known fact that the most widely used password, owing to the fact that employees are lazy and do not understand (or often care about) security, is "PASSWORD." Easy-to-crack passwords involve variations of people's names, their addresses, their pet's names, or the names or nicknames of their favorite sports team. If a match fails on these easy passwords, the password cracker employs a dictionary that very rapidly tries words until the password is discovered. In general, the password cracker can no longer just try each potential word at the locked door (firewall) of the target site, for now most sites can detect such efforts and will not accept password attempts beyond about three. So, some other method must be used, such as locating the password file on the

victim's computer and trying to decrypt it, or catching passwords "on the fly" with a "sniffer."

Port scanners "knock on the door" of networks to see if they are unlocked. Many, many computers and services connected to the Internet, for example, have no protection against penetration. Port scanners try to find these unprotected ports and then gain access to information on the victim computer. Many of the "no need to dial up" or "on all the time" services (Integrated Services Digital Network (ISDN) and "Web TV" fall into this category) can place their users in a vulnerable position if they do not include security services. It is the function of port scanners to find those unsecured computers. "Strobe" is an example of such a scanner. It "attempts to locate and build a picture of all ports on one or several hosts in a given network, using what is considered a very efficient algorithm that helps optimize speed. It then displays all those ports that are turned on, or 'listening.' "[8] Strobe is available on the Internet at no cost.[9]

War dialers organize banks or networks of modems to dial the same number repeatedly in order to overload it or keep it from receiving other signals, or they might dial many numbers rapidly in the hope of detecting a computer on the other end. These can be very effective in situations where computers are networked but also employ modems to the outside via phone lines. Often computers are manufactured with internal modems installed. Users then merely have to connect their computers to a telephone line, and they can operate in cyberspace outside the firewall that protects the network to which their computers are also attached. Because users can connect to the outside directly, the "outside" can also enter their computers via this route, around the firewall or protective device. War dialers are easy to implement, and can be used with devastating effects on a targeted site.

General network vulnerability scanners. Perhaps the most famous of these is SATAN, the Security Administrator's Tool for Analyzing Networks. It has many functions and has been available, also for free, literally for years on the Internet. SATAN analyzes a target computer system and provides the user a detailed report on the kind of equipment, directories, and hosts supported.

Intrusion detection systems help secure computer systems. They have a variety of bells and whistles, some of which are detailed record keeping of attempted intrusions, alerts to operators of attacks, and recommended actions to correct the problem or even to respond. In this class one finds ISS SafeSuite, Cisco Net Ranger, NAI CyberCop, and AXENT Technologies NetRecon, to mention only a few.

In addition to these technical tools, there are also "social tools" commonly in use. For example, there is "dumpster diving," where trash is screened for

passwords, file information, personal information, and any other data that might aid a perpetrator's efforts. This is a common procedure; it has been used for years, and it still pays off. Often, armed either with the material gathered from dumpster diving or sheer gall, a potential attacker will then engage in what has become known as "social engineering." For example, a telephone call will be made to an employee in the targeted organization and a misrepresentation made in order to elicit the compromise of protected information. A common ruse is to call an employee and pretend to be an "information management systems troubleshooter." The employee is told that the system is experiencing difficulties, and that the employee's system name and password are needed to fix the problem. For many of the same reasons that "password" has the highest frequency of usage, this technique is very often successful, because it takes advantage of the propensity of people to pay little attention to security.

Peter G. Neumann has summarized quite succinctly the potential for "computer misuse," in the table reproduced below:

Mode	Misuse type
External	
Visual spying	Observing of keystrokes or screens
Misrepresentation	Deceiving operators and users
Physical scavenging	Dumpster-diving for printout
Hardware misuse	
Logical scavenging	Examining discarded/stolen media
Eavesdropping	Intercepting electronic or other data
Interference	Jamming, electronic or otherwise
Physical attack	Damaging or modifying equipment, power
Physical removal	Removing equipment and storage media
Masquerading	
Impersonation	Using false identities external to computer systems
Piggybacking attacks	Usurping communication lines, workstations
Spoofing attacks	Using playback, creating bogus nodes and systems
Network weaving	Masking physical whereabouts or routing

Pest programs	Setting up opportunities for further misuse
Trojan horse attacks	Implanting malicious code, sending letter bombs
Logic bombs	Setting time or event bombs (a form of Trojan horse)
Malevolent worms	Acquiring distributed resources
Virus attacks	Attaching to programs and replicating
Bypasses	Avoiding authentication and authority
Trapdoor attacks	Utilizing existing flaws
Authorization attacks	Password cracking, hacking tokens
Active misuse	Writing, using, with apparent authorization
Basic active misuse	Creating, modifying, using, denying service, entering false or misleading data
Incremental attacks	Using salami attacks
Denials of service	Perpetrating saturation attacks
Passive misuse	Reading, with apparent authorization
Browsing	Making random or selective searches
Interference, aggregation	Exploiting database inferences and traffic analysis
Covert channels	Exploiting covert channels or other data leakage
Inactive misuse	Willfully failing to perform expected duties, or committing errors of omission
Indirect misuse	Preparing for subsequent misuses, as in off-line preencryptive matching, factoring large numbers to obtain private keys, autodialer scanning

Source: Peter G. Neumann, *Computer-Related Risks* (New York: Addison-Wesley Publishing Company, 1995).

Targets

The variety of objectives, the multiplicity of actors, and the great array of tools together are a clear indicator that the target set is large and rich. Targets range from very specific systems, persons, or infrastructures that are linked tightly with a perpetrator's objectives, to sheer random, serendipitous discoveries. Depending on the motivation of attackers and the tools available to them,

the attack might be precisely focused on a known, discrete target; or it might take the form of a blunt, across-the-board destructive blow to an entire information system. The attacker might use a variety of techniques to gain access, and the effort might take a long time—perhaps spanning months, or even years.

Monetary flows and financial databases, because they offer the prospect of great gain with comparatively low pain or risk, are prime targets. Presumably, the greater the sensitivity or the value of information, the more carefully it will be protected. This is only a presumption, however, because many information systems and vital services were designed, and constructed—and they are operated—with no conception of, or attention to, any threat.

National infrastructures have come under increasingly intense scrutiny in recent years as potential targets for information attack. Because of the growing danger, President Clinton, on July 15, 1996, issued Executive Order 13010 establishing a Presidential Commission for Critical Infrastructure Protection (PCCIP). Chaired by retired Air Force General Robert T. Marsh, the commission identified eight infrastructures that must be protected from the depredations of information and other kinds of attack. These were: electrical power, gas and oil (storage and transportation), telecommunications, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government services. The PCCIP presented the results of its inquiry in October 1997.

Another attractive target is the US Department of Defense. The Deputy Secretary of Defense testified in 1998 that "95 percent of all of our communications now go over public infrastructure—public telephone lines, telephone switches, computer systems, et cetera."[10] Much of this departmental information is routine and administrative, which is not to say that it is unimportant. Virtually all logistics and medical information on service members travels over the public infrastructure, for example. If antagonists were unaware of such a dependency before, they clearly are now mindful of that vulnerability, and one prudently must assume that they are planning ways to exploit it.

If, indeed, essentially all computers in the world are connected, then that constitutes about as target-rich an environment as can be imagined.

Results

The horizons being very wide and deep for information operations, and specifically computer network attack, the results also occupy a broad spectrum. From a mere nuisance of defacing a web page with a political message to the loss

of great amounts of money, or potentially lives, the results vary with the objectives, attackers, tools, and targets, as well as the vigor, and the rigor, with which targets are defended.

Exhortations have been raised that the United States is a prime candidate for an "Electronic Pearl Harbor." Those who issued such a warning meant that the United States is unprepared and not watching very closely, can be surprised, and that the results might well be truly shocking. Of course, beyond the initial trauma, what Pearl Harbor (and the subsequent declarations of war) accomplished was to anger the American public and focus it laser-sharp on conducting war against the Axis powers. Given these facts, some argue that the reason more catastrophic events have not occurred—bringing down the Internet, for example, which some have contended is possible—is that potential attackers fear the "post-Pearl Harbor" backlash.

To date, no catastrophic event has occurred because of computer network attack. Estimates of loss are difficult to make and for that reason often lack credibility. If a particular company is prevented from doing business on the Internet for, say an hour, what is the cost of that? Was a once-in-a-lifetime opportunity missed, with incalculable costs? Opportunity costs are especially difficult to estimate, and that is frequently what is lost in a computer network attack.

So, results could vary from the time lost to clean up the graffiti on a defaced website to, perhaps, billions of dollars in a financial transaction, drug deal, or extortion. National infrastructures could be successfully attacked by CNA, with very disruptive results, and perhaps high innocent loss of life.

The potential to wreak great damage virtually anywhere in the world, almost instantaneously, at very low cost, by almost anyone is imminent. International law offers a prospective tool to attempt to help control or mitigate the potential dangers. Each of the ingredients of an attack listed above offers a possible pressure point for legal application. As analyses and discussions on the subject proceed, these five points can provide a useful framework upon which to build.[11]

Notes

1. Distinctions have been made in the literature of information warfare between data, information, knowledge, and wisdom. This essay deals with tangibles: information is data that has been *organized* or *assessed* in some manner. *Knowledge* and *wisdom* have no independent existence outside the observer. Data and information exist regardless of whether they are known or interpreted.

2. Thomas J. Czerwinski, *The Third Wave: What the Tofflers Never Told You*, 3 STRATEGIC FORUM #72 (1996).

3. For an extended discussion, see Roger W. Barnett, *Information Operations, Deterrence, and the Use of Force*, NAVAL WAR COLLEGE REVIEW, Spring 1998, at 7–19.

4. "Hackers" seek to differentiate between themselves and "crackers." They view the latter as malicious, irresponsible social elements, while they, merely in the interest of science—or perhaps helpfulness—are doing no harm.

5. William Cohen, Janet Reno, William Daley, and Jacob J. Lew, Preserving America's Privacy and Security in the Next Century: A Strategy for America in Cyberspace, A Report to the President of the United States, September 16, 1999.

6. Revelation and LOA [Legion of the Apocalypse], The Ultimate Beginner's Guide to Hacking and Phreaking, Volume 2, April 1, 1997.

7. Bruce Middleton, *Using the Hacker's Toolbox*, SECURITY MANAGEMENT MAGAZINE, June 1999, www.securitymanagement.com.

8. *Id.*

9. According to Middleton, *supra* note 7, most of these free tools can be acquired at: ftp://coast.cs.purdue.edu/pub/tools.

10. *Quoted in* US Joint Chiefs of Staff, INFORMATION ASSURANCE: LEGAL, REGULATORY, POLICY, AND ORGANIZATIONAL CONSIDERATIONS 55 (4th ed., 1999) 52.

11. Following is a short list of references on the subject:

JAMES ADAMS, THE NEXT WORLD WAR: COMPUTERS ARE THE WEAPONS AND THE FRONT LINE IS EVERYWHERE (1998).

Bruce D. Berkowitz, *Warfare in the Information Age,* ISSUES IN SCIENCE AND TECHNOLOGY, Fall 1995.

JOHN ARQUILLA AND DAVID RONFELDT, IN ATHENA'S CAMP: PREPARING FOR CONFLICT IN THE INFORMATION AGE, Santa Monica, CA: RAND, (1997).

RICHARD BRODIE, VIRUS OF THE MIND: THE NEW SCIENCE OF THE MEME (1996).

ALAN D. CAMPEN AND DOUGLAS H. DEARTH, CYBERWAR 2.0: MYTHS, MYSTERIES, AND REALITY (1998).

DOROTHY E. DENNING, INFORMATION WARFARE AND SECURITY (1999).

David J. DiCenso, *IW Cyberlaw: The Legal Issues of Information Warfare*, AIRPOWER JOURNAL, Summer 1999, at 85–102.

LAWRENCE T. GREENBERG, SEYMOUR E. GOODMAN, AND KEVIN J. SOO HOO, INFORMATION WARFARE AND INTERNATIONAL LAW, Washington, D.C.: National Defense University, (1997).

MARTIN C. LIBICKI, WHAT IS INFORMATION WARFARE? Washington, D.C.: National Defense University, (1995).

WALTER GARY SHARP, SR., CYBERSPACE AND THE USE OF FORCE (1999).

MARK RUSSELL SHULMAN, LEGAL CONSTRAINTS ON INFORMATION WARFARE, Occasional Paper No. 7, Maxwell Air Force Base, AL: Air University, 1999.

DON TAPSCOTT, GROWING UP DIGITAL: THE RISE OF THE NET GENERATION (1998).

Chairman of the Joint Chiefs of Staff, Joint Publication 3-13, Joint Doctrine for Information Operations, (1998).

Internet sites:

www.infowar.com

www.terrorism.com/infowar/index.html

www.cert.org/

www.twurled-world.com/Infowar/Update2/cover.htm

www.antionline.com

www.itaa.org

IV

Information Operations, Information Warfare, and Computer Network Attack

Their Relationship to National Security in the Information Age

Daniel T. Kuehl*

Introduction

What is "information warfare"? Is it nothing more than a bumper sticker, used as a "quick fix" rescue for budgets and programs that find it useful to attach themselves to the hot new concept? Is it such a revolutionary new amalgam of technologies and concepts that old and traditional forms of warfare are soon slated to fall into the same receptacle in which outmoded military technologies such as the catapult and war galley slumber? Is warfare as we understand it, featuring "blast, heat, and fragmentation," about to become obsolete?[1] The intent of this brief introduction to information warfare (IW) and information operations (IO) is to both explore these issues and present the thesis that they are best understood in light of the environment in which they take place—the information environment—and to explore the relationship of that environment to the specific topic on which this book is focused, computer network attack.

What is Information Warfare?

A useful starting place is to trace the evolution of the term information warfare itself. The earliest use of the term in the United States probably originated in the Office of Net Assessment, where in the 1970s Dr. Tom Rona was investigating the relationships among control systems, a field known as cybernetics. Dr. Rona described the competition between competing control systems as "information warfare," in the sense that control systems can be described as the means for gathering, processing, and disseminating information, processes which can be diagrammed and described with flow and feedback charts of mind-numbing dryness and complexity.[2] In 1993 the Department of Defense published an official definition for the term, in a highly classified DoD Directive, TS3600.1. There were actually several definitions, at differing levels of classification.[3] Not surprisingly, this definition was frequently revised as the operational and organizational implications of the concept evolved. The current definition has the record for longevity—more than five years at the time of this writing, since the promulgation of the current guidance on information warfare and information operations in DoD Directive 3600.1 on December 9, 1996.[4] The publication of Joint Publication 3-13, Joint Doctrine for Information Operations, in October 1998 probably ensures that the current official DoD definitions of IW and IO will remain in effect for some time longer.[5]

The present definitions leave much to be desired, however, if one is hoping to find explanations that clarify and explore what might constitute the character, conduct, and intent of IW and IO. But since one must understand what IO is in order to move to its less comprehensive building block, IW, these definitions do provide a useful starting point:

> Information Operations: Actions taken to affect adversary information and information systems while defending one's own information and information systems.

> Information Warfare: Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.

There is actually a second sub-activity of IO that is critical to national security in the Information Age, namely information assurance (IA), defined thus:

> Information Assurance: Information operations that protect and defend information and information systems by ensuring their availability, integrity,

> authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.[6]

While these definitions throw a less-than-blinding light on their constituent activities, there is one critical theme that they are intended to bring out, and that involves "who" does them and "when" they are done. IW is clearly a military activity conducted under a special set of circumstances, whereas IA involves not only the military, but also government at all levels, and even portions of the private sector. Therefore, IO as an activity goes far beyond just the military during conflict, to include the government and a wider range of private sector activities than perhaps that sector or even the government recognizes.

Most US service concepts of IW rest in part on the concept of the "information environment." Whether described as an environment, realm, domain, or whatever, there is a clear sense that information has become some kind of "place" in which crucial operations are conducted. The Army's trailblazing 1996 doctrinal publication, Field Manual 100-6, Information Operations, even speaks of a "global information environment [and] battlespace" in which conflict is waged. The latest version of the USAF's basic doctrinal publication, Air Force Doctrine Document 1, published in 1997, explicitly addresses the need to dominate the information realm, and discusses information superiority as "the ability to collect, control, exploit, and defend information while denying an adversary the ability to do the same . . . [it] includes gaining control over the information realm. . . ."[7] Joint Pub 3-13 defines it somewhat differently as "[t]he capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same." Both, however, share the sense that information superiority involves doing something to the adversary while protecting ourselves in order to control and exploit the information environment. Using this philosophy, then, IW and IO can be described as the *struggle to control and exploit the information environment*, a struggle that extends across the conflict spectrum from "peace" to "war" and involves virtually all of the government's agencies and instruments of power.[8] One appeal of this approach is that if one replaces "information" with "aerospace" or "maritime," you have defined air and naval warfare, or more appropriate to our purposes, airpower and seapower. Information operations can thus be described as those activities that governments and military forces undertake to control and exploit the information environment via the use of the information component of national power.

This immediately raises another question: what is the information component of national power? More than just another bit of computer-age terminological fluff, its origins actually predate this decade, starting with the strategies developed by the Reagan Administration in its very real struggle with the former USSR. In 1984 the Reagan Administration issued National Security Decision Directive 130, US International Information Policy, which outlined a strategy for employing the use of information and information technology as strategic instruments for shaping fundamental political, economic, military, and cultural forces on a long-term basis to affect the global behavior of governments, supra-governmental organizations, and societies to support national security.[9] This is hardly a new concept, and clearly governments and leaders have been exploiting the information environment for centuries. Indeed, one could argue that the stone carvings that Assyrian rulers made of conquered peoples and cities being enslaved and pillaged were intended as much to cow and terrify current and potential subjects as to inform archeologists thousands of years later about what hard and cruel folks they were. Regardless of the fact that the information technology being employed was stone and chisel, and not microchip and computer network, this was exploitation of the information environment for strategic political objectives.

Two examples from this century will suffice to illustrate the critical importance of this environment to national security. The first took place on August 5, 1914, when the royal cableship *Telconia* sortied into the North Sea and severed all five of Germany's direct undersea telegraph links with the outside world. After that date, the view that the rest of the world had of The Great War increasingly passed through a lens located in London. This enabled British information warriors to mount a very effective strategic perception management campaign that eventually helped bring the United States into the war on the side of the Allies, thus moving from strict neutrality to waging war to "make the world safe for democracy." Great Britain was exploiting the information component of national power. The second example comes from the Cold War and the efforts by the United States and some of its allies to exploit another segment of the information environment—radio—to weaken the political cohesion of the Soviet Union and the peoples it controlled. Radio Free Europe did not by itself, of course, cause the fall of communism and the Soviet government, but it certainly had its role to play. It is perhaps instructive that certain elements within the former Soviet Union still blame Western IO for communism's collapse.[10] Yet since both these examples employed old information technologies—telegraph cables and radio—they also beg the question: what is the role of the computer in all of this?

A New Geostrategic Context

The previous examples raise the question of what is so new and different about the current state of the "information environment" to warrant all the fuss about "computer network attack" and information warfare. The answer is fourfold: cyberspace, digital convergence, global digital omni-linking, and computer control of infrastructures, all of which are synergistically combining to create a new geostrategic context for national security.

One's receptivity to the changes of the information revolution is often revealed by the reaction to the word "cyberspace." At the very utterance of the word, doubters and skeptics display intellectual and sometimes even physical discomfort, while the "digerati" and those at ease with the technologies of the information age react as if someone had said "traffic" or "radio" or any other commonplace term. Almost everyone is familiar with the use of information as a tool, a process, even a weapon—recall the earlier comment about "blast, heat, and fragmentation"—yet while all of these remain not only applicable but even vital to the new and evolving "American way of war," none in isolation goes far enough. This chapter argues that the synergistic effects of electronic digital technology, acting in and on societies that are becoming increasingly information-dependent, have made information into a virtual environment, with cyberspace as its physical manifestation. Cyberspace, defined here as that place where electronic systems such as computer networks, telecommunications systems, and devices that exert their influence through or in the electromagnetic spectrum connect and interact, has always existed, but not until mankind invented technologies that operated via the electromagnetic spectrum did it become "visible" and noticed.[11] A useful analogy is outer space. It has always been there, but not until humans developed technologies for extending our activities into it and used it to affect terrestrial affairs did we fully comprehend that it is another physical and operational environment in addition to the land, sea, and air. Outer space does not have the same physical presence or properties of land or water because you cannot "weigh" it or "measure" it in a useful sense, but it nonetheless exists because we can see the physical results of things that happen there.[12]

The physical laws and principles that govern and delineate how systems function in these environments are the borders that fix their boundaries.[13] Submarines, for example, function very well in an environment governed by the laws of hydrodynamics, but they cannot fly. Armored fighting vehicles function effectively on land, but they are useless in space. All of these distinct and unique environments synergistically interact with each other, and the same holds true for cyberspace. The devices and systems that operate in cyberspace—radios,

radars, microwaves, computer networks—function because they conform to and exploit the laws governing radiated and electronic energy. We can date our use of this environment to the mid-19th Century and the invention of the telegraph, which was the first telecommunication system to operate in accordance with the laws of this medium.[14] The following century saw regular and ever-more technologically sophisticated advances in our ability to control and exploit this medium—undersea telegraph cables, radio, television, microwave relay, even communications satellites—that extended the reach of telecommunications to continental and eventually intercontinental distances. We have increased the volume of information that we can store, manipulate, and transfer to previously unimaginable proportions, but it was only in the closing quarter of the 20th Century that the fortuitous, perhaps even serendipitous, marriage of these technologies with the microchip led to attainment of "critical mass" and the emergence of cyberspace as a full fledged environment in which military forces and society in general—politics, business, education, and more—began to learn how to operate. Given this definition of cyberspace, we see the link to computer network attack; cyberspace is the physical environment in which such operations take place.

Cyberspace is the basic arena in which two additional developments of the information revolution are transforming the strategic landscape: the increasing capability to transform almost any kind of information into ones and zeroes, in what is known as *digital convergence*, and the growing Internetting of global telecommunications media in a condition referred to here as *global omni-linking*. Although these developments are distinctly different, they are at the same time synergistic and interdependent. Thomas Kuhn suggested in his landmark study of scientific revolutions that the history of technological advancement has not been one of steady discoveries or developments, but rather one marked by spikes or sharp advances that flow from extraordinary finds or revelations that yield discontinuous and revolutionary changes.[15] Such has been the case with information technology. Advances in communication technologies prior to the middle of the 20th Century were relatively linear—telegraph to telephone to radio and so forth. The break point came with the invention of the microchip because the synergistic advances in information storage, manipulation, and transmission capabilities made possible by digital convergence are happening at an ever-increasing and nonlinear rate. These developments have occurred in two areas, the *speed* of information manipulation/transmission, and the *volume* of information that can be manipulated/transmitted. The combination of these attributes with computer-enhanced and controlled telecommunications systems have led to the "*omni-linking*" of the electronic digital world. In a word, the globe is now

"wired." The explosion that has resulted from the application of the microchip to communications technologies has formed the new science of telematics—the marriage of computers and telecommunications.

Telematics has created a new operational environment. The technology of the telematic age we use to exploit cyberspace is new, perhaps less than two decades old, and global omni-linking is inseparably tied to the emergence of cyberspace as an operational environment. While current technology is actually rudimentary compared with what the future holds in store—compare the level of aviation technology in the 1930s (biplanes) with what came just half a century later (747s and B-2s)—the omnilinking of the world is increasing every day, as more and more computer networks and telecommunications systems tie together and pass the lifeblood of today's economic and political world . . . digital information. The degree to which our societal dependence on this environment is growing is startling. Our military forces already depend on it. The Persian Gulf War of 1990-91 simply could not have been fought in the way we fought it without precision information for precision weapons, command and control systems that enabled us to operate like a matador around a woozy and half-conscious bull, or satellite communications links that enabled organizations half a world away (NORAD) to monitor Iraqi missile launches and pass targeting information to Patriot batteries to engage the missiles.[16] Our microchip-driven information collection, storage, manipulation, and transmission capabilities are so advanced, and the links that move the information around so Internetted, that we worry that TV news commentators on the east coast could skew election results on the west coast by announcing "analysis of voting trends indicate candidate 'Z' has won the election." The global economy cannot function without the constant supply of digital electronic information. It has become a form of energy or capital, and global business is utterly dependent on telematic systems and capabilities to keep the world's economy going twenty-four hours a day. Business practices such as "just in time inventory," or military techniques such as "just in time logistics," cannot function without the digital information that fuels it. In a very real sense, Joint Vision 2010,[17] which could be called the "new American way of war," is possible only if American forces possess "information superiority," defined by Joint Pub 3-13 as "[t]he capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same." The "Internet" is neither a finite place nor a collection of gadgets such as routers and switches; it is a description of the increasing omni-linking of the world. Thinking of the Internet in terms of its users, such as "America OnLine" or "CompuServe," or in terms of uses, such as chat rooms or E-commerce, is as shortsighted as describing

aerospace in terms of an airline. While some dismiss this environment and the Internet as merely entertainment or worse, this view ignores the fact that a very large percentage of the information currently available on TV or in print would fall into the same category. Few, however, would deny the impact of visual media on the American populace's support of the Vietnam War or the impact of the printed word on democracy and freedom via the "Declaration of Independence" or "Emancipation Proclamation." What is different is that the Internet and omni-linking make it increasingly possible for that televised image to be seen instantly by an ever increasing percentage of the world's population, or for that opinion-shaping paper to be sent to tens or even hundreds of millions of people simultaneously and in their own language.[18] Digital convergence, combined with connectivity, adds up to the second major part of the fundamental difference between the information age and the period "BMC"—"Before the Micro Chip."

The final major development shaping the new geostrategic context is the increasing reliance on computerized networks for the control and operation of key infrastructures in advanced societies. The growing reliance on these systems for the control and functioning of an increasingly large segment of the infrastructures on which we depend for economic, social, political, and even military strength is both a boon and vulnerability. As suggested by Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.1, Defensive Information Warfare, "use breeds dependence, and dependence creates vulnerability."[19] Whether it be the supply of energy (electricity, oil, gas), the management of transportation (railroads, air traffic control, motor vehicle movement), the transference of digital wealth (electronic funds transfer, digital banking, control of stock exchanges), or the operation of the very telematic media that supports the entire structure, look below the surface of almost any segment of daily life in modern societies and one will find Internetted and interlinked computer systems.[20]

The degree to which this is invisible to the general populace is illustrated by a real incident. In February 1996, Washington DC suffered a tragic but relatively typical industrial-age accident—a train wreck. During a snowstorm a commuter train collided with a freight train, and several people were killed. The investigations by the news media examined almost every aspect of the accident, including the signaling system that provided instructions to the train operator (who was also killed, heroically trying to warn passengers instead of saving himself) via the ubiquitous signal lights that line railroad tracks all over the world. The news media focused on whether the operator saw the signals, whether they were properly placed, or whether they functioned properly. None asked whether the signals

had been electronically tampered with (they had not been), nor even raised the issue of how the signals were controlled or where those controls were located. They were controlled, of course, by Internetted computer systems, and the computers which control the rail signals for the trackage in Washington DC are located at the operations center for CSX Railways, in Jacksonville, Florida, several hundred miles distant. This is an illustration of how deeply imbedded within modern societies such control systems have become, and how unaware most of us are of their functioning.[21]

It is a government responsibility, however, to not only be aware of such developments, but also to take precautionary and preventive measures to mitigate potential disruptions to the effective functioning of systems upon which the society and national security depend. In July 1996, the Clinton Administration issued Executive Order 13010, which directed the formation of a unique commission, the President's Commission on Critical Infrastructure Protection, or PCCIP, which brought together senior governmental officials and representatives from those private sector industries and businesses that comprised these key infrastructures into a commission tasked with studying the vulnerability of these infrastructures to disruption. While the commission examined both the physical and cyber threats, they freely acknowledged that their emphasis was on the cyber threat, in part because it was—and remains—less well understood than physical threats. Their conclusion that the threat is real and growing might seem unsurprising and perhaps even preordained, but nonetheless reflects the growing awareness that our very dependency on computerized control of infrastructures creates an inherent vulnerability that is at the heart of hypothetical scenarios for information warfare in which computer network attacks on critical infrastructures "take down" key segments of those infrastructures and thus generate cascading effects on such systems as transportation, banking, or emergency services. It was the need to respond to this vulnerability that caused the Clinton Administration to issue Presidential Decision Directive (PDD) 63 on May 22, 1998, establishing a national coordinator for infrastructure protection within the National Security Council and creating an organizational structure by which such threats and vulnerabilities could be mitigated. PDD 63 called for a public sector-private sector partnership to develop cooperative procedures and organizations to assess the threats and vulnerabilities and create countermeasures, and thus stands as a landmark step in what is now called computer network defense (CND) against the threat of what has in some quarters been termed "infrastructural warfare" employing computer network attack (CNA).[22] But as perhaps the key element in information warfare, is the computer network the target, or merely the means to the target?

Computer Networks, National Security, and the "Metanetwork"

This chapter has already used several terms relating to computer networks without defining those activities. The current CJCSI 3210.1, Joint Information Operations Policy, dated November 6, 1998, currently includes three such activities, defined thus:

> Computer Network Attack (CNA): Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.
>
> Computer Network Defense (CND): Measures taken to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction.
>
> Computer Network Exploitation (CNE): Intelligence collection operations that obtain information resident in files of threat automated information systems (AIS) and gain information about potential vulnerabilities, or access critical information resident within foreign AIS that could be used to the benefit of friendly operations.[23]

The thread that ties these activities together is the computer network. The network may be the actual target, in the sense that the attacker wishes to make the network cease its function of transferring information. It may be the means to affect another target, such as a database or other information-based process, in which the attacker does not want to cut the network, but rather use it in order to impact or degrade an adversary's decision-making process. The objective of computer network defense is to prevent an adversary from doing either of these to our networks. Computer network exploitation is specifically concerned with intelligence operations. While the dividing line between CNA and CNE may well be very murky—indeed, a single keystroke might be the only difference—we will not discuss CNE or even CND further, in part because those operations bring along their own baggage train of thorny issues and unresolved questions. CNA will be a sufficiently difficult problem to address here.

Imagine for a moment that a warrior (the specific service or warform is irrelevant) has just destroyed a critical target, comprised of all the computerized databases contained in the enemy's central C3 facility. Does it matter if this was done with a laser-guided aerial bomb, a five-inch round from a warship at sea, a

120mm round from a tank, a ballistic weapon dropped from space, or via malicious programming code "delivered" by computer intrusion? The definition of CNA cited above does not clearly state the answer, but it is this author's contention that the means used is immaterial; since the intent clearly conforms to the spirit of the definition, any or all of the examples just cited could be CNA. In all but the last case, however, warriors and jurists alike probably consider themselves to be on fairly firm ground. It is the last case that gives everyone pause. In part, this comes from our intellectual and doctrinal desire for clarity. Warriors seek to clearly distinguish between different kinds of operations so that they can establish clear lines of authority and control. Unfortunately, this may not be fully possible in the information battlespace. The example cited above could be air, naval, land, or space warfare, in addition to being information warfare. This is not unique to information warfare, although we do not often examine military operations from such a multi-doctrinal perspective. During the October 1973 Yom Kippur War, for example, once Israeli armored forces crossed the Suez Canal in their counteroffensive they began destroying Egyptian surface-to-air missile forces, which enabled the Israeli Air Force to expand operations. This is a wonderful example of what airmen term Suppression of Enemy Air Defenses, or SEAD. Doctrinally, SEAD is a part of what is in turn called Counterair Operations—things done to seize and maintain control of the air. Thus, armored forces were part of an air superiority operation at the same time they were engaging in what ground forces would call maneuver warfare. This same kind of doctrinal flexibility must also be applied to information warfare and CNA.

The first aspect of CNA mentioned above focused on the destruction or negation of a network. Regardless of whether this is accomplished kinetically—the laser guided bomb, for example—or via cyberspace, the intent remains the same, to prevent the adversary's use of the network. We will not consider kinetic means further, since they are already well understood, but the use of the computer to negate another computer is less well understood. There is no need here to discuss the intricacies and details of computer code, and such issues are addressed in great detail in a myriad of books on computer security and information technology. That said, a word or two on the basic context are in order.[24] The basic objective of virtually any computer intruder or hacker is to be able to operate within the system as if he/she owned it. Once this level of access is gained, the pseudo-owner can then change programs, functions, addresses, and almost any other aspect of the way the computer or the entire network in which it resides operates. Thus, an intruder that obtains root access into a computer network that controls personnel records, for example, could perhaps alter the content of those records or change how those records are stored or transferred.

The implications of this for the proper functioning of any computer network, be it military, government, or business, are obvious.

As pointed out earlier, modern technologically advanced societies are increasingly dependent on computer networks for a growing range of societal and national security needs. If the computer system that controls rail operations in the southeast United States can be degraded, for example, it will slow down or perhaps even stop the movement of military forces that depend on rail links to move to their deployment locations. If the telephone system that supports Scott Air Force Base, headquarters of US Transportation Command, Air Mobility Command, and the Tanker-Airlift Coordination Center, can be severely degraded it could seriously hinder the movement of US forces overseas. If the energy management system (electric, gas, and oil) in the northeast could be degraded during severe winter weather it might cause a refocusing of national political and strategic attention away from a distant and perhaps poorly-understood overseas problem to an unfolding disaster right at home. Some of the discussion of infrastructural vulnerability seen recently has given far too little credit to the resiliency and robustness of these networks. However, while loose talk of "taking down" entire national infrastructures is fanciful at best, it also remains true that all of these infrastructures are in some degree vulnerable to intrusion and degradation. Examples as recent as the 1999 Kosovo conflict, during which a variety of allied computer networks such as the NATO e-mail system came under attack via what was a "denial of service" effort to overload the system with electronic traffic, indicate that this will be an active battlespace in the future.[25]

If the intent of a CNA is to partially or completely deny access to or use of the network, defenders are faced with a thorny set of problems, but at least they will probably be aware that the system has been targeted. When you receive multiple thousands of unanticipated e-mail messages within a short span of time in what is termed a "spam" or denial of service attack, you can reasonably assume that someone—even though you might not know whom—means you harm. CNA that does not attempt to overtly prevent use of the system, however, but rather is intended to covertly subvert its purpose by changing the content, is perhaps an even more difficult problem. Let us use the analogy of a pipeline that is carrying jet fuel. In traditional, kinetic warfare, we would target it for destruction from the air, and a smart airplane carrying PGMs would come along and neatly blow the thing apart, thus preventing the enemy from refueling his jets from it. But what if we did not want to be so noisy? We could send a special operations unit to the pipeline, attach to it a small pumping device that injects a small but fatal (from a jet fuel standpoint, at least) amount of some nasty foreign substance, and, even though the pipeline itself is still intact, render the stuff flowing through the

pipeline unusable. It is a perfect analogy for digital modification of data, and it might be virtually invisible until too late. Let us assume that the computer code for "bomb, 500 pound" is a combination of forty-four ones and zeros, while the code for "bomb, 4,000 pound" is another combination of forty-four ones and zeroes—almost, but not quite, identical. The opportunity for logistical chaos is immediately apparent. If one eighth the anticipated number of munitions show up at Base X, but all of them are too large for the aircraft at that base to carry, some significant friction has just been injected into the air war. We have a long history of instances where accidental but incorrect computer code in systems that deal with telecommunications or energy has caused significant malfunctions with those systems, and we have seen a growing number of cases of intentional intrusion into these and other such computer networks.[26]

The mindset of many senior strategic leaders regarding the computer still seems to be that they are large, expensive, and stand alone in their respective "data center" somewhere. The reality is just the opposite—for they are small (and getting smaller every week), cheap (and getting cheaper every week), and interconnected on a global scale. It can be a difficult realization that if you operate a computer that is plugged into a telephone, you are theoretically connected to every other computer on the face of the earth that is also connected to a telephone, even if it is a cell phone—hence the strategic importance of what this chapter calls "omni-linking," because the globe is literally covered with countless individual computer networks that are nonetheless all part of the growing global "metanetwork" to which tens of millions of individuals, organizations, and entire societies are connected. It would seem to be inescapable that as more and more human activity is conducted in cyberspace via the metanetwork, it will become a battlespace and an arena for conflict. But will it be war?

Information Warfare—Is it "War"?

Perhaps a necessary starting point for this question is: what is war? Most members of the military and the national security community would have no difficulty recognizing Clausewitz's characterization of war as "an act of [physical] force . . . a pulsation of violence."[27] Too often, perhaps, the rest of the phrase, "to impose our will," is forgotten. The reason for the force and violence is the imposition of the will of one political entity onto another political entity. The issue at hand now is the potential ability of political actors to impose their will through informational means.

In the Clausewitzian paradigm, war was waged by a special class of actors, "warriors," on behalf of a special kind of political entity, "States." The warriors

were the uniformed military—soldiers, sailors, later airmen—and the States were the legitimate and recognized holders of international legal authority to engage in the force and violence of warfare. Almost at the same time (late 19th Century) as the Clausewitzian paradigm began rising to international prominence another force arrived on the scene, the international codification of legal norms for the conduct of war and the protection of certain classes of society. These norms, first enacted a century ago (1899) at The Hague, almost immediately encountered two extremely powerful forces: the nature of the modern industrial State and the influence of new technological means of warfighting.

The modern industrial State possessed an unprecedented amount of killing and dying power. Although this was clearly hinted at by the course of the American Civil War, the great European military powers failed to recognize it until too late.[28] The result was the stalemate and slaughter of The Great War and the Western Front, in which the amount of destructive force that the industrial State could generate was matched only by the amount of destructive force it could withstand. Twenty years later these same great powers demonstrated that their killing/dying power had actually increased, with the result that World War II's toll far exceeded that of World War I. This was made possible by the State's ability to employ and draw upon power sources that cut across almost the full breadth of society. These sources crossed the boundaries of what had been intended as sanctuaries and protected groups, such as undefended towns or noncombatants such as women. But did the concept of an undefended town mean anything useful in an era of nationwide air defense systems with flak belts and fighter patrols? Was "Rosie the Riveter" a protected person when she and her sisters left their homes to build U-boats or liberty ships?[29] It became increasingly obvious that the modern industrial State was a series of networks or infrastructures, and the American doctrine for strategic airpower in World War II was based on exploiting this fact. The "industrial web" theory of targeting, developed at the Air Corps Tactical School in the 1930s, came from precisely this paradigm and was based on the belief that if the critical nodes or "centers of gravity" (a 1990s adaptation of a Clausewitzian term) of an industrial State could be negated, the resulting stresses on the entire system would cause it to unravel like a spider's web whose critical connecting points have been cut.[30] The result of the interplay of these factors was a change in our paradigm of warfare, from the "limited" dynastic wars of the 19th Century to the "total" wars of survival—political, religious, racial, ideological—of the 20th Century.

A second critical factor was the development of new forms of warfare based on the exploitation of new forms of technology. The first great revolution in military affairs (RMA) of the last century was the adaptation of the internal

combustion engine to warfare, and by the end of the century's second decade warfare had become incredibly more complex than it had been in 1900 because it was now multidimensional. No longer was warfare waged on the surface. Now it went on below the ocean's surface and above both the sea and the land, and military success became increasingly dependent on the successful coordination of operations in all three dimensions. Thus, the invention and employment of the submarine and the airplane transformed warfare, a fact that was clearly visible during World War II in that no nation that failed to dominate all three environments was successful. To make the situation more complex, by 1945 it was clear that any force that was unable to operate in yet a 4th dimension—the electromagnetic spectrum, or what has here been defined as cyberspace—would have great difficulty operating successfully in any of the other three dimensions. This trend has continued and been intensified with military exploitation of yet another physical environment, outer space. The strategic and operational environment for warfare at the cusp of the new millennium now enfolds geospatial awareness, global connectivity, and a host of new factors that have further complicated the art of war. Not surprisingly, the legal context for conflict, which includes the law of war and the complex series of agreements and treaties that provide a framework for the affairs of State and conduct of statecraft, has been outpaced by the technologies available to global society. At the outset of the 20th Century, issues such as unrestricted submarine warfare and strategic bombing held promise of a disconnect between the law and war, while at its close other issues, such as netwar or the weaponization of space, hint at further uncertainty in how States and societies will attempt to regulate conflict. The same two forces that arose at the opening of the last century are still at work, with the notable difference that instead of the industrial age it is the information age that is changing the paradigm.

In some ways, the impact of the information revolution on warfare is quite apparent, and the application of advanced information technologies to traditional military capabilities and weapon systems—what could be termed information "in war"—serves to make "blast, heat, and fragmentation" work more efficiently and effectively. Information used as a weapon, tool, or even target is nothing new, even though the new technologies vastly increase its impact as an enabling capability or force multiplier. Sending target photos via secure fax from intelligence organizations in the United States to air campaign planners in NATO, thus enabling the destruction shortly afterwards of key Serbian infrastructure nodes via precision guided munitions, is an example of this fact. This exponential power as an enabler is an important, even vital aspect of what the Air Force calls "information in war,"[31] a critical foundation for information warfare,

but it is not synonymous with it. Information warfare is a new warform that is evolving from the synergistic effects of several new and unique factors, all part and parcel of the information revolution.

This brings us back, however, to the entering question: is this "war"? Does this fit with the Clausewitzian paradigm of force and violence? If a State is able to degrade an adversary's military capability, damage its key infrastructures, and inject great disorder into political systems or economic affairs, all without the use of kinetic force and violence, might not the recipient of such effects argue that they had indeed been "attacked" and were thus "at war" with the inflictor? During a recent exercise conducted annually at the Air Force Wargaming Institute by students from all of the DoD's senior military colleges, the "red team" developed a war plan against "blue" that included information warfare attacks against such targets as the air traffic control system, financial centers, energy distribution network, and telecommunications infrastructure, with the intent of degrading and disrupting blue's political will and strategic capability. The red team's objective was to seriously undermine the ability and will of both blue and its allies to continue armed opposition to red's other operations. This exercise in information warfare—which the students named "Dangerous Opportunity"—might be seen as a mirror-imaging of American attitudes and mindsets, but it also reflects technological conditions and vulnerabilities that the information environment may make available in any future conflict. It also closely tracks with recent publications by some senior Chinese officers, who postulated precisely such operations in their concept for "Unrestricted Warfare."[32] But does this perspective reflect any sort of consensus on what IW and IO are?

Perspectives and Doctrines

Earlier it was pointed out that the terminology of IW and IO are still evolving; not surprisingly, so are the various operational and doctrinal concepts held by the different organizations involved in the IW/IO effort, both in the United States and globally. It is worth some time to briefly explore some of these doctrinal and operational concepts. In the American military much of the future direction for IW/IO will come from "Joint Vision 2010," published by the Joint Staff in 1996, amplified in 1997 by "Expanding Joint Vision 2010: Concept for Joint Warfare," and further amplified by "JV 2020" in the summer of 2000.[33] JV2010, as it is called, postulated several dynamic changes in the overall strategic environment and the emergence of new operational concepts. A key hypothesis of JV2010 is that dramatic changes in new information technologies will make attaining and maintaining information superiority a critical requirement.

Concepts such as Dominant Battlespace Awareness or Network Centric Warfare are based on the assumption that new information technologies will enable US forces to develop and exploit networks of sensors, decision-makers, and shooters that can operate far faster than their adversaries, and thus translate information superiority into actual combat power.[34]

If the technologies of the information revolution are creating an information-based RMA, it remains for the American military to bring this to fruition by creating organizations, doctrines, and operational concepts to exploit technological advantages, and turn them into actual military capability.[35] In 1998 the Joint Staff finally published Joint Publication 3-13, Joint Doctrine for Information Operations. Like any such publication, it represents what all of the various coordinating parties could agree on, including the four military services. It is not a visionary document with radical new operational concepts, but it does emphasize that IO is not a technical capability, but rather a coordinating strategy for operations in the information environment, and it makes three critical points. First, joint forces at all levels must organize to conduct IO, and every one of the combatant commands, such as European or Central Command, have created full-time planning cells for IO. Next, the IO planning process must begin long before operations begin; it is too late to begin planning just a few days before the operation's scheduled initiation. Finally, joint forces must train and exercise in an information-intensive environment and engage all of the applicable organizations, including perhaps private sector or combined-multinational entities.

All US services—Army, Navy, Marine Corps, and Air Force—have approached IW/IO somewhat differently, viewing them through their individual warfighting lenses. The Army was the first service to publish specific doctrine for IO, and Field Manual 100-6, published in 1996, contained eloquent language about the "global information environment [and] battlespace," as mentioned earlier. But the doctrine's perspective was clearly on the need to "integrate all aspects of information to support and enhance the elements of combat power," those being the rather traditional: infantry, armor, artillery, and, to a lesser extent, airpower delivered via rotary-winged helicopters. The Army has chartered an organization, the Land Information Warfare Activity (LIWA) at Fort Belvoir, Virginia, to develop both concepts and capabilities for IO, and LIWA personnel have been active in the Balkans for much of the 1990s, assisting Army IO efforts there. The Navy views IO as something that enables fleet operations and makes those operations more efficient and effective. The Navy's perspective on IO also reflects the expertise and experiences of several of its different "communities," with two in particular, space/electronic warfare and cryptology, as having special interest and impact on IO. The Navy has two

key organizations, the Fleet Information Warfare Center (FIWC) at Little Creek, Virginia, and the Naval Information Warfare Agency (NIWA) at Fort Meade, Maryland, dedicated to its efforts to develop IO. While the Marine Corps does not have a specific IO doctrine or organization, it sees IO as larger than merely another weapon or tool to be used when appropriate, as something that makes the entire range of Marine Corps capabilities and operations more efficient and effective. Finally, the Air Force has perhaps the most visionary approach to IO, with several doctrinal publications that explicitly focus on the information realm as an arena for combat and as an operational environment in which operations needed to be coordinated with and integrated into those in the air and outer space. It, too, has made organizational changes, and was the first service to dedicate an organization to the effort, recasting the existing USAF Electronic Warfare Center into the Air Force Information Warfare Center (AFIWC) in 1993.[36] None of these approaches are "right" or "wrong," but they do reflect the perspectives of warfare and warfighting held by their originating services. While some will see narrow parochialisms at work here, it would be more optimistic to think that from these differing perspectives will come a more robust, richer and more comprehensive concept for IW and IO than we have at present.[37]

In a simpler time, "joint" would have meant the four services acting in unison, but that is insufficient for effective IO. Not only are there a range of non-service DoD organizations that are critical to the military's ability to wage IW, using the previously-cited definition of IO means that virtually the entire apparatus of the federal government is involved in some way with the national security exercise of information power. While perhaps only a handful of federal organizations would be involved with CNA, others would be involved with CNE, and virtually every one with CND, because in the information age every organization is increasingly dependent on its electronic and computerized information networks for its efficient functioning. One of the most critical, if little-noticed, segments of PDD 63 was the tasking of each federal department or agency's chief information officer (CIO) with the responsibility for information assurance within that organization. This ties into another of PDD 63's critical actions, the assignment of specific segments of the government to work with their private sector counterparts (Department of Energy with the electric industry, for example) in developing the strategic partnership called for in the document. The latest National Security Strategy (December 2000) contains repeated references to the critical importance of safeguarding national infrastructures from intrusion or attack, whether that attack comes from the physical world or via CNA.

While some feel that the US military's interest in IW and IO is a reflection of a peculiar American affinity for technology and the degree in which information technology is embedded within our systems and structures, the growing interest of the rest of the world indicates that IW/IO is not solely an American issue. While this is neither the time nor place to make a detailed exploration of non-US perspectives on IW/IO, a few examples are in order. The British military has been pressing ahead both operationally and educationally, as have most of our other English-speaking allies, and their interest has included the pressing need to provide CND to counter the threat of CNA against vulnerable infrastructures.[38] Several other governments, including that of Norway, have undertaken specific PCCIP-type studies of their own national infrastructures because of the growing awareness that national security, including economic health and prosperity, depends on the smooth and confident functioning of these computer networks. The Swedish National Defense College (Forsvarshogskolan) has integrated IO into the core of its curricula, and the other Scandinavian countries are following suit. The Russian and Chinese perspectives have already been cited, albeit too briefly, and the views of one senior Indian national security strategist are enlightening. Major General Yashwant Deva recently wrote that the "metaterritorial" nature of IW was blurring the boundary between peace and war, and he argued that India's national security strategy must have an information strategy component to be effective.[39] These are perceptive insights from a country possessing the world largest "Silicon Valley" and one which is a global leader in information technology. Finally, the rapidly increasing use of cyberspace and computer networks for political objectives by nongovernmental organizations, whether they be humanitarian groups such as the Red Cross, political and environmental activists such as Greenpeace, or revolutionary groups such as the Tamil Eelam (Sri Lanka), Zapatistas (Mexico), or Hezbollah (Middle East), poses an interesting problem for governments and supra-national organizations that are uncomfortable working outside of the traditional and terrestrial boundaries of national security. In cyberspace all actors look somewhat alike, and as some recent incidents such as the Solar Sunrise case have illustrated, it can be very difficult to determine if the intruder is a lone individual or the agent of a State acting for State-sponsored purposes.

Concluding Thoughts

Those old enough to remember sayings and slang from the war in Southeast Asia may recall one that went "When you're up to your backside in alligators, it's kind of hard to remember that your initial mission was to drain the swamp."

Right now, in the field of information warfare, we are hip-deep in the swamp of unresolved issues, and there are a number of alligators circling. At the outset of this discussion we faced the Clausewitzian paradigm of warfare, which was based in part on the concept that wars are waged by "warriors" in service of identifiable States. In a postulated paradigm of war by keystroke, are those that operate from the keyboards to be considered "warriors?" We have seen examples in which young hackers, skilled at moving from database to database via cyberspace, never physically leaving their keyboards, have been inducted into the armed forces of their home countries.[40] Could this be used to provide a cadre of super-skilled operators who now have the technology of States at their fingertips, instead of what they can afford from Radio Shack? One thinks of the case of the Dutch hackers who vainly offered their services to Saddam Hussein during the Persian Gulf War. Could such individuals, if acting in the interests and behalf of a State, be considered cybermercenaries?[41] Equally plausible is the potential for them to act on behalf, not of a recognized State, but of some other interest group, whether it have political, religious, or even simply monetary motivations.

Our existing paradigm for war requires kinetic actions, destroying things, or crossing physical boundaries with physical objects such as airplanes or tanks. What are the political and legal regimes for actions that do not cross the physical limits of territorial sovereignty or cause kinetic destruction, but still have serious impact on the national security of the "attacked" State? Where are the lines of sovereignty in cyberspace, and how does the State respond to the provocations and intrusions of what may be a shadowy and virtual opponent? More and more of the key infrastructures that support civil society also support, in a strategic sense, the military power and capability of the State. Electric grids, oil and gas pipelines, transportation networks, and telecommunications are just some of those dual-use infrastructures and architectures that support both civil society and military strength. Those kinds of assets have been attacked and destroyed in wartime before, and they will be again, but what is the impact if the means of negation comes across the Internet in the forms of bits and bytes? Just as troubling is the question of who can and should defend those infrastructures? National armed forces protect them against attack by "traditional" military means, but does this mission extend into cyberspace? In the United States the answer from PDD 63 seems to be that this is a shared public sector-private sector responsibility that will require the coordination and cooperation of those communities to solve the problem of infrastructure vulnerability, but this may not necessarily be the answer in other countries that have different political-economic systems and traditions. These are just a sample of the questions and issues to be discussed and analyzed in the pages of this volume.

For more than a century and a half, from the era of Napoleon and Clausewitz, to that of strategic bombing and national liberation organizations, western political society has had a paradigm of warfare that has focused on the means employed: force and violence, employed to defeat or destroy the enemy's powers of physical resistance. Information "in war" is a continuation of this paradigm, and thus—as important as those capabilities are for the capability to employ traditional military force—is incomplete because of the new capabilities for influence, power, and the imposition of will offered by the new information technologies. Information warfare and information operations do not replace the older forms, but they do augment, modify, and change those forms. The difference between the terms is important, even vital, and we dare not ignore it, lest an adversary who lacks our bureaucratic and intellectual shackles and does not "understand our rules" use our very dependence on computer networks to administer a nasty strategic defeat via the very same environment and metanetwork we are so confidently constructing.

Notes

* The views expressed in this paper are those of the author and do not reflect the official policy or position of the National Defense University, the Department of Defense, or the United States Government

1. I am indebted to Lieutenant General Mike Hayden, Director of the National Security Agency—the DIRNSA—for this very descriptive phrase.

2. This author first met Dr. Rona and heard his concepts during a presentation on June 13, 1994, at the Information Resources Management College, National Defense University, in Washington DC. He defined IW as "*the sequence of actions undertaken by all sides in a conflict to destroy, degrade, and exploit the information systems of their adversaries. Conversely, information warfare also comprises all the actions aimed at protecting information systems against hostile attempts at destruction, degradation and exploitation. Information warfare actions take place in all phases of conflict evolution: peace, crisis, escalation, war, de-escalation and post conflict periods.*" Dr. Rona, a gentle man and brilliant analyst, unfortunately passed away in December 1997. For an example of his work, see Weapon Systems and Information War, a study prepared for Boeing in 1976.

3. This author vividly remembers the initial classroom meeting of the School of Information Warfare & Strategy's first group of students in August 1994, during which the sixteen students reacted with dismay to the plethora of official and unofficial definitions of information warfare. Some argue that any attempt to formally define IW is premature and counterproductive; others argue that some degree of consensus is essential, emphasizing that unless the different organizations that are involved in the issue have some common language and currency, any attempt to develop and execute plans and operations that not only span the entire government, but also involve the private sector and international community as well, are doomed to frustration and failure. While this author agrees that trying to put a "stone tablet on the wall" degree of finality on the terminology of IW is futile because the discipline is still evolving, some kind of terminological commonality is vital, even if it only provides a common target that all parties agree is "wrong."

4. While the Directive itself is classified Secret, this definition is unclassified.

5. One of the reasons for the creation of the term IO is the visceral dislike and mistrust of the word "war" by many of the agencies and people who are beginning to find that the information age envelops their activities and mission. Thus the creation of a term—IO—that points at the larger arena in which information activities are conducted, but does not tie those operations so visibly to the military and warfare.

6. See Chairman of the Joint Chiefs of Staff, Joint Publication 3-13, Joint Doctrine for Information Operations (1998), for these and other related definitions.

7. *See* Field Manual 100-6, Information Operations, (US Army Training and Doctrine Command, or TRADOC) (Aug. 1996); *see also* Air Force Doctrine Document 1, Air Force Basic Doctrine, (USAF Doctrine Center) at 31–32 (Sept. 1997); the Air Force's IO doctrine manual, AFDD 2-5, Information Operations (Oct. 1998).

8. *See* the author's Defining Information Power, Strategic Forum #115, Institute of National Strategic Studies, National Defense University, 1997, www.ndu.edu.

9. *See* National Security Decision Directive (NSDD) 130, US International Information Policy (March 6, 1984). The concept described above is based on NSDD 130, but paraphrases it and expands on some of its key components.

10. DANIEL R. HEADRICK, THE INVISIBLE WEAPON: TELECOMMUNICATIONS AND INTERNATIONAL POLITICS, 1851–1945, at 140–141 (1991). For Radio Free Europe's role, see Kevin J. McNamara, *Reaching Captive Minds with Radio*, ORBIS, Winter 1992, at 23–40; Walter Laqueur, *Save Public Diplomacy*, FOREIGN AFFAIRS, Sept.–Oct. 1994, at 24. For Russian views, see Tim Thomas, *Dialectical Versus Empirical Thinking: Ten Key Elements of the Russian Understanding of IO*, JOURNAL OF SLAVIC MILITARY AFFAIRS, March 1998 at 40–62.

11. While it is impossible to say when the term "cyberspace" was first used, several authors stand out as being among the leaders. William Gibson's classic work of science fiction, *Neuromancer* (1984), first raised the concept of humans seamlessly operating within a cybernetic, virtual-reality environment, while Nicholas Negroponte's book *Being Digital* (1995) is an exploration of the impact of cyberspace on our daily lives. The term itself has only recently come into widespread use. A search of several automated databases, for example, covering the years 1986–89 and 1986–91 contained only 17 "hits" on the term!

12. Of course, outer space can be measured in a scientific sense, but not in terms which are useful in a lay sense.

13. The question of where the borders of cyberspace lay is an intriguing one. Michael Benedikt has written perceptively on it in his book *Cyberspace: First Steps* (1991), while the late Anne Wells Branscomb in a recent monograph, Cybercommunities and Cybercommerce: Can We Learn to Cope? (Harvard University, Program on Information Resources Policy), suggested that the borders of cyberspace are discernible at the interconnection points between segments of the Internet, with network managers and systems administrators acting as the border guards, in a sense.

14. This construct omits communication methods such as signal flags, smoke signals, drums, or even heliograph because they did not require manipulation of the electronic environment.

15. THOMAS KUHN, THE STRUCTURE OF SCIENTIFIC REVOLUTIONS (1970).

16. This warning system used Air Force Space Command's space-based platforms to note Iraqi Scud missile launches; US Space Command to assess the indications; and Patriot missile systems operated by US Central and European Commands to engage the Scuds. This system thus crossed several physical boundaries (outer space, several oceans, the atmosphere, and cyberspace), national boundaries (the United States, Israel, and Saudi Arabia, at a minimum), and organizational boundaries (one service major command and at least three joint Unified Commands), all at the speed of light. This example illustrates a few of the capabilities, opportunities, and difficulties of warfare in the information age.

17. JV2010 is available electronically at www.dtic.mil/jv2010/.

18. This runs into the strawman view that since only a small minority of the world's population currently has immediate access to the Internet it is unimportant. One counter to this is that in 1776 only a certain segment of the American population supported the American Revolution, or could even read the Declaration of Independence, yet who would argue that document's political significance?

19. CJCSI 6510.1, Defensive Information Warfare Implementation (May 31, 1996).

20. Richard S. Berardino, SCADA and Related Systems: Critical and Vulnerable Elements of Domestic Components of National and Economic Security, unpublished research paper on file with author at National Defense University.

21. See the *Washington Post*, Feb. 24, 1996, at 4, for a detailed analysis of the accident.

22. For the PCCIP, see the Commission's report, Critical Foundations: Protecting America's Infrastructures, which at the time of this writing is electronically available via the website of the Commission's follow-on organization, the Critical Infrastructure Assurance Office, or CIAO, www.ciao.gov. The concept of "infrastructural warfare" has even generated an electronic journal, *The Journal of Infrastructural Warfare*, www.iwar.org.

23. *See also* Office of the General Counsel, Department of Defense, An Assessment of International Legal Issues in Information Operations (Nov. 1999). The paper is appended to this volume as the Appendix.

24. Two recent and very good examples of this are DOROTHY DENNING, INFORMATION WARFARE AND SECURITY (1998) and EDWARD WALTZ, INFORMATION WARFARE: PRINCIPLES AND OPERATIONS (1998).

25. *See* Lisa Hoffman, *US Opened Cyber-War During Kosovo Fight*, WASHINGTON TIMES, Oct. 24, 1999; Frederick H. Levien, *Kosovo: an IW Report Card*, JOURNAL OF ELECTRONIC DEFENSE (Sept. 1999), www.jedonline.com.

26. A lengthy and growing bibliography exists on the subject of infrastructure vulnerability. A recent contribution from the Center for Strategic and International Security (CSIS) is CYBERCRIME . . . CYBERTERRORISM . . . CYBERWARFARE . . . AVERTING AN ELECTRONIC WATERLOO (1999); a growing number of official studies and reports echo this theme, including several from the General Accounting Office, as well as congressional hearings. *See, e.g.*, Security in Cyberspace: Hearings Before the Permanent Subcommittee on Investigations of the Committee on Governmental Affairs, US Senate, 104th Congress, May 22–July 16, 1996.

27. See CARL VON CLAUSEWITZ, ON WAR, Bk. 1, Ch. 1, for his complete analysis of these relationships.

28. See JAY LUVAAS, THE MILITARY LEGACY OF THE CIVIL WAR: THE EUROPEAN INHERITANCE (University of Kansas Press, 1988; originally University of Chicago Press, 1959) for the best discussion of how the European powers essentially ignored the lessons of the war of 1861–1865.

29. Actually, "Rosie" only built Liberty ships, not U-boats; one of the signal failures of the Nazi regime was its reluctance to significantly tap into this source of labor, one that the democracies fully exploited.

30. For a good discussion of this, see ED MANN, THUNDER AND LIGHTNING: DESERT STORM AND THE AIRPOWER DEBATES (1995).

31. For a discussion of the Air Force's doctrinal distinction between "information warfare" and "information in warfare," see Air Force Doctrine Document (AFDD) 2-5, Information Operations (1998).

32. *See China's Military Plots 'Dirty War' Against the West*, LONDON SUNDAY TELEGRAPH, Oct. 17, 1999; *see also* the longer explanation in the Foreign Broadcast Information Service translation from HONG KONG TA KUNG PAO, Sept. 19, 1999.

33. See the JV2010 website, *supra* note 17.

34. *See* DOMINANT BATTLESPACE KNOWLEDGE (Stuart J. Johnson & Martin C. Libicki, eds., 1995); DAVID S. ALBERTS, JOHN J. GARSTKA, & FREDERICK P. STEIN, NETWORK CENTRIC WARFARE: DEVELOPING AND LEVERAGING INFORMATION SUPERIORITY (1999). Both are available electronically via the DODCCRP website at www.dodccrp.org. The latter book is an expansion of the concept first promulgated by Admiral Arthur K. Cebrowski in *Network Centric Warfare*, US NAVAL INSTITUTE PROCEEDINGS, (Jan. 1998), at 28–35, www.usni.org.

35. For a fuller discussion of this, see the compilation of RMA-related articles in the Summer 1998 issue of JOINT FORCE QUARTERLY, www.dtic.mil/doctrine.

36. *See* Field Manual 100-6, Information Operations (1996); Chief of Naval Operations Publication, Navy Information Warfare Strategic Plan (1998); Major General J.E. Rhodes, *A Concept for Information Operations*, MARINE CORPS GAZETTE (Aug. 1998); USAF Doctrine Documents (AFDD) 1 and 2-5 (1997 and 1998 respectively). The USAF renamed the AFIWC as the AF Information Operations Center (AFIOC) in 2001.

37. See the author's Joint Information Warfare: a Paradigm for Information-Age Jointness, Strategic Forum #105, Institute of National Strategic Studies, National Defense University, March 1997, www.ndu.edu.

38. *See, e.g.*, Adam Cobb, Thinking About the Unthinkable: Australian Vulnerabilities to High-Tech Risks, Research Paper #18, 1997–98, Department of the [Australian] Parliamentary Library, Canberra, Australia, June 29, 1998.

39. Yashwant Deva, *National Perspective on Information War*, JOURNAL OF THE UNITED SERVICE INSTITUTION OF INDIA, Jan.– March 1998.

40. It is interesting that young Ehud Tenenbaum, the "Analyzer" from 1998's well-known Solar Sunrise incident, was called up for military service in the Israeli Defense Forces shortly afterwards. What service he is performing for the IDF is not known.

41. Only relatively recently in history have mercenaries acquired the general approbation which they now enjoy. After all, the first great victory of the American Continental Army, the day after Christmas, 1776, was at the Battle of Trenton. Washington's opponent: the Hessians, hired by the British crown.

V

International Law, Cybernetics, and Cyberspace*

Anthony D'Amato

My pleasant assignment this morning is to talk about the future of computer network attack under international law. Any prediction is difficult to make, but the hardest thing of all to predict is the future. If I wanted to play it safe I would just stand here and be quiet for thirty minutes. Yet we all know that if there is one prediction that can be asserted with a confidence level of 100%, it is—no matter what the topic might be—any law professor in this country who is given the job of talking about it will talk about it.

There has already been a lot of talk this week about rules of international law, and I sense a certain amount of discomfort about the old, received rules of international law. We have been cited rules dating from 1949, 1945, 1929, and back as far as 1907 and 1899. Somehow they seem archaic when compared with a revolutionary new technology. Professor Yoram Dinstein has advised the convening of an international conference to update the old humanitarian rules of warfare. But pending the replacement of existing rules by new ones, Professor Dinstein contends that the existing rules will serve us well enough if we apply them as written. He appears to view these rules as a kind of international

* Address delivered at the Symposium on Computer Network "Attack" and International Law, Naval War College, June 1999.

legislation. I do not completely share that point of view. Perhaps this betrays my common law bias, but I think there is a kind of spirit of international law that shapes the rules on the books and provides a basis for interpreting them.

This spirit is evolutionary. Being aware of it gives us a basis for predicting how the rules of international law may bend and change to fit new situations. Since any international crisis will appear quite different to decision-makers on the inside than all the previous ones they have experienced, simulated or studied, it is indeed a kind of rigid thinking to say we should treat this crisis by applying the same rules we applied to the last one. It would be somewhat like accusing generals of fighting the previous war. But rules of law are like that; as words on a paper or on a screen, they do not change by themselves, they stay the same. And they were obviously fashioned to cover past situations. Thus, I argue that we cannot take our stand solely upon the rules of international law as written. These rules have to be interpreted in light of new circumstances.

And yet it is clear that if we simply change the old rules to apply to new situations, the rules will be sapped of all their vitality. There is no use having any rules of law at all if they can be changed at will; that would amount to anarchy. Therefore, I want to argue that we are constrained in the degree of latitude that we can give to the interpretation of old rules to fit new situations. And this constraint comes, I argue, from a good faith appreciation of the structure of international law itself.

What is the structure of international law? We begin by recognizing that it is, and must be, a self-perpetuating coherent set of rules that operate within the arena of international relations. Because it is dependent upon a multi-State environment for its own existence, international law consists of rules that are designed to maintain the peace and stability of those States, for total anarchic war is the absence of rules. International law opts for stability by ensuring that its rules minimize the friction among States and provide for peaceful resolution of disputes. If war breaks out despite its rules, then international law attempts to contain the war, minimize the damage caused by war, and provide for a secure peace following the war. An example of a set of international legal rules providing for the containment of war are the complex and realistic rules of neutrality, fashioned over centuries, which specify the acts that neutral nations may or may not take during a war in order to maintain their neutrality. And a classic example of a rule favoring an agreement to stop the war is the rule that treaties of peace are valid even though the losing side could be said to have been coerced into signing the treaty by the threat of continued war if it did not sign.

Although the content of the rules of international law has not changed qualitatively over the course of the past five thousand years, existing rules have been

adjusted and modified to meet new situations and contingencies. This adjustment operates through an elaborate system of customary law that modifies rules in light of feedback mechanisms. These mechanisms include courts, foreign offices interacting with each other (the "*dedoublement fonctionnel*"), diplomatic communications, international legal conferences and codification conventions, negotiations of bilateral and multilateral treaties, and so forth. International law is, in brief, a cybernetic system. Its rules are useful only if they are functional—that is, only if they promote the stability of the system. The feedback mechanisms, which are the hallmark of cybernetic systems, continuously measure whether rules of the system operate to resolve disputes rather than aggravate them. If a rule has a tendency to aggravate disputes, then it is reinterpreted, modified, or in drastic cases overruled and replaced by a rule that stabilizes the system.

It follows that too rigid an interpretation of any given rule could lead to a rupture in the system. Let me call an absolutely rigid interpretation a "robotic" interpretation. A robot will interpret a rule exactly, without taking into account its real-world consequences.[1] For example, the Standing Rules of Engagement for US Forces of October 1, 1994, provides in its first rule that a military commander has the right to use all necessary means to defend the military unit, and that none of the remaining rules in the ROE can limit this inherent right. If a robot were programmed with this rule alone, it would not hesitate to employ a hugely disproportionate weapon in the defense of its unit, including a nuclear missile that could start a global conflagration. Thus, the first rule of the ROE cannot be given a robotic interpretation. The rule is instead directed to a commander who is familiar with many other rules within the ROE, with the requirements of warfare, and with the general principle of military proportionality. In short, the rule on the books was made by humans with the often unarticulated premise that humans like them would interpret the rule. A military rule presupposes a military interpreter.[2]

Sometimes the laws of war build terminological flexibility right into their own language. Many of the older rules of warfare, for example, prohibit acts that are "not justified by military necessity." Such rules also betoken the good military judgment of a human being. Legal restraints on warmaking stem from the need to keep the international system stable. Many years ago Quincy Wright put this another way: the goal of the military during a war is not just to win the war but to win the subsequent peace. If force is used that is not justified by military necessity, the seeds will be sown of future revenge; hence, a stable peace may not have been secured. "Military necessity" should be construed as "necessary to win the engagement at hand" and not to demonstrate brutality by unrestrained killing of enemy civilians.

The cybernetic system of international law is thus a purposive system. Its rules cannot be interpreted literally or applied mechanically because each rule is simply an indication of how the system should deal with disruptions that may arise. Our bodies are purposive systems; if surgery is needed to remove a tumor, the surgeon operates with as little damage to the surrounding tissue as possible, for obviously the idea is to remove the tumor and not to kill the patient. A ship is an example of a self-contained purposive system. The primary purpose of a purposive system is survival—persistence through time.

In order to survive, purposive systems attempt to maintain systemic equilibrium. When our bodies are invaded by a flu virus, our temperature rises so as to provide a hostile environment for the invaders; when the virus is defeated, our temperatures return to normal. Similar servomechanisms exist on larger military vessels; a torpedo hit on the hull may trigger an automatic seal-off of the compartment that is being flooded. A thermostat is one of the simplest servomechanisms; there are many more we can think of.

Purposive systems are able to survive and to reverse disequilibrating interruptions because they have elaborate internal communications systems. We do not have to tell our bodies to raise our temperature; our blood stream carries the message of outside virus invaders to our central nervous subsystem which communicates with the subconscious parts of our brains and in effect turns up the heat. On board a ship, the internal communications are elaborate and highly structured to carry messages of the ship's condition to all hands. There are fail-safe mechanisms that operate by default in case the intra-human messages are disrupted.

he communications on board a ship are structured by elaborate rules, jurisdictional assignments, protocols, and regulations. These constitute the internal laws of the system. Any person on board who acts in a way that jeopardizes the survival of the ship is immediately arrested; any person who acts to upset the equilibrium of the ship is also stopped. All the everyday rules and regulations of the ship are designed to actualize the two primary goals of persistence through time and the maintenance of systemic equilibrium.

Just as a ship's rules are designed to maintain the integrity of the floating military unit, the rules of international law are designed to maintain the integrity and peace of the States of the world in their international relations. The essence of all these rules is the communication of information. Naval rules are worthless unless communicated. The equilibrium of our bodies is maintained by an elaborate system of neuron communications into and out of the brain and spinal column.

My thesis is based upon the signal importance of the communicative aspect of rules. Without communication the rules do not work. And if the rules do not work, the entire system can break down, with adverse consequences to everyone.

The importance of communication in international law is illustrated by one of its most ancient rules: the personal immunity of diplomats and ambassadors. Even during wartime nations realized the importance of keeping open the channels of communication with their enemies. Diplomatic immunity under international law is well known. The relation to Internet communications is obvious. I would like to discuss a more subtle and perhaps more illuminating practice allowed by international law that also has a long history—letters of marque and reprisal.

Back in the days when there were no international courts, no international peacekeeping organizations, and nations did their best to avoid war because of the unforeseeable calamities that war could bring, a curious practice of a kind of limited private law arose. Key to this practice is what might be termed "unilateral communication." A message is sent out that is intended to be received, but a response is not required. The message is contained in a letter of marque and reprisal.

To envisage the situation, imagine five hundred years ago that merchant M in nation A was one of a class of rich international traders, importing and exporting goods. In the course of his trade, M sends a caravan of silks, which he purchased in A, into nation B to be sold. With the selling price (in B's currency, of course), M intends to buy goods in B that are relatively scarce back in A, and transport those goods back to A to be sold there. In every transaction, as usual, M takes a percentage for himself. M and his fellow merchants are very important to the king of A because taxes on their profits are the king's primary source of revenue.

Now let us assume that a greedy provincial governor in B, seeing the large amount of money that M has obtained by selling the silks in his province, decides to levy a 100% tax on the money that M's trading activities in B have amassed. M's employees in B are simply merchants; they do not have the power to resist the provincial governor. As a result, their capital as well as their profits are confiscated and they return to A empty-handed.

An outraged M reports to the king of A the "denial of justice" within B. But the king does not want to start a war against nation B. There are too many risks and uncertainties in war, and, in addition, the king simply cannot afford to finance an all-out war. True, the king admits, the queen of B does not want war either, and for the same reasons. But once a war between two sovereign nations is started, who knows what the result will be?

So we assume that at that point, M offers to mount a private mercenary attack against B. In that way, by looting and pillaging, M can get his money back while teaching B a lesson. Such an action would probably drive the king into an unwanted war. And the king may not be quite powerful enough to stop M from doing it, especially if M recruits his fellow tradesmen to help in the enterprise.

Thus the stage is set for a deal between the king and M. The king wants M to go ahead but in a limited way, one that would be sufficiently justified so that the queen of B would not feel honor-bound to go to war to resist it. The only thing that would be so justified would be what Aristotle called compensatory justice. M should have the right to be compensated for his losses plus the cost of obtaining that compensation. So the king issues to M a letter of reprisal. The letter contains the terms of M's planned expedition into nation B. It specifies the geographical limitation of the expedition—in this case, the particular province whose governor took away M's assets and profits. It specifies the amount that can be recovered—in this case, property and other valuables equal in amount to M's losses plus interest plus the cost of paying the mercenaries. It specifies the persons against whom the losses can be recovered—in this case, probably, all officials and all private citizens in the province, perhaps with officials coming first. The fact that innocent civilians are going to be robbed to pay for M's losses is unavoidable. In principle, they should seek recompense from the queen of B, who should levy against the governor of the province and who, in the future, should ensure that none of his subordinates mistreat foreign traders in this fashion.

M's motivation in obtaining the letter of reprisal is not so much so that he can show it to officials (or the queen) in B during his mercenary expedition there, but rather to legitimize his expedition in his home country A. After all, if M proceeds without the king's approval, he might eventually return to A only to face arrest for his private breach of the peace. Moreover, M's ability to recruit mercenaries within A will be greatly facilitated by the legitimacy of the letter of reprisal; otherwise, a potential recruit would reasonably worry about arrest in A when the expedition is completed. Therefore, as I have said, the letter is just a one-way communication within nation A. It is not necessary for the queen of B to read it; its "power" is exhausted once M receives it from the king of A. But if M respects the conditions of his reprisal raid into B, then the queen of B can see, by the results, that M confined himself to the province of which he complained that his assets were confiscated by the governor, and that M helped himself to compensatory justice.

In this fashion, many limited wars were fought under the aegis of letters of marque and reprisal. Sometimes the mere issuance of such letters was enough to provoke the monarchs of neighboring countries to offer restitution in order to avoid the impending mercenary raid into their territory. And naturally, over the course of time, the conditions for the issuance of letters of marque and reprisal were spelled out in treaties of peace. The Treaty of Westphalia recognizes the potential legitimacy of limited armed attacks as reprisals for denial of justice. Farther along in time, reprisal raids were replaced by judicial procedures. By the

1920s, for example, the United States and Mexico set up a Joint Arbitration Tribunal which settled all outstanding claims between American citizens against Mexico on the one hand, and Mexican citizens against the United States on the other. Since payments to the aggrieved plaintiffs were secured by net-net transactions between the two governments, only the monetary difference at the very end had to be paid in specie.

This subsequent history shows that the early letters of marque and reprisal,[3] by allowing limited war, operated as a deterrence to general war. When people are robbed, they need restitution. When they are robbed by another country, the alternative is either war or self-help. The history of the use of letters of marque and reprisal constitutes an example of my general point that even a war can be, in some circumstances, not systemically disequilibrating, but rather a method of preserving and restoring systemic equilibrium. If all wars in the future are intended to be limited wars (we can hardly contemplate a world war in this era of weapons of mass destruction, though we must be ever vigilant that it will not erupt by accident), then we need to be very careful about preserving the communications network that in the past has been instrumental in keeping wars limited.

Thus, I contend that the main lesson for present purposes of this short history of letters of marque and reprisal is the importance of communication—both internally and externally—as a means of limiting warfare. In considering the escalatory potential of destroying computer Internet traffic in future conflicts, we should not just look at the disruption of communications with the enemy, but also consider the severe negative consequences to ourselves if the disruption cannot be pinpointed and spreads to affect the network in its entirety. For although a letter of marque and reprisal signified an agreement between the sovereign and one of his subjects (the king of A and his subject M in my example), it was also meant as a communication to a foreign country (to the queen of B, in my example). While it was desirable that the foreign sovereign read the letter, it was not necessary. Many communications today are of this one-way type. In the recent NATO bombing of Yugoslavia, for example, NATO leaders held numerous press conferences which they were confident were being monitored by Milosevic and others in Belgrade. Limited-war aims must be communicated to the enemy whenever possible. They must be credible (as, indeed, were the letters of marque and reprisal, which were not casually issued by any means). And they must be continuously communicated, for when the enemy is suffering its darkest days it must be fortified by the belief that its leadership continues to hold the key to armistice and a peaceful settlement.[4]

Of course, no one can foresee what will cause future wars to break out, but among the causes that have led to wars has been the need to protect by armed force the lives of innocent persons in foreign countries. When those innocent lives were a country's own citizens, then intervention to protect them has been a common *casus belli* for several centuries. Only recently has intervention extended from nationals to non-nationals. As I contended in an article in 1982, intervention of the latter type is designed to protect our "internationals."[5] Our internationals are people everywhere, with whom we share a mutual commitment of protection under the developing international law of human rights.

Once any war has begun, the international system tries to bring the system back to equilibrium. Thus, we have in international law the phenomenon of the humanitarian laws of war. Occasionally I have had the feeling during this conference that some military planners and targeters appear to believe that the laws of war are an evil imposed by the lawyers and politicians, and that their job is to adhere to the letter of the rules while violating the spirit. They seem to say that the most important goal in war is to win it as soon as possible—and indeed there is a logic to that position. Ending a war quickly will often save many lives. The problem is that nations that get an upper hand during a war often convince themselves that the quickest way to end the war is to terrorize the enemy's civilian population. I think that General Curtis LeMay's terror bombings of Tokyo suburbs in the spring of 1945 were well-intentioned in this regard. Nevertheless, those raids constitute, for me, the clearest example of a war crime in the entire Second World War. What did the bombing "communicate" to the people of Japan? That they should surrender unconditionally to an enemy who was ruthless enough to drop flaming napalm on women and children living in wooden homes? If LeMay believed he was saying, "Surrender now and we won't keep on doing this," he may in fact have communicated "Better to die than surrender to the devil incarnate." What the humanitarian laws of war do is to take this kind of calculation away from those who would emulate General LeMay. The laws of war prohibit the deliberate targeting of civilians. I think in the judgment of most observers, military and civilian, the exercise of this kind of restraint during a war is more likely to lead to a quick peace and, similarly, to a lasting peace.

Moreover, from the international systemic viewpoint, given the fact that war itself may be a necessary equilibrating adjustment to preserve deeper systemic values, prolonging a war is not necessarily a bad thing. It may be important for systemic value preservation to prosecute the war the right way even if doing so prolongs the war. This is perhaps a deeper reason for ruling out the deliberate terror bombing of civilians.

But the viewpoint of the international system is not the only possible viewpoint. You can obtain the same result from the point of view of a nation looking outward at the international system. For if the maintenance of the system is necessary for lasting peace and order, then each nation partakes of that systemic goal in its own foreign policy. The systemic viewpoint is primarily a useful heuristic that enables us to predict the ways in which the system itself strives to maintain its equilibrium. Once we have identified the ways, each country's national interest is served in facilitating them.

I have mentioned so far the rules of diplomatic immunity and the history of letters of marque and reprisal as two of the ways that the international system recognizes disruptions to the system and is able to communicate effectively to restore equilibrium. A third mechanism is that customary international law permits espionage. Although each nation may punish spies, they are often exchanged for a nation's own spies who have been caught by the exchanging country. It would have been easy for international law to have generated a rule prohibiting espionage, but the fact that it allows for espionage is a further strong affirmation of the importance of the exchange of information. There have been many instances in which a nation's military posture appeared bellicose to a neighbor, yet intelligence networks exposed the reality that there was no bellicose intention. Without that information, the neighboring country might have launched a preemptive attack, starting a war by mistake. Even when a nation is attempting to start a war against its neighbor, the international system is well served by intelligence information that allows the neighbor to get prepared for an attack. Preparation often dissuades the attacker from going ahead. None of this is to say that the exchange of information prevents all wars from breaking out. But it has stopped some wars that would have been the result of a mutual mistake, and it has served to limit wars that have already broken out by conveying information as to military intentions.

In recent years observers have been somewhat surprised by the slow and deliberate way the Security Council has conveyed to countries such as Iraq and Yugoslavia the intentions of the major powers if those countries did not cease and desist their unlawful acts. The clarity of communications is probably responsible for a greater reduction in casualties than would have occurred if the UN's motives and intentions had been kept secret.

Where do these arguments lead, in terms of international law? They lead me to predict that attacks on the Internet will soon be seen as clearly illegal under international law. Maybe customary international law has already reached that position. No matter what short-term military advantage might be seen in disrupting another country's Internet system, the disruption may spread to the

point where it is totally counterproductive. But even if it can be kept contained within the target State, it nevertheless violates, in my view, the international system's attempt to end the war and win the peace. In a sense—although I do not want to be taken literally on this—disrupting the Internet is like unleashing biological warfare: the limits are unpredictable and the method is inhumane. What is inhumane about disrupting a target State's Internet communications is that it deprives innocent people within that target State from the only possibly effective means they have of obtaining external information and using it to communicate with each other, possibly to oppose the war from within. In the recent NATO attack on Belgrade, some citizens of that city were able to obtain news of the war from nongovernmental sources.[6] Unfortunately NATO targeted some of the Belgradian communications facilities. I think that was a mistake; it set a precedent that could backfire and it did not noticeably shorten the war.[7] Whether that targeting was illegal is not a question that will be addressed in any foreseeable forum. But I believe that informed international legal opinion will in the near future weigh in on the side of the illegality of attacks against the Internet.

I believe this because the stability of the international system is dependent upon the free and efficient flow of information within and among the units that make up the system. The more freedom of international communication we have, the less the likelihood of war and other disruptions to the stability of the international system. The global Internet, with its already achieved interconnectivity across national boundaries, is a natural heir to the rules of diplomatic immunity, letters of marque and reprisal, legality of espionage and intelligence-gathering, and many other communicative aspects of international law.

I am not claiming that during a war there would be a prohibition against disrupting the enemy's command-and-control communications system. If that system is separate from the Internet, it is fair game as it always has been. However, if the enemy is instead using the Internet itself for its military command and control system, then why disrupt it when a better alternative is to break through its code? Of course, in an actual conflict the military commander on the ground will decide whether such an alternative is better. That is why I am making the stronger point that a rule of absolute prohibition of Internet disruption is in the best interests of both sides in the long run and therefore is likely to be soon recognized as a foundational principle of international customary law.[8]

Finally, I predict that in the near future we will see massive public support throughout the world for the inviolability of the Internet. Although a very recent phenomenon, the Internet in my view is securing for itself a place in public consciousness that will be impossible to dislodge. Indeed, the Internet has

become one of our vital national interests. It will be something we will have to protect in the event of a war. It is not just a mechanism like previous communications systems (the telephone, the radio, and television). Instead, it has fostered a new kind of community awareness and empowerment.

I hope it does not sound too much like science fiction to say that some people already are living in virtual communities. Their chat room partners come from all over the world, people who share similar interests. We will see an increasingly specialized and fine-tuned system of chat rooms where we will be able to see on our computer screens the faces of the people with whom we are communicating—GeoCities in real time in full color. People who live in these virtual communities also live in real communities; they have dual citizenship. A person can be an American and also a citizen of America On-Line; another can be a citizen of Ecuador and Excite; another of the Netherlands and Netscape; and another a dual citizen of Yemen and Yahoo. People are now able to buy and sell goods directly from each other—foodstuffs from exotic places, native works of art and artifacts (which are skyrocketing in price on the Internet), travel, and services. People can play games against opponents from all over the world. Many people are finding the Internet passionately consuming of their spare time, and others are finding a way to make a living on the Internet—either creating technology, or investing, or buying and selling, or providing the one thing in business transactions that computers are still deficient in—a human touch.

I have exaggerated my point, of course, but in this risky game of prediction we sometimes have to think outlandishly. As the world shrinks in size, as communication and knowledge-sharing become the key concepts of the twenty-first century, the Internet will increasingly be valued as a precious resource, the "heritage of mankind" in the words of international law. For this reason, as well as the systemic considerations I outlined earlier, I think that computer network attack will soon be the subject of an outright prohibition under customary international law.

Notes

1. Of course, a list of "real world consequences" can be programmed into the robot in the first place, in which case the robot will take those consequences into account. But if the consequences are not foreseen by the human programmer at the time of the programming—which is the usual case in war where surprises are part of the strategy of war—then the robot will simply not know about them and will not take them into account. At the present and reasonably foreseeable state of computer technology, a computer cannot "see" and "analyze" the real world and "evaluate" whether a given operation could be counterproductive in terms of its foreseeable real world consequences.

2. It is not clear, however, whether the rules contained in the Internal Revenue Code presuppose human interpreters, even though it is often claimed that IRS agents are human interpreters.

3. Even the Constitution of the United States gives Congress the power to issue letters of marque and reprisal (although the power was actually exercised only during the sea war of 1800 with France, and it was not a "classic" situation of self-help, but rather a roundabout way of enlisting the help of private vessels in a national war).

4. Controversy remains whether the Allied insistence upon "unconditional surrender" unnecessarily prolonged World War II. Of course, in 1945 German and Japanese leaders did not know about the potential of being tried as war criminals. If they had been able to foresee Nuremberg and the Military Tribunal for the Far East, would they have surrendered at all? I discuss some of the problems of negotiating a peace when the negotiators themselves may find themselves indicted for war crimes once the peace is established in Anthony D'Amato, *Peace v. Accountability in Bosnia*, 88 AMERICAN JOURNAL OF INTERNATIONAL LAW 500 (1994).

5. Anthony D'Amato, *The Concept of Human Rights in International Law*, 82 COLUMBIA LAW REVIEW 1110 (1982).

6. It was in NATO's interest to accurately inform Serbian citizens about the war and about NATO's limited war aims. Consider what happened in the first half of 1945 in Japan. The Japanese people were incessantly reassured by the press that the Allies were on the verge of being beaten and peace was imminent. Well, the papers were right about the imminence of peace, they just had the sides mixed up. If the Internet had been invented at that time, there would have been no way for the Japanese people to have been fooled by the Japanese controlled media. Our campaign to demoralize the Japanese people could have been accomplished more swiftly and with considerably less loss of life. In the aftermath of the Kosovo air campaign, Loral Space and Communications Limited said it might be forced to cut transmissions into Yugoslavia from one of its satellites under the general trade embargo that was proposed by the United States. Fortunately, State Department spokesperson James Rubin quickly denied that there were plans to interfere with Internet access for citizens of Yugoslavia.

7. Indeed, the Serbian news sources that remained in Internet communication provided useful information to American citizens and the American press. During the recent NATO bombing of Yugoslavia, I got my news of the progress of the bombing attacks from Belgrade and other Serbian Internet sources. I soon found out that the *New York Times* and the *Washington Post* were getting their information from the same Internet sources that I was using. What reason did we have to trust any of this information when we knew that the Milosevic government was censoring it? Let us take a specific case: a building in downtown Belgrade is struck by a missile, and the collateral damage in fact kills ten civilians. Now the Serbian Internet could inflate the casualties and say there were 50 civilians killed. But this kind of inflation, repeated over many bombings, could intimidate and terrorize the population of the city, and Milosevic could be counted on not to want to do that. All right, take the opposite extreme: they report no civilian deaths. But that falsification would encourage NATO to increase the bombardment, figuring that it is a surgically precise destruction of Serbian infrastructure with no loss of civilian life. So the safest path, the path of the least chance of government interference, is simply to report the accurate number of deaths, in this case ten. And as the *Times* and the *Post*, and I for that matter, discovered in the course of the war when there was independent empirical verification, Serbian Internet information about the bombings was by and large rather close to accuracy.

8. I believe that the United States has far more to lose if our computer networks are attacked than we could ever hope to gain by attacking the computer networks of other countries. Earlier in this conference someone shrugged off the damage that might happen to our banking and brokerage system by saying, "Well, so what if the Dow Jones drops 30%?" If that is all that happens, I would agree. But that is not what is going to happen. What will happen is people across the nation will find their Internet connections down and the television saying, "Don't worry, you haven't lost your life's savings." And they will call their banks and stock brokers and get a busy signal. And the word will sweep the nation that credit cards are no longer going to be accepted, and if you have

some hard cash on hand that is the only thing that will get you food. And there will be riots in every city and village, and people will raid the grocery stores and steal all the food. You and everyone else will fear that all their money—in banks, in stock accounts, in retirement plans—may have been wiped out by the Internet attack. Even if later it turns out that there was enough redundancy in the storage system to retrieve many of the financial records, it may come too late to prevent riots and insurrections. The dimensions of a national disaster of this kind could far surpass anything in our nation's history.

VI

Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter

Daniel B. Silver

Introduction

Awareness has been growing in recent years that modern societies, increasingly computer-dependent, are highly vulnerable to malicious intrusion into their computers and computer networks. Concern about this issue is especially high in the United States; in all likelihood, no other country is more at risk. The reality of these concerns is underscored by news reports chronicling an active "cyberwar" that appears currently to be underway. This is not, however, a conflict involving another State or even a terrorist group as the adversary. Instead, this struggle pits federal law enforcement officials against computer "hackers" who have defaced US Government Internet sites (including the website of the National Infrastructure Protection Center) and have threatened the electronic destruction of Internet servers if the federal government continues the battle.[1]

At the moment, the reality of such computer network attack (CNA) by private individuals and non-State actors may be more pressing than the use of CNA as an instrument of hostile action by one State against another. Whether CNA

actually has been used as an instrument of State action is uncertain as of this writing. According to numerous press reports, President Clinton approved a covert action against Serbian leader Slobodan Milosevic that was intended to include computer network attacks against Milosevic's financial assets held outside Yugoslavia.[2] It also has been reported that General Henry H. Shelton, Chairman of the Joint Chiefs of Staff, acknowledged that the United States used CNA against Serbian computer networks in the course of the Kosova conflict and that the Defense Department is actively engaged in organizing for the coordination not only of defensive measures to protect military computer networks from "cyberterrorists," but of offensive CNA operations.[3] However, unnamed "senior defense officials" also have been quoted as saying that the United States refrained from implementing plans to use CNA against Serbian computer networks for purposes of disrupting military operations and basic civilian services, due in part to legal guidance from the Defense Department's Office of General Counsel that certain uses of CNA could be considered as "war crimes."[4]

Thus, it remains unclear whether the United States attempted to use CNA in connection with the Kosova conflict. There is no doubt, however, that the Department of Defense has made an extensive study of the international legal issues that such use could engender[5] and that US military and national security experts, looking to the possibility of using CNA in future conflicts, have an understandable interest in understanding the implications of CNA under international law.

Such legal issues can arise under both the *jus ad bellum* and the *jus in bello*. This discussion is confined to the former, specifically to the extent to which peacetime use of CNA by or on behalf of a State (including use in the course of hostilities that do not attain the status of a war under international law) can be characterized as an exercise of "force" under Article 2(4) of the United Nations Charter.[6] Because the discussion is limited to this threshold question, it will not extend into other areas, in particular, when CNA that constitutes force under Article 2(4) might also rise to the level of an "armed attack" under Article 51 of the Charter or might be lawfully used as a defense against such an attack.[7]

At the outset, it may be useful to define the "rules of engagement" for this discussion. Reisman has pointed out that jurists' formulations, which characteristically take the form of "this is the law," often refer "simultaneously and without discrimination to descriptions about flows of decisions in the past, predictions about the way decisions may be taken in the future, or statements of preference."[8] This criticism seems particularly applicable to statements about international law. It thus is appropriate to make clear what kind of statements this chapter is intended to make.

It is too early for any legal authority to have emerged on the status of CNA under Article 2(4). Consequently, analysis of the question must proceed on the basis of analogy to such possibly relevant authority and doctrine as exists in other contexts. The statements about the law set forth in this chapter, therefore, do not purport to describe the flow of past decisions directly on point. Nor do they state a policy preference unless explicitly identified as such. Rather, they are predictive of where it appears that existing legal doctrine, found in other contexts, reasonably would carry a court seized with an issue concerning the status of peacetime CNA under Article 2(4).

The conclusion to which such predictive analysis leads is that there is no "bright-line" rule. Instead, certain applications of CNA are likely to be held to constitute force under Article 2(4), but many other applications are likely not to. This nebulous conclusion may disappoint the proponents of two positions that have emerged in scholarly and military circles. The first, focusing on the inherently malicious and destructive nature of CNA, advocates that it should be considered to be a prohibited use of force under Article 2(4) and thus to violate international law, except when otherwise authorized under the Charter. The second, viewing CNA as having the beneficial potential to achieve military or political objectives with less violence than traditional means of warfare, points in the opposite direction—CNA (except maybe in its most extreme applications) should not be viewed as a prohibited use of force, because to do so would promote the application of more lethal techniques. Approaching the question in a predictive mode, however, leads one to conclude that both these extremes are examples of wishful thinking, conflating a policy objective with a fair reading of the state of the law.[9]

Preliminary Questions

Before addressing the core question, several preliminary issues merit discussion, namely the definition of CNA, the techniques that it encompasses, and, finally, whether there is any real prospect that the status of CNA under Article 2(4) will be clarified without creating a new legal regime or clarifying instrument for that purpose.

The Definition of "Computer Network Attack"

A threshold question is what is meant by "computer network attack." CNA has been defined in Joint Chiefs of Staff doctrine as "operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks,

or the computers and networks themselves."[10] For the sake of convenience, this definition will be adopted for present purposes. But it should be noted that it sweeps too broadly to be truly useful, because it includes a range of physical techniques of attack that could be directed at almost any target.

Unless it be contended that computer facilities have a different status in international law than other facilities (a proposition for which there is no authority), targeting a kinetic weapon, such as a missile, bomb or other explosive device, at a computer (or, more likely, a structure known to house computing facilities) should not raise any different question under international law than if the same weapon were targeted at another piece of equipment or a structure used for a different purpose. The operation itself almost certainly will be characterized as a use of force.[11] Thus, because it includes techniques of physical attack that are not unique to computers but instead are widely applicable without distinction as to target, the Joint Chiefs' definition of CNA has limited utility as a tool of legal analysis.

At the same time, the definition contains an ambiguity that also may limit its usefulness, in that it is unclear whether it encompasses the manipulation of a computer network to achieve an effect extrinsic to the network itself, as opposed to merely rendering the network ineffective. An example of such an extrinsic effect would be the hostile manipulation of a computerized railway control system as to produce train wrecks.[12] Similar hypothetical examples abound, running from the potentially catastrophic[13] to the merely vexatious.[14] While such operations could be viewed as a form of "degrading" the information resident in the computer, the definitional fit is awkward. Since these manipulative variants of CNA are, however, potentially among the most important from a force perspective, they will be assumed to be included within the definition for purposes of this discussion.[15]

Techniques of CNA

How CNA is accomplished can have a bearing on the legal analysis. CNA is not a monolithic technique. On the contrary, there are many methods by which computer networks have been, or could be, attacked. Nor is CNA capable only of being directed at a single objective. Instead, a broad array of purposes can be served by hostile intrusion into computers or computer networks. These include, among others: (i) extracting the information held in the target computer (espionage); (ii) disseminating information through the adversary's information network in order to deceive the adversary or stimulate political instability; (iii) preparing the battlespace by incapacitating the adversary's command, control, and communication capabilities; or (iv) causing property damage, physical

injury, or death by manipulating infrastructure or operational systems controlled by the target computer.

It should be obvious that which technique is being considered, as well as the purposes for which it is to be employed, can make a significant difference to the legal outcome. As noted above, a traditional physical attack (e.g., bombing the building that houses the computers) seems to present no legal issues specific to the fact that the target is a computer or computer network. The legally most interesting applications of CNA are those methods of attack which are highly specific to computers because they make use of the methods by which computers themselves operate.

Concern about infrastructure security and the potential vulnerability of the United States to malicious intrusion on computers and computer networks has generated considerable discussion of the non-kinetic technical means by which computers might be attacked.[16] It is not necessary here to rehearse the technical details. It is sufficient to note their general outlines. What is unique to computers is their vulnerability to what has been called "digital data warfare" [17] namely the covert introduction of malicious computer code into a computer system or network to achieve an objective.

There is a rich lexicon describing variants of malicious computer code (e.g., "virus," "worm," "Trojan horse," "flying Dutchman," "time bomb," "logic bomb"[18]), but the labels do not matter here. What is significant in the present context is that malicious computer code can be designed to lie dormant until triggered and to self-destruct and eliminate evidence of its presence after the mission has been accomplished. Also significant is that most computer systems are linked electronically to other systems and that malicious code usually can be introduced into a computer system by electronic data transfer (over the Internet or directly) as long as the attacker can evade or overwhelm whatever defenses are built into the system. Malicious code also can be introduced into a computer system by concealing it in hardware or software that the operator of the target system unwittingly incorporates into the system. There also reportedly are back-door techniques for introducing malicious code into computer systems without any use of media for which the system was designed, for example by manipulating the power system or using high-energy radio frequencies or carefully controlled electromagnetic pulses.[19]

The Prospects that the Law will be Clarified

Although the application of UN Charter Article 2(4) to CNA is an intellectually interesting question, there is reason to wonder whether, as a practical matter,

the issue ever will arise in a context requiring an actual decision. The most important obstacle may be the difficulty of attributing CNA to State action. Moreover, even if State use of CNA were to emerge as a recognizable phenomenon, such CNA would have to occur in relative isolation in order squarely to pose the relevant legal issue. Because this seems improbable, it likely will be a long time, if ever, before the practice of States, decisions of the International Court of Justice (ICJ), or other recognized sources of international law yield a clarification of how Article 2(4) applies to CNA. Thus, the best prospect for a prompt and authoritative elucidation of the status of CNA under Article 2(4) would be if States were to agree to define the legal parameters of CNA through an appropriate international instrument.

1. State action. Although various authors have posited a number of forms that an incident of CNA could take, from disrupting air traffic control systems to "busting" dams or oil pipelines, the rub is that, at least up to the time of this writing and to the best of the author's knowledge, none of these imaginable instances of CNA actually has been perpetrated by a State or with publicly-discernible State sponsorship.[20] Indeed, the more extreme (and therefore more interesting) examples apparently have not occurred at all.

It certainly is true that numerous instances of intrusion into computer networks by private individuals (generally called "hacking") have taken place recently.[21] Some of these have been fairly primitive, such as the flooding of US Government Internet websites with messages ("spamming") emanating from Serbia and protesting US bombing of that country.[22] Others have been more sophisticated and potentially quite harmful, including attacks on Defense Department and other US Government computer networks. But most appear to have been the work of individuals or groups not identified (at least not in any source accessible to the public) as sponsored by a State.

Lacking acknowledged, or at least provable, State action or State sponsorship, such events must be considered as raising problems in international criminality, not public international law. Moreover, to date there appears to have been no State reaction to CNA in the international legal arena. Because no State has yet taken any action or asserted a legal position vis-à-vis another State arising out of an incident of CNA, there is a lack of the State practice that could illuminate the international legal analysis of CNA, whether under Article 2(4) or under customary international law.

This state of affairs is not surprising. CNA is a new phenomenon. Moreover, unlike many other putative techniques of force, most forms of CNA may be difficult or impossible to trace to the real perpetrator. Indeed, the most effective forms of CNA are likely to be contrived so as to conceal the fact that they

occurred at all, leaving the target State in doubt as to whether the affected computer network was externally attacked or simply failed for other reasons. Obviously, to the extent that it is not possible plausibly to demonstrate the existence of an event of CNA, even less the identity of the perpetrator and a nexus to a State sufficient to imply State responsibility, any State response based on an alleged violation of Article 2(4), or indeed any other norm of international law, would lack credibility.

This issue is exacerbated by the amorphous structure of the Internet. If an incident of CNA is effected by "indirect penetration"[23] over the Internet, it may be difficult to determine where it originated. There is no inherent reason why the point from which the attack is launched must be in the territory of the State that caused the act to be done. Moreover, even if the identity of the immediate perpetrator is discovered, it may be impossible to demonstrate a link between that person or organization and a State to which responsibility for the CNA can be attributed. To date, the mode of CNA in actual practice is the computer "hacker," wreaking havoc for sport or, occasionally, for some ideological motive. One would expect any State that chose to use CNA as a weapon to attempt to make its efforts look like those of a hacker.

Moreover, the contexts in which a State is most likely to use CNA unaccompanied by an array of traditional military instruments are intelligence collection and covert action, for example, the use of CNA to sow unrest in the target State's population. Such applications of CNA, however, probably are also the least likely to be publicly acknowledged by, or credibly attributable to, the State that perpetrates them.

2. Unlikelihood of Isolated Use. In order for the status of CNA under Article 2(4) to emerge as an issue, the incident in question probably would have to be considered in isolation. If, as may have been the case in the Kosova conflict, CNA is used in the context of a military operation conducted by traditional means that indubitably constitute force, the target State would have little interest in raising a legal dispute on the sole issue of CNA. (Thus, Serbia may have tenable claims that the entire operation conducted against it was a violation of international law, but it is unlikely that it would single out US hacking into its computer networks, if it occurred, as a separate violation, even less one worthy of an individualized response.)

The Status of CNA Under Article 2(4)

Lacking any directly applicable precedents or other sources of international law, the status of CNA under Article 2(4) only can be predicted by drawing

analogies to other phenomena whose status is better established. If CNA in all its manifestations easily could be assimilated to armed force, further discussion would be superfluous, since Article 2(4) indisputably encompasses armed force. Neither every form of CNA nor every purpose for which CNA can be used, however, readily can be analogized to armed force. Some applications of CNA (including, notably, those the United States is reported to have contemplated using against Slobodan Milosevic) operate only in the economic or political sphere, thus making highly relevant the question whether Article 2(4) encompasses measures of economic or political coercion, or, if not all such measures, at least those that threaten the target State's territorial integrity or political independence. Moreover, because it may be unclear (given the inherent problems of tracing CNA to its source) whether an incident of CNA has been conducted by military forces, another relevant issue, if one is to reason by analogy, is whether non-military uses of physical force can fall within the scope of Article 2(4).

Economic and Political Coercion as Force

Virtually since the Charter was adopted, controversy has existed as to whether measures of economic and political coercion constitute force under Article 2(4). The weight of scholarly opinion supports the negative view,[24] but that does not appear to have put the question to rest, at least as applied to CNA. Thus, one recent analysis of CNA under Article 2(4), while admitting that the "prevailing view" among scholars would confine Article 2(4) to "armed force," asserts that a more balanced, contextual view of Article 2(4) would conclude that economic and political sanctions can threaten international peace and a target State's territorial integrity and political independence and therefore can fall within the ambit of Article 2(4); the author's conclusion that CNA generally falls within Article 2(4) derives from this premise.[25] In contrast, another recent analysis of the status of CNA under Article 2(4) adopts the opposite conclusion, that "the prohibition of the threat or use of force includes armed, but not economic or political coercion."[26] The same author goes on to comment, however, that the borders of force do not necessarily "precisely coincide with armed force, i.e., physical or kinetic force applied by conventional weaponry."[27]

On balance, the latter perspective is better founded. Although a conclusion that economic or political coercion standing alone constitutes force under Article 2(4) might well contribute more to the purposes of the Charter and to the maintenance of world order than the contrary, that does not make it tenable as a matter of legal analysis. A number of points sustain the view that Article 2(4) does not apply to measures of political or economic coercion. These include the following:

- The historical background of Article 2(4) shows that it was conceived against a background of international efforts to eliminate unilateral recourse to armed force.[28] Measures of economic and political coercion were not the issue.
- The *travaux preparatoires* of the Charter indicate that the San Francisco Conference declined to adopt a proposal that was advanced to extend the prohibition on the use of force to include economic sanctions. Subsequent General Assembly declarations, principally the Declaration on Friendly Relations[29] and the Declaration on the Enhancement of the Effectiveness of the Principle of Refraining from Threat or Use of Force in International Relations,[30] provided an opportunity for the General Assembly to clarify the issue by delineating economic and political coercion as equivalents of armed force for purposes of Article 2(4). Efforts were made by some Members to this end, but they met resistance from other Members and were unsuccessful,[31]demonstrating that there is no common understanding among Members that would support extending Article 2(4) to economic or political coercion.
- There is no decision of the International Court of Justice (ICJ) holding that measures of economic or political coercion constitute force under Article 2(4). Indeed in the *Nicaragua* case,[32] in which the Court generally considered the customary international law prohibition against the use of force to be coterminous with Article 2(4) (which was not itself at issue), Nicaragua complained of substantial measures of economic pressure. These were considered to be violations of the bilateral treaty of Friendship, Commerce and Navigation between Nicaragua and the United States, however, and were not even mentioned as possible violations of the customary international law prohibition on the use of force. Moreover, the Court held that even the United States' furnishing of substantial financial support to insurgent forces in Nicaragua, support that was used to sustain acts of violence, did not constitute the use of force under customary international law.[33] It would seem, if financing an armed insurrection is not force, that, *a fortiori*, other economic measures that have a less direct nexus to armed violence would not be either.

Thus, despite arguments advanced to the contrary, the fact remains that the drafting history of the Charter is inconsistent with such an extension, that this question generally has divided Western States from significant components of the "Third World," and that no international consensus has emerged defining economic and political coercion, standing alone, as force, although there is a

strong basis for concluding that such forms of coercion may violate other norms of international law, such as the principle of non-intervention.[34]

An argument can be made that the prevailing view regarding economic and political measures of coercion should not apply to CNA. Although ultimately not convincing, it proceeds along the following lines. In more than half a century of debate over the application of Article 2(4) to economic and political coercion, the kind of coercion that has been envisaged has been primarily external and gradual—trade sanctions, withholding economic benefits, unequal trading practices, interference with the target State's external commercial relations. In contrast, the kind of economic coercion that CNA might make possible, crippling the banking system, or shutting down the securities markets, operates on the internal economic structures of the target State and does so through a swift and devastating blow. Therefore, since CNA is a different phenomenon, it can be argued that the earlier debate over economic and political sanctions as force is irrelevant.

While the factual premise underlying this argument may be valid, all it demonstrates is the neutral fact that CNA is a new form of hostile activity. That CNA may differ from earlier forms of economic and political coercion does not tell us whether CNA comes within the intended scope of Article 2(4) or instead should be viewed as another manifestation of the types of economic and political coercion that various states have failed to persuade the international community to acknowledge as falling within the definition of "force."

In analyzing the application of Article 2(4) to CNA in order to predict how the ICJ and the world community will view CNA, it seems prudent, in light of existing legal authority, to acknowledge, however much a different conclusion might be desired on policy grounds, that there is little likelihood that purely economic or political coercion, even if effectuated in novel ways, will be considered to violate Article 2(4). If this proposition is correct, it suggests that the touchstone in any future analysis of CNA under Article 2(4) will be whether the specific application of CNA at issue more closely resembles economic and political coercion, on the one hand, or, on the other hand, military force as the latter concept is commonly understood.

Non-Military Physical Force

Another interpretive issue under Article 2(4) that bears on the status of CNA is whether non-military physical measures can also constitute force for purposes of Article 2(4). Examples of such measures would include: a State intentionally acts to cause flooding in an adjacent down river State; a State sets a forest fire in a

frontier region intending that it spread into the target State; a State releases noxious substances into the environment, knowing that the effect will be felt in the target State. Opinion is divided as to the status of such acts under Article 2(4) and there is no decisional authority directly on point. Some scholars admit the possibility that in certain circumstances a hostile use of such non-military forms of physical force could fall within Article 2(4), especially if the results rose to a level of magnitude that could be viewed as the equivalent of an armed attack triggering the right of self-defense under Article 51.[35]

The better view would appear to be that non-military physical force can indeed fall within Article 2(4), even if the consequences do not rise to the level of an armed attack. The principal reason why scholars have opposed such an extension of Article 2(4) appears to be a "slippery slope" fear that applying Article 2(4) to non-military physical force when its effects approximate those of military force would open the door to applying Article 2(4) to measures of economic and political coercion that have similarly devastating effects. This fear is misplaced. In the case of non-military physical force, the fact that the force is physical is enough, first, to distinguish it from coercive economic and political measures and, second, to support an analogy to those military forms of physical force that clearly lie at the core of Article 2(4).

If one is prepared to admit that non-military physical measures can constitute force for purposes of Article 2(4), it is hard to see why this should be the case only if the consequences are of a type and degree of seriousness that would rise to the level of an armed attack. It is widely recognized that not all force under Article 2(4) necessarily constitutes an armed attack under Article 51. The ICJ implicitly so stated when it indicated in the *Nicaragua* case that supplying arms and other support to armed rebel bands in another State is not an armed attack but could constitute a violation of the customary international prohibition on the use of force.[36] To require non-military force to rise to the level of an armed attack in order to violate Article 2(4) would obliterate the important distinction between Articles 2(4) and 51. Such a position would either legalize under Article 2(4) a broad range of hostile and destructive physical acts that fail to reach the armed attack threshold or would provide an incentive to lower the Article 51 threshold, with a concurrent risk of expanding violence under the pretext of legitimate self-defense. Thus, on balance, it seems better to conclude (although admittedly without the benefit of any supporting authority) that intentional, hostile uses of non-military physical force by one State against another can fall within the scope of Article 2(4) when they sufficiently resemble military force in their physically destructive effect, whether or not the criteria of an armed attack are met.

Flexibility of the Concept of Military Force

Even if one were to accept the restrictive view that force under Article 2(4) means military force, it should be noted that the latter concept carries a large measure of flexibility. As the techniques of warfare evolve, so too does the general understanding of what constitutes "military" force. If this were not so, the prohibition of Article 2(4) would become ossified at the level of military technology that existed at the end of World War II and would become increasingly irrelevant to the modern world. Thus, we have no difficulty in recognizing that new forms of biological and chemical warfare, directed energy, lasers, and other innovative technologies, if used intentionally by a State to cause physical injury or property damage in another State, will constitute forms of military or armed force. This applies even when the instrument itself, like a laser beam, is not inherently harmful but also is used for a range of beneficent purposes.

The hard question is how one recognizes when a new technology has become a form of military or armed force. The answer is not always obvious, but one significant criterion is whether the technique is associated with the armed forces of the State that uses it. Thus, in the case of CNA, if this technique were to be deployed only by intelligence agencies in conducting covert actions, it seems less likely that it would be generally accepted as a form of military or armed force than if it were used by the armed forces. Consequently, it is likely that the fact that the US Department of Defense (apparently joined by the military forces of other countries) is making preparations for the military use of CNA will hasten the day when a State's offensive use of CNA, at least for purposes of causing physical injury or property damage, will be considered a use of force under Article 2(4).

Preliminary Conclusions

Against the background of the foregoing discussion, what preliminary conclusions can be reached about the application of Article 2(4) to CNA? The basic conclusion appears to be that force is like pornography: the law will recognize certain forms of CNA as force when it sees them. The present state of legal development does not permit laying down any hard and fast rules as to when that will be. It does, however, permit one to make some predictions about the circumstances in which State use of CNA may be likely to be held to constitute force under Article 2(4).

- CNA is not a single form of activity, nor is it potentially capable only of being directed at a single purpose. Thus there is no basis for concluding

that all forms of CNA per se constitute a violation of Article 2(4). Consequently, whether and when CNA will fall within the force category must be determined on a case-by-case basis. The question is how.

- CNA is most like traditional military force, and thus most likely to constitute force under Article 2(4), if its direct and foreseeable effects are physical injury or property damage.
- CNA that directly and foreseeably produces physical injury or property damage similar to that resulting from the use of traditional forms of weaponry is likely to be viewed as a use of force under Article 2(4), especially if that CNA is carried out by a State's armed forces.
- CNA that produces effects (even if direct and foreseeable) that are only of an economic or political nature is not likely to be held to be within the scope of Article 2(4). (Thus a program of CNA that crippled the financial infrastructure of a target State would not be a use of force under Article 2(4). Even if angry investors rioted and tore down the stock exchange, that physical damage would not be direct and foreseeable.)

The notion that CNA will be recognized as force under Article 2(4) when it sufficiently resembles military force implies that views on particular forms of CNA are likely to evolve in light of developments in military operations. These may lead to surprising conclusions. For example, before NATO's campaign against Serbia, one might have predicted that using CNA to produce transitory power outages in a target State would not be recognizable as an analog or equivalent of military force, because it causes no permanent damage to the targeted power system, and the effects on users of power, including the military, are uncertain, indirect and incalculable. Transitory outages seem more of an economic measure or a psychological weapon (intended, if one may put it this way, to induce a sense of powerlessness in the target State's population and leadership) than a military one.

In the last year, however, it was reported that the United States, on behalf of NATO, employed an innovative form of weapon against Serbia, a type of carbon filaments used against electric power facilities.[37] The filaments were dropped from aircraft, like a bomb, with the intention of causing property damage. Thus, it seems incontrovertible that their use was a form of armed force, even though the attacks did little or no permanent damage, merely shorting out the power system and disabling it for a brief period, thereby producing some disruption to the economy and the military effort, but having principally a psychological effect.

The same kinds of effects on the power system could be produced by CNA. Should this ever occur, it is likely that the earlier military use of the analogous

weapon described above will color the way the world looks at such use of CNA to shut down a target State's power system through manipulating its computerized controls. The existence of a military, non-CNA precedent, it is submitted, will create a predisposition to try to fit such an incident of CNA into the force category.

The Views of Other Commentators

A small number of commentators have addressed the status of CNA under Article 2(4) and have come to widely divergent conclusions. A few assert that CNA causing destructive effects is *ipso facto* a use of "force." Others espouse the view advanced in this chapter, that CNA will only constitute force under Article 2(4) if it sufficiently resembles what the world recognizes as armed or military force and focus on attempting to provide a more precise way of identifying the principles that underlie such recognition.

1. Destructive effect as the touchstone. In one of the most extensive examinations of this issue to date, Sharp has proposed a rule that appears both sweeping and simple: "*Any* computer network attack that intentionally causes *any* destructive effect within the sovereign territory of another state is an unlawful use of force within the meaning of Article 2(4) that may produce the effects of an armed attack prompting the right of self-defense."[38]

It should be noted that this rule is not without its own interpretive issues. Does the term "destructive" mean only physical destruction, for example, or does it include economic harm? Sharp suggests that it could include the latter in some circumstances. He concludes that Article 2(4), while not including all coercive economic and political sanctions that are intended to influence another State's policy or actions, does extend to coercive political and economic sanctions that threaten the territorial integrity or independence of another State.[39] Thus, a non-physical destructive effect (such as disruption of financial markets) should be considered force under Article 2(4) if it is sufficiently serious to threaten the target State's territorial integrity or independence.

Aside from the fact that this conclusion is inconsistent with the weight of legal authority, extending the concept of "destruction" to include coercive economic and political measures, but only if they threaten another State's territorial integrity or independence, seems likely to deprive the posited rule of much of its apparent objectivity and simplicity, because it is not easy to determine when economic and political measures are likely to have such an effect unless the judgment is being made after the effect already has been produced.

For example, the Arab boycott of Israel manifestly was intended to threaten that country's territorial integrity and independence; it was carried out by States

that had declared war on Israel and espoused as their war aim the total elimination of the target country. Did that set of economic measures, or the associated political measures intended to delegitimize Israel in the international arena, really "threaten" Israel's territorial integrity and independence? With the benefit of hindsight, the answer clearly seems negative, but at different points in time the outcome was not so clear. Would we therefore conclude that the Arab boycott was a violation of Article 2(4) at certain periods in Israel's history and not at others? Such a result seems an unworkable rule of law. The example illustrates the difficulty, except perhaps in the most extreme cases, of applying a rule that depends on determining when a threat exists to territorial integrity or political independence.

In advancing the "destructive effect" standard, Sharp reasons on the basis of the proposition that other forms of non-military physical force constitute force under Article 2(4),[40] citing as examples the release of floodwaters or the spreading of fire across a border.[41] The argument then proceeds to adumbrate types of significant property damage, as well as possible human fatalities, that could be effected through CNA, such as flooding, train wrecks, plane crashes, chemical explosions, and fires. If these physically destructive events would constitute force under Article 2(4) if produced by a State agency using non-military means, it is argued, why should they not also be considered force when produced by CNA?

Although the underlying premise does not seem to be supported by judicial decision or State practice, the conclusion nonetheless is reasonable and should be widely accepted if confined to the examples given above. The analysis becomes markedly less compelling, however, when this already untested proposition is used as a springboard to make a leap into the arena of the financial, political, or psychological. The analogy to flood or fire is not convincing as a basis for concluding that causing "a run on banks or a massive financial crisis by crashing national stock exchanges"[42] also would constitute force. It pushes the underlying principle too far. (It should be noted that this assessment is not intended as a value judgment. Such State intervention in the affairs of another ought to be prohibited by international law and, indeed, may well may be on other grounds, such as the principle of non-intervention. The sole question, here, is whether Article 2(4) provides the norm.)

There might well be narrow circumstances in which Article 2(4) could be held applicable to an attack having effects solely or primarily in the economic or political sphere, but, if so, it is submitted, this would be because of the *means* employed, not the nature of the target. For example, if a State were to use physical but non-military means to achieve these results (e.g., dispatching intelligence

operatives into the target State to cut a fiber-optic cable on which essential financial information is transmitted), scholars might well conclude that an incident of force had occurred. Suppose instead, however, that a State sought to achieve the same end, financial disruption in the target State, through purely non-physical means, such as large-scale falsification of trading orders or dissemination of false market information. These seem to be quintessential measures of economic coercion, and it is very unlikely that scholarly opinion would sustain the view that such acts constituted force under Article 2(4). Thus, identity of ultimate effects, standing alone, simply does not supply a sufficient basis for concluding that Article 2(4) applies. The reason why the act of sabotage might be held to constitute force is not the end result (that the stock exchange crashes), but cutting the cable would involve an intrusion on the target State's territory that, although arguably "non-military," would achieve a physical effect closely resembling the use of kinetic action.

2. Characteristics of armed force as the touchstone. In a recent analysis, Schmitt, recognizing that within the existing framework of international law, CNA will be deemed to be Article 2(4) force only when it sufficiently resembles armed force, embarks on an impressive effort to delineate a principled basis for identifying those cases of CNA that meet this test.

He notes that traditional notions of force are instrument-based: the Article 2(4) prohibition against using a particular instrument, namely military force, against another State is tied to the high degree of congruence between its use and reprobated consequences, primarily physical destruction and injury. This, it is posited, explains why armed force, which almost always results in physical destruction or injury, is prohibited force, while economic or political coercion, whose tie to predictable physical destruction or injury is tenuous, is not.[43]

This observation is not entirely satisfying, however, because, as Schmitt has recognized, "the instruments do not precisely track the threats to shared values which, ideally, the international community would seek to deter."[44] It is clear that many technologies that would be recognized as weapons when used for the purpose of causing physical damage or personal injury, e.g., laser beams, can be entirely beneficent in other uses, such as medicine. Thus, when we assign one of those technologies to the "armed force" category, it is not because of its inherent lethality but because of the potential destructiveness of the way it is being used or the purpose for which it is deployed. The same could be said of CNA. And, for this reason, it seems unlikely that many would debate that CNA used directly to cause physical destruction or injury (busting a dam, rupturing a pipeline, causing airplanes or trains to crash) is tantamount to a weapon for purposes of Article 2(4), making its use force. The question is whether, applying criteria that will be

recognized as consistent with the current understanding of Article 2(4), any other use of CNA is sufficiently similar to these easy cases to be placed confidently in the force category.

To answer this question, Schmitt has suggested that, unless the international community is prepared to adopt a new normative structure to apply to inter-State coercion, the analysis of CNA must be fit into the traditional instrument/consequence based frame of reference by looking to see whether particular uses of CNA meet the criteria that distinguish armed force from political or economic coercion.[45] These criteria, he suggests, are: *severity*—the higher threat of physical injury or property damage associated with armed force; *immediacy*—the comparative swiftness of harm arising from armed force, as compared with other forms of coercion; *directness*—the relatively direct connection between armed force and negative consequences, as compared with other forms of coercion; *invasiveness*—the fact that in the case of armed force the act causing harm generally crosses into the territory of the target State whereas measures of economic or political coercion normally do not; *measurability*—the greater ease and certainty of assessing the consequences of armed force as compared with other forms of coercion; and *presumptive legitimacy*—the fact that violence is presumptively illegal under domestic and international law, whereas most (or at least many) techniques of economic and political coercion are presumptively legal.[46]

It would be desirable to be able to delineate criteria for identifying those types of CNA that should be treated as analogous to armed force. Yet, it is not clear that Schmitt's proposed six criteria reliably serve this purpose. Rather, examination of the criteria suggests that virtually any event of CNA can be argued to fall on the armed force side of the line, except perhaps as regards the criterion of severity, and that the criterion of severity in effect is just another way of articulating the observation that, for an event of CNA to be considered a type of force under Article 2(4), it must produce (or at least threaten to produce) personal injury or property damage similar to that caused by military weapons. Review of the proposed criteria, it is submitted, substantiates this proposition.

Immediacy: CNA ordinarily occurs with great immediacy, once its destructive potential is triggered. While malicious software may be designed to lie dormant for an extended period until some triggering event occurs, once it becomes active, the disruption of the targeted computer or computer network can be expected to be immediate, as well as immediately perceptible in result, even if the owner of the computer does not recognize that CNA is the cause of its degradation or destruction. (It is hard to imagine circumstances in which a slow, imperceptible deterioration of the targeted computer would be advantageous to the

author of the attack.) Thus, there seems to be little difference between CNA and ordinary armed force.

Directness: Compared to economic or political coercion, many applications of CNA are as direct as traditional armed force. The consequences generally flow directly from the act of attack itself and do not depend on intervening or contributory factors in order to have a harmful effect. Directness might become an issue if the only harmful effect were property damage and any effect on human beings was reactive. Thus, there could be a significant difference between CNA that caused a dam's floodgates to open and kill people, and CNA that merely inconvenienced the target population (e.g., by disrupting financial markets) to such a degree that rioting ensued. On the other hand, the path even from the latter form of CNA to the reprobated result of physical injury and tangible property damage is no more (or less) indirect than similar consequences, such as starvation or health disasters, arising from a military blockade. Yet a military blockade is undeniably a use of force. To the extent that the directness criterion is useful, it really seems to do no more than restate the proposition that to constitute force an event of CNA must directly cause physical injury or property damage and not operate solely in the economic or political realm.

Invasiveness: At least at the level of electrons, the act causing the harm in a CNA attack usually crosses into the target State, whether it be by importation of a corrupted item of hardware or software, the actions of an agent of the hostile State (a cyber saboteur), or cross-border data transmission over the telephone network. There appears to be no difference, in this regard, between CNA and traditional armed force.

Measurability: There seems no reason to assume that the consequences of an event of CNA would be any harder to measure than the negative consequences of armed coercion.

Presumptive legitimacy: Many States already have enacted laws outlawing CNA when perpetrated by private parties within the territory. As more and more States become aware of the threat, it is likely that this technique, at least when used by non-State actors, will be viewed in most States as presumptively illegal,[47] thus eliminating any distinction between CNA and what traditionally has been regarded as armed force.

Factoring out those of the criteria that do not appear reliably to distinguish CNA from armed coercion, all that is left is *severity*. Moreover, severity, as defined for this purpose, seems applicable only to physical injury and property damage, compelling the conclusion that CNA will be considered within the force category only if its foreseeable consequence is to cause physical injury or property damage and, even then, only if the severity of those foreseeable

consequences resembles the consequences that are associated with armed coercion. In short, what seems at first blush to be a nuanced way of analyzing incidents of CNA in practice may in fact turn out to do no more than identify the cases that would be clear without applying a criterion any more formal than was suggested in the preliminary conclusions above: CNA will be considered as force when it causes physical injury or property damage that is recognizably similar to that produced by instruments generally identified as weapons.

The limitations of the proposed factors are demonstrated by Schmitt's own comparison of two hypothetical uses of CNA.[48] In the first, CNA is used to disable an air traffic control system, causing airplanes to crash. According to Schmitt, this meets the criteria and is force. In the second example, the attacker destroys a university computer network for purposes of disrupting military research being conducted on campus. This does not meet the test and is not force. Schmitt suggests that there should be a different result in the attack on the university because the desired outcome, diminished capacity on the battlefield, is too remote from the event of CNA and too dependent on indeterminate factors. But this is not persuasive; the question of remoteness depends on how the outcome is defined. The immediate objective of the hypothetical CNA is to degrade the functioning of the targeted computer network, and the nexus between the act and that outcome is immediate. (One could as well argue that dropping filaments on Serbian electric power facilities to produce temporary power outages is remote from the ultimate objective, impairing Serbia's ability to maintain military operations. Yet few would gainsay that the NATO bombing raids in which these devices were dropped constituted force under Article 2(4).) Thus, except for this purported difference in directness, Schmitt's two examples are remarkably similar with respect to the proposed factors. In reality, it is submitted, the only tenable reason, and the real underlying explanation, for the difference in the posited outcome is that in the first case there is physical injury and significant property damage and in the second there is not.

That severity does not reliably predict the legal outcome unless it is confined to the severity of physical injury and/or property damage is shown by considering another hypothetical use of CNA, disruption of the target State's financial system through interference with the computers through which securities are traded, money moves, and financial transactions are recorded and settled. If successfully used against the United States or many other Western countries, the resulting social and economic disruption and monetary losses would be staggering. For each of Schmitt's factors, this event of CNA seems comparable to disabling an air traffic control system, except for the fact that it does not directly and foreseeably result in physical injury or property damage. In terms of severity,

more broadly construed, can there be any doubt that the impact of such an attack would be orders of magnitude more serious than if a hostile State, through a missile attack that caused no loss of life, obliterated a military warehouse full of uniforms—an incident that no one would hesitate to describe as within the scope of Article 2(4)? Yet, applying the existing legal framework for analyzing Article 2(4), this hypothetical attack on the country's financial infrastructure probably would be considered to fall outside the Article 2(4) force category, because it much more closely resembles economic coercion than traditional armed force.

Conclusion: The Unsatisfactory Reality

There is no legal authority directly applicable to the status of CNA under Article 2(4). The most significant interpretive issue under Article 2(4) that might support extending it to a broad range of types of CNA is whether force includes economic or political coercion, and the weight of prevailing opinion is that it does not. Against this background, two approaches recently have been suggested in the literature. The first, destructiveness as the criterion, is relatively simple to apply (or could be made so with a few clarifications) and might be an appealing rule in a legislative context. The problem is that it is not founded in sufficient legal authority to engender confidence as a correct predictive statement of international law under Article 2(4). The second recognizes the limitations imposed by prevailing interpretations of Article 2(4) and tries to remain faithful to them, while positing criteria by which one can recognize those uses of CNA that fall in the force category. The exercise turns out to be somewhat illusory, however. At bottom, it leads to a conclusion that probably can be reached by reference to only one criterion: whether the foreseeable consequence of a particular manifestation of CNA is physical injury or property damage comparable to that resulting from military weapons. If so, the CNA will be held to fall within the force category. Otherwise it will not.[49]

What we are left with, it is submitted, is a situation in which general agreement probably can be reached on the proposition that there are some kinds of CNA that so resemble armed force that, like other manifestations of non-military physical force that have been suggested as falling within Article 2(4) (e.g., diverting a river in the hostile State so as to cause flooding in the target State), they will be held to fall within the scope of Article 2(4). It is likely that these forms of CNA will be recognized widely as Article 2(4) force if and when they occur, but it is difficult to articulate the precise bases on which recognition will rest. The one basis that seems most reliable is that physical injury or property damage must arise as a direct and foreseeable consequence of the CNA and must

resemble the injury or damage associated with what, at the time, are generally recognized as military weapons.

This conclusion appears highly unsatisfactory, leaving the law in a state of uncertainty, but does it really matter that much? First, it is clear that, whether or not they violate Article 2(4), most significant uses of CNA probably will violate other rules of international law, such as the prohibition against intervention in the affairs of other States, which the ICJ has held to be a principle of customary international law.[50] Various specific techniques used in carrying out CNA are likely to violate other international treaties, such as those relating to telecommunications. Thus, responsible decision-makers concerned about determining the legality of proposed uses of CNA are not bereft of legal principles to guide them.

Second, at least from the target State's perspective, the key issue is whether an incident of CNA gives rise to a right to take counteraction in self-defense. For that right to arise under the Charter, there must be an armed attack within the meaning of Article 51, a standard that goes beyond the existence of force under Article 2(4). It is difficult to say whether an event of CNA that caused significant physical injury and/or property damage, standing alone, ever could be considered an armed attack. In all likelihood, however, a State's use of CNA of such magnitude would not occur in isolation; instead it probably would form part of a coordinated offensive, other elements of which undeniably would constitute armed attack. In such a context, the legal status of the CNA element in isolation probably would be of little importance.

Third, worrying about the status of CNA under Article 2(4) may be fiddling while Rome burns. The notion that the Charter represents the sole legal structure under which coercive force can be exerted by one State against another largely has been discredited—both by the failure of the Security Council mechanism to function as envisioned by the Charter's framers and by the practice of States in ignoring recourse to the Security Council in favor of unilateral (including alliance-based) interventionism. The recent NATO humanitarian intervention in Serbia, which was given the fig leaf of a Security Council resolution only after its military aims were achieved, may be a step on the road to a better and more moral system of international law, but it was only the most recent in a series of events that, over the decades, have dealt a heavy blow to the system supposedly established by the Charter.[51] These events sustain the view that, while Article 2(4) represents an aspiration, (perhaps, like another form of prohibition, a failed "noble experiment"), the reality of international law on the use of force lies in the development of a "nuanced code for appraising the lawfulness of individual unilateral uses of force"[52] that is different from Article 2(4). If so, it can be

expected that over time a set of understandings as to the lawfulness of CNA will evolve outside the Charter framework.

This patient approach will not satisfy many, especially those who view CNA as a dangerous phenomenon. Enormous benefits to humankind, both actual and potential, derive from the use of computers. Advanced societies are moving towards pervasive dependence on the interplay of computer networks and advanced communications technologies. While not all consequences necessarily are welcome (loss of privacy, for example, is a significant concern), technologically sophisticated countries like the United States are experiencing enormous benefits in terms of increased productivity and enhancement of many aspects of the quality of life. These are benefits to which the rest of the world appears to aspire.

Yet technological sophistication engenders a degree of vulnerability that would have been unimaginable in earlier generations. (Who would have imagined a few decades ago that significant numbers of people would fear the end of a millennium not for religious reasons but because of a computer programming issue?) Human well-being throughout the world increasingly will depend on the inviolability of computer networks and the communications links that connect them. The world, it can be argued, should not have to rely for protection on unclear and debatable interpretations of the Charter or on principles of customary international law, such as non-intervention, that are honored in the breach and carry no ready enforcement mechanism. Nor should civilian populations be exposed to the risk that a code of rules on the use of CNA will evolve only after devastating examples of its use have pointed the way.

Thus, it is suggested (and this is an explicit expression of a policy preference, not a statement about the law as it is), efforts should be made towards the adoption of an international convention that would bind the parties not to use CNA for any military or hostile use. This should be accompanied by enhanced efforts, whether in the context of the same convention or separately, to achieve global legal cooperation in fighting CNA perpetrated by non-State actors, by making such action criminal under domestic laws regardless of purported justification, and by allowing prosecution of the perpetrators wherever apprehended or their extradition to the country in which the target computer or computer network was located.

Notes

1. *Hackers Hit More Federal Web Sites*, WASHINGTON POST, June 5, 1999, at A5.

2. *See, e.g.*, Bruce D. Berkowitz, *Operation Backfire: Covert Action Against Milosevic is Neither Secret nor Smart*, WASHINGTON POST, July 18, 1999, at B1; Philip Sherwell, Sasa Nikolic & Julius

Strauss, *Kosovo: After the War: Clinton Orders "Cyber-sabotage" to Oust Serb Leader*, SUNDAY TELEGRAPH, July, 4, 1999, at 27; Gregory L. Vistica, *Cyberwar and Sabotage*, NEWSWEEK, May 31, 1999, at 38.

3. John Markoff, *Cyberwarfare Breaks the Rules of Military Engagement*, NEW YORK TIMES, October 17, 1999, News In Review, at 5.

4. Bradley Graham, *Military Grappling with Guidelines for Cyberwar*, WASHINGTON POST, November 8, 1999, at A1.

5. *See* Office of General Counsel, Department of Defense, An Assessment of International Legal Issues in Information Operations, (Nov. 1999) [hereinafter DoD/GC Paper]. The paper is appended to this volume as the Appendix.

6. Article 2(4) is one of the basic principles in accordance with which members of the United Nations are obligated to act. It provides that "[a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations." UN Charter, art. 2, para.4.

7. It generally is accepted that "force" under Article 2(4) is not necessarily always an "armed attack" under Article 51. The present discussion leaves to others the attempt to define the circumstances in which the use of CNA would rise to the level of an armed attack or would be a legitimate measure of self-defense under Article 51. UN Charter, art. 51.

8. W. Michael Reisman, *Allocating Competences to Use Coercion in the Post-Cold War World: Practices, Conditions and Prospects, in* LAW AND FORCE IN THE NEW INTERNATIONAL ORDER 26, at 28 (Lori Damrosch Fisler & David J. Scheffer eds., 1991).

9. That the law is unclear and possibly lacking should be no surprise. There can be little argument that Article 2(4) is not well adapted to rapidly evolving technologies. Nor would many be heard to contend that the Charter framework, including Article 2(4), is a perfect and effective instrument for controlling undesirable hostile activities directed by one State against another (not to speak of failing adequately to address the growing threat of hostile activities by non-State actors).

10. Chairman of the Joint Chiefs of Staff, Joint Publication 3-13, Joint Doctrine for Information Operations (1998).

11. Whether that use of force violates international law will depend on the circumstances, including, *inter alia*, the nature of the target (military or civilian), whether the event occurred in war or in peacetime and, in the latter case, whether the operation fell within an exception to the Article 2(4) prohibition (e.g., an exercise of the right of self-defense under Article 51).

12. *See* President's Commission on Critical Infrastructure Protection, Critical Foundations: Protecting America's Infrastructures, at A-48 (1997), *cited in* Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUMBIA JOURNAL OF TRANSNATIONAL LAW 885 (1999).

13. For example, the manipulation of a hospital's computer-controlled life-support systems to cause them to malfunction. *See* Lawrence G. Downs, Jr., *Digital Data Warfare: Using Malicious Computer Code as a Weapon, in* ESSAYS ON NATIONAL STRATEGY XIII 43, 54 (Mary A. Sommerville ed., 1996).

14. Downs reports that unidentified persons are studying "psycho-electronics" by which a virus introduced into a computer system causes the video screen to flicker, inducing headaches in users of the video display, such as radar operators. *Id.*

15. The range of potential CNA activities perhaps could be more accurately captured, without destroying the alliterative symmetry of the Joint Chiefs' current definition, by amending it to include "operations to disrupt, deny, degrade, destroy or deleteriously deploy information resident in computers and computer networks, or the computers and networks themselves."

16. *See, e.g.*, Downs, *supra* note 13.

17. *Id.* at 44.

18. *Id.* at 45.

19. *Id.* at 49–50.

20. As noted above, press reports suggest that some form of CNA may have been approved for use by NATO forces in operations against Serbia. *See, e.g.,* William Drozdiak, *Allies Target Computer, Phone Links,* WASHINGTON POST, May 27, 1999, at A1. It appears, however, that what really was involved was the targeting of the public telecommunications system. While degradation of the public switched network almost certainly will cause substantial collateral effects on computer networks, it is questionable whether general attacks on telecommunications or electric power infrastructures, both of which can massively affect computer networks, usefully can be considered a form of CNA. In the case of Serbia, in any event, the question is of little interest in the present context, since NATO's bombing attacks indubitably constituted a use of force. In any event, the United States now appears intent on disavowing any such uses of CNA in the Kosova conflict. *See supra* note 4.

21. *See, e.g.*, General Accounting Office, Information Security: Computer Attacks at Department of Defense Pose Increasing Risks, AIMD-96-84 (May 22, 1996).

22. Ellen Joan Pollack & Andrea Peterson, *Serbs Take Offensive In The First Cyberwar, Bombing America,* WALL STREET JOURNAL, April 8, 1999, at A1.

23. Downs, *supra* note 13, at 49.

24. *See, e.g.*, YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENSE 18 (2d ed. 1994); Albrecht Randelzhofer, *Article 2(4), in* THE CHARTER OF THE UNITED NATIONS: A COMMENTARY 112 (Bruno Simma ed., 1994).

25. WALTER GARY SHARP, SR., CYBERSPACE AND THE USE OF FORCE 88–91 (1999).

26. Schmitt, *supra* note 12, at 908.

27. *Id.*

28. *See generally,* Edward Gordon, *Article 2(4) in Historical Context,* 10 YALE JOURNAL OF INTERNATIONAL LAW (1985).

29. Declaration on Principles of International Law Concerning Friendly Relations and Cooperation Among States in Accordance with the Charter of the United Nations, G.A. Res. 2625 (XXV), UN GAOR, 25th Sess., Supp. No. 28, UN Doc. A/8082 (1970).

30. G.A. Res. 42/22, UN GAOR, 42d Sess., 73d plen. mtg., Agenda Item 131, annex (1988).

31. *See* Schmitt, *supra* note 12, at 905–908, for a discussion of this history.

32. Military and Paramilitary Activities (*Nicaragua v. United States*) 1986 I.C.J. 4 (June 27).

33. *Id.* at 119.

34. *See generally, e.g.*, Schmitt, *supra* note 12, at 904–908.

35. Randelzhofer, *supra* note 24, at 113.

36. Military and Paramilitary Activities, *supra* note 32, at 108, 109–110, 126–127.

37. *NATO Warplanes Jolt Yugoslav Power Grid,* WASHINGTON POST, May 25, 1999, at A1.

38. SHARP, *supra* note 25, at 140. Essentially the same conclusion is reached by a law student author of a case note on information warfare. *See* Todd A. Morth, *Considering Our Position: Viewing Information Warfare as a Use of Force Prohibited by Article 2(4) of the U.N. Charter,* 30 CASE WESTERN RESERVE JOURNAL OF INTERNATIONAL LAW 567 (1998).

39. SHARP, *supra* note 25, at 90–91. The author suggests that CNA having purely economic consequences could even rise to the level of an armed attack, citing the example of a "complete and long-term crash of the New York Stock Exchange." *Id.* at 117. This conclusion appears highly debatable.

40. *Id.* at 101, *citing* IAN BROWNLIE, INTERNATIONAL LAW AND THE USE OF FORCE BY STATES at 113 (1963).

41. SHARP, *supra* note 25.

42. *Id.* at 102.

43. Schmitt, *supra* note 12, at 911.

44. *Id.* at 914.

45. *Id.*

46. *Id.* at 915.

47. One could question the utility of this criterion, since it may well apply as much to economic or political coercion as it does to other forms of CNA and to traditional armed force. While some instruments for exercising such coercion are presumptively legal under both domestic and international law (such as cutting off financial aid to the target State or imposing trade sanctions), others (such as creating economic pressure by massive fraud or theft or destabilizing the target State's political process by corrupt payments to government officials) are presumptively illegal under domestic law and may well violate norms of international law other than Article 2(4), such as the principle of non-intervention.

48. Schmitt, *supra* note 12, at 916–917.

49. Schmitt seems to imply, at least in theory, that there might be a form of CNA that does not cause physical injury or property damage but which causes consequences which approximate the nature of those involving armed force and thus comes within the scope of Article 2(4), but no example is given.

50. Military and Paramilitary Activities, *supra* note 32, at 106.

51. To this effect, see, for example, Michael Glennon, *The New Interventionism*, FOREIGN AFFAIRS, May/June 1999, at 2.

52. W. Michael Reisman, *Criteria for the Lawful Use of Force in International Law,* 10 YALE JOURNAL OF INTERNATIONAL LAW 297, at 280 (Spring 1985).

VII

Computer Network Attacks and Self-Defense

Yoram Dinstein

Armed Attack and Self-Defense

The general prohibition of the use of force in the relations between States constitutes the cornerstone of modern international law.[1] It is currently embedded both in the Charter of the United Nations [Article 2(4)[2]] and in customary international law (which has consolidated under the impact of the Charter).[3] Indeed, the International Law Commission has identified the prohibition of the use of inter-State force as "a conspicuous example" of *jus cogens*[4] (i.e., a peremptory norm of general international law from which no derogation is permitted[5]). The Commission's position was cited by the International Court of Justice in the *Nicaragua* case of 1986,[6] and in two Separate Opinions the peremptory nature of the proscription of the use of inter-State force was explicitly emphasized.[7]

The correct interpretation of Article 2(4) of the Charter subsequent to the *Nicaragua* Judgment is that there exists in international law today "an absolute prohibition of the use or threat of force, subject only to the exceptions stated in the Charter itself."[8] The only two exceptions spelled out in the Charter are collective security pursuant to a Security Council decision (by virtue especially of Article 42 [9]) and individual or collective self-defense (consistent with

Article 51[10]). This chapter will focus on self-defense, namely, forcible counter-measures put in motion by States acting on their own (individually or collectively), in the absence of a binding Security Council decision obligating or authorizing them to behave in such a fashion.

In accordance with Article 51 of the Charter, the right of self-defense can only be invoked in response to an "armed attack." The choice of words in Article 51 is deliberately restrictive. The phrase "armed attack" is not equivalent to "aggression" (a much broader and looser term, used, e.g., in Article 39 pertaining to the powers of the Security Council[11]). An armed attack is actually a particular type of aggression. This is borne out by the French text, which speaks of *"une agression armée."* The expression "armed attack" denotes the illegal use of armed force (i.e., recourse to violence) against a State.

For an illegal use of force to acquire the dimensions of an armed attack, a minimal threshold has to be reached. Since Article 2(4) of the Charter forbids "use of force" and Article 51 allows taking self-defense measures only against an "armed attack," a gap is discernible between the two stipulations.[12] The gap is due to the fact that an illegal use of force not tantamount to an armed attack may be launched by one State against another, but then (in the absence of an armed attack) self-defense is not an option available to the victim. Logically and pragmatically, the gap has to be quite narrow, inasmuch as "there is very little effective protection against states violating the prohibition of the use of force, as long as they do not resort to an armed attack."[13] If a victim State is barred from responding with counter-force to force, this ought to be confined to the sphere of application of the ancient apothegm *de minimis non curat lex.* In other words, all that the gap conveys is that the illicit use of force has to be of sufficient gravity.[14] When the use of force is trivial—say, a few stray bullets are fired across a frontier—no armed attack can be alleged to have occurred.[15] In that case, there is no room for forcible counter-measures of self-defense.[16] By contrast, when the use of force is of sufficient gravity, an armed attack is in progress even if it is characterized by small magnitude. *Au fond,* whenever a lethal result to human beings—or serious destruction to property—is engendered by an illegal use of force by State A against State B, that use of force will qualify as an armed attack. The right to employ counter-force in self-defense against State A can then be invoked by State B (and, as we shall see *infra,* also by State C).

To better understand the legal position, it is necessary to distinguish between an armed attack, on the one hand, and an ordinary breach of international law—or even a mere unfriendly act—on the other.

State A can commit an unfriendly act against State B without thereby being in breach of any binding norm of international law. Such unfriendly conduct by

State A is liable to upset State B. It may cause the latter psychological embarrassment or even material harm in the political, diplomatic, or economic arena. Yet, as long as no breach of international law is committed, State B does not possess any legal standing (*jus standi*) for objecting to the conduct of State A.

Acts that may highlight the phenomenon of unfriendly acts, carrying with them no connotations of infringement by State A of international law, are: (i) refusal to permit an official visit of State A by the Head of State B;[17] (ii) a notification that a member of the diplomatic staff of State B accredited to State A is *persona non grata*;[18] (iii) the prohibition of the import of certain goods from State B into State A (absent treaty commitments to the contrary);[19] and (iv) espionage carried out by clandestine agents of State A.[20] The fact that, strictly speaking, all these activities—and similar ones in the same vein—are legal (albeit unfriendly) does not mean that State B is completely helpless in terms of potential response. State B may opt to indulge in "retorsion" by taking equally legal yet unfriendly steps (such as a reciprocal expulsion of diplomats sent by State A).[21]

A breach of international law transcends unfriendliness, crossing the red line of illegality. If State A ignores the immunity from local jurisdiction enjoyed by duly accredited diplomatic agents of State B;[22] if State A's trawlers fish in the exclusive economic zone off the coast of State B;[23] if State A fails to extradite a fugitive from State B notwithstanding clear-cut obligations in a treaty concluded by them—State A will bear international legal responsibility vis-à-vis State B. In keeping with the international law of State responsibility, "[t]he injured State is entitled to obtain from the State which has committed an internationally wrongful act full reparation in the form of restitution in kind, compensation, satisfaction, and assurances and guarantees of non-repetition, either singly or in combination."[24]

Seeking reparation, State B—as the injured party—may present a legal claim against State A before any international court or tribunal which may be vested with jurisdiction over the dispute. Alternative avenues are also open. State B is always free to bring the dispute with State A to the attention of the Security Council [under Article 35(1) of the Charter[25]]. The Council may then recommend appropriate methods of adjustment [pursuant to Article 36(1)[26]] or even determine the existence of a threat to the peace (in compliance with the above-mentioned Article 39).[27] Acting on its own, State B may also apply non-forcible reprisals against State A[28] (e.g., by declining to extradite a fugitive from State A under the same treaty provision). A reprisal differs from retorsion in that the act in question (non-extradition) would have been illegal—in light of the treaty obligations postulated—but for the prior illegal act of State A.[29] Whichever channel of response is chosen by State B against State A, the

quintessential point is that, as a rule, the fact that State A incurs international responsibility towards State B does not create for State B a legitimate option to initiate force against State A. Even an ordinary violation of the UN Charter itself does not excuse response by force.

The only time—consistent with the Charter—when State B (without acting at the behest of the Security Council) may lawfully wield force against State A, in response to an illegal act by State A, is when that illegal act amounts to an armed attack and the counter-measures can be appropriately subsumed under the heading of self-defense.

Computer Network Attacks (CNAs)

The scientific and technological revolution, which has rendered the computer ubiquitous, has also "changed the scope and pace of battle."[30] This is evident to all where the computer serves as an instrument of command, control, communications, and intelligence (not to mention simulation, surveillance, sensors, and innumerable other military purposes). But the modern computer can also become a weapon in itself by being aligned for attack against other computer systems serving the adversary. A "computer network attack" (CNA) can occur either in wartime—in the midst of on-going hostilities—or in peacetime. The former situation is governed by the *jus in bello* and does not come within the scope of the present paper. The question to be analyzed here is the latter. More specifically, the fulcrum of our discussion is whether a CNA mounted in peacetime may be categorized as an armed attack, thus justifying forcible counter-measures of self-defense in compliance with the *jus ad bellum*.

A CNA is often defined inadequately as disrupting, denying, degrading, or destroying either information resident in a computer network or the network itself.[31] This definition is rooted in a presupposition that a CNA is no more than a device to counter the antagonist's electronic capabilities. Had the definition been legally binding—or had it factually mirrored the whole gamut of the technical capabilities of the computer—the likelihood of a CNA ever constituting a full-fledged armed attack would be scant. However, whereas CNAs recorded heretofore have admittedly been circumscribed to operations of intrusion and disruption, it would be extremely imprudent to extrapolate current restraints into the years ahead. A credible forecasting of future developments must start from the indisputable premise that potential CNAs (by feeding false messages into a target computer system) may also encompass grievous sabotage, designed to leave behind a trail of death and devastation through induced explosions and other malicious "malfunctions."[32]

The determination whether or not an armed attack has taken place—so as to justify response by way of self-defense—does not necessarily depend on the choice of weapons by the attacking party. The International Court of Justice aptly commented, in the *Nuclear Weapons* Advisory Opinion of 1996, that the provision of Article 51 does not refer to specific weapons; it applies to any armed attack, regardless of the weapon employed.[33] Of course, the detonation of weapons of mass destruction (say, nuclear warheads) makes it easier to stigmatize the strike as an armed attack. Still, what counts is not the specific type of ordnance, but the end product of its delivery to a selected objective. After all, even unsophisticated pernicious tools—like the poisoning of wells in a desert area—may give rise to exceedingly grave results.

From a legal perspective, there is no reason to differentiate between kinetic and electronic means of attack. A premeditated destructive CNA can qualify as an armed attack just as much as a kinetic attack bringing about the same—or similar—results. The crux of the matter is not the medium at hand (a computer server in lieu of, say, an artillery battery),[34] but the violent consequences of the action taken. If there is a cause and effect chain between the CNA and these violent consequences, it is immaterial that they were produced by high rather than low technology.

When a CNA emanates from within the territory of the same country in which the target is located (assuming that no foreign State is involved in the operation and no attempt is made to route the attack through a conduit abroad), this is a matter that in principle can—and should—be regulated by the domestic law of that country. Generally speaking, subject to few exceptions (see the next section), international law comes into play only at a point when the CNA turns into a cross-border operation.

Even in a cross-border scenario, CNAs are not all of the same nature. It is necessary to distinguish between four discrete rubrics of CNAs originating from State A and directed against State B, depending on whether they are unleashed by: (i) individual computer hackers who are residents of State A, acting on their own initiative for whatever personal motive (benign or otherwise) without any linkage to the government of State A; (ii) terrorists[35] based in State A, acting on behalf of any chosen "cause" inimical to State B, unsupported by the government of State A; (iii) terrorists overtly or covertly sponsored by the government of State A; and (iv) official organs—either military or civilian—of the government of State A.

The first two categories usually call for coercive action by the proper authorities of State A itself, with a view to precluding or terminating hostile acts conducted from within its territory by hackers or terrorists against State B. The

International Court of Justice proclaimed, in the *Corfu Channel* case of 1949, that every State is under an obligation "not to allow knowingly its territory to be used for acts contrary to the rights of other States."[36] In implementing this international obligation, State A should take resolute steps to suppress the perpetration of hostile activities from within its territory against State B—optimally by preventing these acts from materializing, but minimally by prosecuting offenders after the acts have already been committed. If the government of State A fails to do what it is supposed to, State B (as we shall see *infra*) can take certain exceptional counter-measures unilaterally.

When terrorists are sponsored by State A, they may be deemed "*de facto* organs" of that State.[37] "[T]he imputability to a State of a terrorist act is unquestionable if evidence is provided that the author of such act was a State organ acting in that capacity."[38] When State A chooses to operate against State B at one remove—pulling the strings of a terrorist organization (not formally associated with the governmental apparatus), rather than activating its regular armed forces—this does not diminish one iota from the full international responsibility of State A for the acts taken and their consequences, provided that "it is established" that the terrorists were "in fact acting on behalf of that State."[39]

The International Court of Justice, in the *Nicaragua* case of 1986, explicitly held that an armed attack encompasses not only action by regular armed forces but also the employment of "irregulars."[40] Granted, not every detail in this delicate area is universally agreed upon. The majority of the Court in the *Nicaragua* Judgment added that the mere supply of arms (or providing logistical and other support) to armed bands cannot be equated with armed attack,[41] whereas Judges Schwebel and Jennings sharply dissented on this point.[42] Be it as it may, there is a consensus that when State A goes beyond logistical support and dispatches a terrorist group to do its bidding against State B, State B can invoke self-defense against State A.

In 1999, the Appeals Chamber of the International Criminal Tribunal for the Former Yugoslavia pronounced, in the *Tadič* case, that acts performed by members of a military or paramilitary group organized by a State "may be regarded as acts of de facto State organs regardless of any specific instruction by the controlling State concerning the commission of each of those acts."[43] The Tribunal concentrated on the subordination of the group to overall control by the State. It opined that the State does not have to issue specific instructions for the direction of every individual operation, nor does it have to choose concrete targets.[44] Terrorists can thus act quite autonomously and still stay de facto organs of the controlling State.

The most crucial flow of events stems from a CNA undertaken overtly by official government organs. The intrusion of the organs of State A into the computer systems of State B may have a whole range of purposes and outcomes, for instance:

(i) Espionage. As indicated *supra*, espionage activities conducted by clandestine agents are merely unfriendly acts. In singular circumstances, official espionage is openly acknowledged by a State;[45] the question whether the act can then be viewed as a violation of international law is debatable.[46] In any event, espionage per se does not constitute an armed attack.

(ii) Disruption of communications and digitized services through the induced failure of computer systems, without causing human casualties or significant destruction of property. This is a CNA, but since the act (whether merely unfriendly or a transgression of international law) does not entail sufficiently grave consequences, the conclusion is the same.

(iii) Fatalities caused by loss of computer-controlled life-support systems; an extensive power grid outage (electricity blackout) creating considerable deleterious repercussions; a shutdown of computers controlling waterworks and dams, generating thereby floods of inhabited areas; deadly crashes deliberately engineered (e.g., through misinformation fed into aircraft computers), etc. The most egregious case is the wanton instigation of a core-meltdown of a reactor in a nuclear power plant, leading to the release of radioactive materials that can result in countless casualties if the neighboring areas are densely populated.[47] In all these cases, the CNA would be deemed an armed attack.

A salient point is that an excessive computer dependency creates a special vulnerability.[48] The more technologically advanced—and, therefore, computer reliant—a State is, the more susceptible it is to a paralyzing CNA. Overall, State A may be less developed scientifically and technologically than State B.[49] Yet, the very advantage of State B becomes a debilitating burden once State A manages to penetrate State B's electronic defenses. This, writ large, is the scenario of a nuclear core meltdown. Through a CNA, State A—having no nuclear capability of its own—can in a sense "go nuclear" by exploiting the scientific and technological infrastructure of State B, thus turning the tables on the target State. State B, as it were, provides the nuclear weapon against itself (the weapon being triggered by agents of State A).

CNAs against Private Individuals and Corporations

It must be appreciated that a computer system subjected to a CNA by State A need not belong to the government, or even to any semi-governmental agency, of State B. An attack may be carried out, e.g., inside US territory (or, for that matter, vessels flying the American flag and aircraft registered in the US) against a computer system operated by either a private individual or a non-governmental entity. The American situation is perhaps the most acute, inasmuch as public utilities in the US are privately owned, and, indeed, corporate America is the principal manufacturer of military equipment, naval platforms, and aircraft serving the American armed forces. But anyhow, it is immaterial whether the civilian computer system under attack is operated by a civilian supplier or sub-contractor of the Department of Defense. Even if the CNA impinges upon a civilian computer system which has no nexus to the military establishment (like a private hospital installation), a devastating impact would vouchsafe the classification of the act as an armed attack. There is no immanent difference between a CNA and a kinetic attack targeting ordinary civilian objects within the territory of State B. Needless to say, the bombing by State A of, e.g., an urban population center (apart from being unlawful per se under international humanitarian law, by not being directed against a military objective[50]) constitutes an armed attack, albeit not a single member of the armed forces of State B is injured in the air-raid. The same rule is applicable to a CNA.

Furthermore, a CNA—just like a kinetic use of force—by State A would qualify as an armed attack against State B even if the computer system inside the territory of State B (including its vessels and aircraft) is operated by an individual or a private corporation possessing the nationality of State C. A corporation, on an analogy with an individual, has a distinct nationality (that of the State under the laws of which it was incorporated and in whose territory it has its registered office).[51] But the foreign nationality of the corporate or individual operator of the computer system under attack is irrelevant from the perspective of State B, as long as the CNA is carried out within its territory.

What happens when a CNA is inflicted by State A outside the territory of State B, but it affects a computer system operated by State B or one of its nationals (individual or corporate)? It goes without saying that a lethal kinetic strike against a governmental installation of State B stationed outside its territory, vessels, and aircraft—such as an embassy of State B in the capital city of State C (or even State A)—will be deemed an armed attack against State B, notwithstanding the geographic disconnection from its territory.[52] This is also true of an

electronic attack against the computer system of State B's embassy in State C (or in State A) culminating with fatalities or destruction of property.

The position differs when the target of an armed attack (kinetic or electronic) by State A is situated in State C, and any injury caused to State B or to its nationals is coincidental. In such a case, State B cannot regard itself as the genuine object of the armed attack. On the other hand, if a destructive CNA is launched by State A within the territorial boundaries of State C (or even State A) against a computer system operated privately by nationals (individual or corporate) of State B—and the target is specifically selected on account of that nationality—State B is entitled to consider the act an armed attack against itself. Thus, if an explosion-inducing CNA strikes a computer operated by US citizens across the ocean—and this is plainly done not at random but because of the American nationality of the operators—the act may be deemed an armed attack against the US (although perpetrated abroad). There are many instances in international relations in which nationals attacked abroad by State A have been protected or rescued by State B in the name of self-defense.[53] This is perfectly legitimate, provided that the attack occurred owing to the bond of nationality existing between the victims and State B.[54] Once more, there is no difference here between an electronic and a kinetic attack.

Self-Defense Responses to CNAs

Just as there are variable settings for the commission of an armed attack by State A in the form of a CNA, there are also several possible responses available to State B in the exercise of its right of self-defense. The most obvious response is "on-the-spot reaction,"[55] where the computer network under attack strikes instantaneously back at the source of the CNA. The trouble, however, is that frequently the server which is seemingly the source of the CNA has only been manipulated by the true assailants (who have routed their attack through it), and swift responsive counter-measures against the intermediary conduit is liable to be counterproductive, as well as unlawful.[56] Establishing the genuine identity of the attacker—and attributing the act to the real (as distinct from apparent) actor—is a major challenge in the present stage of technological development (see discussion *infra*).

On the whole, the most effective modality of self-defense against an armed attack in the shape of a CNA is recourse to defensive armed reprisals, to wit, forcible counter-measures undertaken at a different time and place. Armed reprisals as such are generally "considered to be unlawful" in peacetime.[57] But there is no reason why armed reprisals cannot come within the framework of self-defense

under the Charter. Armed reprisals can constitute a legitimate response to an armed attack within the ambit of Article 51, provided that they are genuinely defensive, namely, future-oriented (deterrent in character) and not past-oriented (confined to punitive retaliation).[58] State practice definitely shows that defensive armed reprisals are part and parcel of the arsenal of States subjected to armed attacks.[59] Indeed, falling back on defensive armed reprisals has certain built-in advantages. Above all, it gives State B an opportunity to review the facts (and determine culpability) while considering options for response.

It should be borne in mind that defensive armed reprisals against a CNA can be performed kinetically even though the original armed attack (justifying them) was executed electronically, and vice versa. Again, whatever is permitted (or prohibited) when kinetic means of warfare are used is equally permitted (or prohibited) when the means employed are electronic; the rules of international law are the same whatever the means selected for attack.

The ultimate type of force stimulated by self-defense may amount to (or may result in) war.[60] In the setting of CNAs, the outbreak of war as a countermeasure of self-defense would be rare. Due to the conditions precedent to the waging of war as an exercise of self-defense (see discussion *infra*), war would constitute a proper response to a CNA only in far-fetched scenarios (such as the calculated prompting of a nuclear core meltdown).

Sometimes, State A—constrained by political or military considerations—would passively tolerate the use of its territory as a base for activities by terrorists against State B, without actively sponsoring those activities or even encouraging them.[61] Such a turn of events would not cloak the terrorists with a mantle of protection from State B. "If a host country permits the use of its territory as a staging area for terrorist attacks when it could shut those operations down, and refuses requests to take action, the host government cannot expect to insulate its territory against measures of self-defense."[62] As already epitomized in the classical *Caroline* incident of 1837,[63] State B may legitimately invoke self-defense to exert counter-force within the territory of State A—targeting armed bands which use that territory as a springboard for operations against State B—when the host government remains inert. The present writer calls such a mode of self-defense "extra-territorial law enforcement,"[64] while others prefer the term "state of necessity."[65] What counts, however, is the substance of the law and not the formal appellation. The substance of the law in this respect relates to electronic, as much as kinetic, terrorism against State B originating in State A.

The Three Conditions of Self-Defense

Three cumulative conditions to the exercise of self-defense are well-entrenched in customary international law: (i) necessity, (ii) proportionality, and (iii) immediacy. The first two conditions were articulated in the 1986 *Nicaragua* Judgment,[66] and reiterated in the 1996 *Nuclear Weapons* Advisory Opinion.[67] Immediacy, while glossed over in the Court's rendering of the law, is of equal specific weight.[68]

Necessity primarily denotes "the non-existence of reasonable peaceful alternative measures."[69] Differently put, non-forcible remedies must either prove futile *in limine* or have in fact been exhausted in an unsatisfactory manner; the upshot is that there is no effective substitute for the use of force in self-defense. In the context of a CNA, it is requisite to ascertain that the CNA is no accident, to verify the genuine identity of the State—or non-State entity—conducting the attack (so as not to jeopardize innocent parties), and to conclude that the use of force as a counter-measure is indispensable. Should there be an opportunity to settle the matter amicably through negotiations, these must be conducted in good faith.[70]

The second condition is chiefly relevant to defensive armed reprisals undertaken in a situation "short of war." The counter-measures taken by State B (kinetically or electronically) must not be out of proportion with the act prompting them.[71] A modicum of symmetry between force and counter-force—injury inflicted on State B by the armed attack versus damage sustained by State A by dint of the self-defense counter-measures—is called for.

Since CNAs are often discharged in a cluster—and inasmuch as each one of them, when examined in isolation, may appear to have only a minor ("pin-prick") adverse effect, yet, when assessed in their totality, the results may be calamitous—the question is whether defensive armed reprisals may be undertaken in proportion to the cumulative effect of the sequence of attacks.[72] The issue, which ordinarily arises in the face of assaults by terrorists, is not free of difficulties.[73] But there is some authority for the position that a State suffering from a series of small-scale attacks is permitted to respond to them aggregately in a single large-scale forcible counter-measure.[74] This would equally apply to CNAs.

The balance between the quantum of force and counter-force, which is the key to the legitimacy of defensive armed reprisals, is not germane to war as the ultimate manifestation of self-defense in response to an armed attack.[75] Once war is in progress, it may be fought to the limit (subject to the exceptions and qualifications decreed by international humanitarian law), and there is no

mandatory correspondence between the scale of force expended by the opposing sides.[76] The meaning of proportionality in the concrete circumstances of war is that the use of comprehensive counter-force in the exercise of self-defense must be warranted by the critical character of the original armed attack.[77] Once the vital justification of a war of self-defense by State B against State A is recognized, there is no additional need to ponder the defensive disposition of every single measure taken by State B. From the outset of a war of self-defense until its termination (which is not to be confused with the suspension of hostilities through a cease-fire[78]), the legitimacy of every instance of the use of force by State B against State A is covered by the *jus ad bellum* (albeit not necessarily by the *jus in bello*). Admittedly, where CNAs are concerned, a war of self-defense would be vindicated as an appropriate response only in *outré* circumstances (such as the catastrophic event of a CNA-induced nuclear core meltdown).

Immediacy intrinsically suggests that the activation of self-defense countermeasures must not be too tardy. Still, this condition is construed "broadly."[79] There may be a time-lag of days, weeks, and even months between the original armed attack and the sequel of self-defense. The delay may be particularly glaring after a CNA, since in cyberspace activities can produce reverberations around the world "in the time that it takes to blink an eye."[80] Still, lapse of time is almost unavoidable when—in a desire to fulfill the letter and spirit of the condition of necessity—a slow process of diplomatic negotiations evolves, with a view to resolving the matter amicably.[81]

Interceptive Self-Defense

The gist of Article 51 of the Charter is that there is no legitimate self-defense *sans* an armed attack. All the same, an armed attack need not start with the opening of fire on the aggrieved party. In fact, at times, it is the victim of an armed attack who fires the first shot. For an obvious example, suffice it to postulate that military formations commissioned by State A intentionally cross the frontier of State B and then halt, positioning themselves in strategic outposts well within the territory of State B (the movement of Pakistani troops into Indian Kashmir in 1999 is a good case in point[82]). If the invasion takes place in a region not easily accessible and lightly guarded, it is entirely conceivable that some time would pass before the competent authorities of State B grasp what has actually transpired. In these circumstances, it may very well ensue that the armed forces of State B would be instructed to dislodge from their positions the invading contingents belonging to State A, and that fire be opened first by soldiers raising the banner of State B. Nevertheless, since the international frontier has been crossed

by the military units of State A without the consent of State B, State A cannot relieve itself of responsibility for an armed attack.

As a matter of fact (and law), an armed attack may be viewed as a foregone conclusion even though no fire has been opened (as yet) and no international frontier has been crossed. Thus, hypothetically, had the Japanese aircraft en route to Pearl Harbor on December 7, 1941, been intercepted and shot down over the high seas by US air forces, Japan would still have incurred responsibility for the armed attack that triggered the Pacific War.[83] A more up-to-date scenario would be that of a missile site whose radar is locked on to a target in preparation for fire.[84] The linchpin question in analyzing any situation is whether the die has been cast. Resort to counter-force in the exercise of self-defense cannot be purely preventive in nature, inasmuch as threats alone do not form an armed attack. Still, if it is blatant to any unbiased observer that an armed attack is incipient or is on the verge of beginning, the intended victim need not wait impotently for the inescapable blow; the attack can legitimately be intercepted. Interceptive (in contradistinction to anticipatory) self-defense comes within the purview of permissible self-defense under the Charter. The theme of interceptive self-defense is apposite to a CNA when an intrusion from the outside into a computer network has been discovered, although, as yet, it is neither lethal to any person nor tangibly destructive of property. The issue is whether the intrusion can plausibly be construed as the first step of an inevitable armed attack, which is in the process of being staged (analogous to the detection of attack aircraft en route to their objectives). It is a matter of evaluation on the ground of the information available at the time of action (including warnings, intelligence reports, and other data), reasonably interpreted.[85]

The Attribution of CNAs to a State

Reference has already been made to the problem of attribution to State A of a CNA as an armed attack for which responsibility devolves on that State. As observed, in the present state of the art, it is often by no means clear who originated the CNA. The inability to identify the attacker undermines in practice the theoretical entitlement of State B to resort to forcible counter-measures in self-defense.[86] State B must not rush headlong to hasty action predicated on reflexive impulses and unfounded suspicions; it has no choice but to withhold forcible response until hard evidence is collated and the state of affairs is clarified, lest the innocent be endangered. However, the following points should be recalled:

(i) The same problem arises in many other situations, for instance when acts of terrorism are committed kinetically. Frequently,

either the perpetrators of the terrorist attack act anonymously—leaving no signature—or those "taking credit" are unfamiliar. Since States sponsoring terrorism usually try to conceal their role: holding such States accountable for their misdeeds may be fraught with great difficulties.[87] Prior to determining its options in combating terrorism, the victim State must establish a linkage between the terrorists and their sponsoring State.[88] CNAs invite a similar approach.

(ii) Not always is attribution shrouded in doubt for long. In the past, wars began with bombings and bombardments. In the future, they are increasingly likely to start with CNAs. But recourse to a CNA does not mean that the enemy wishes to remain incognito indefinitely. It is within the realm of the possible that a CNA will be merely the precursor of a wave of later attacks, which will be mounted with traditional means and be easily traceable to an irrefutable source. Hence, it would be a mistake to assume that a CNA inevitably manifests an attempt at deception and perfidy. The CNA may be designed merely to achieve surprise and cause temporary havoc, without trying to hide the identity of the perpetrator for a prolonged stretch of time.

(iii) Future advances in technology are likely to make it much easier to identify the attacker, just as current—unlike past—technology enables the immediate registration of the source of an incoming telephone call (although, patently, identification of that source does not conclusively establish which person is actually making the telephone call; the same is true of the user of a computer).

Collective Self-Defense

Pursuant to Article 51 of the Charter, collective—no less than individual—self-defense is permissible against an armed attack. The rule does not discriminate between different classes of armed attacks, and therefore it pertains *inter alia* to a CNA crossing the threshold of an armed attack. The right to collective self-defense means that any third State in the world[89] (State C) is free to join State B in bringing forcible measures to bear against State A, with a view to repelling an armed attack. The occurrence of an armed attack by State A against State B as a *conditio sine qua non* to the exercise of collective self-defense against State A by State C was underscored by the International Court of Justice in the

Nicaragua case.[90] The majority of the Court further held that State C may not exercise that right unless and until State B has first declared that it has been subjected to an armed attack by State A.[91] This dictum has been cogently challenged in a dissent by Judge Jennings,[92] but it may have some merit against the background of a CNA. Certainly, States B and C must see eye to eye on the identification of an elusive attacker. State C is enjoined from taking collective self-defense action against State A if State B (the immediate target) declines to confirm that State A is indeed accountable for a CNA constituting an armed attack.

The exercise of collective self-defense in conformity with the Charter is a right and not a duty. The right can be transformed into a duty should States B and C become contracting parties to a mutual assistance treaty or a treaty of guarantee, and *a fortiori* to a military alliance.[93] Thus, if State B happens to be a member of NATO, other members of the alliance are expected to extend military aid when an armed attack occurs against it (within certain geographic bounds).[94] But there is no need for a collective self-defense treaty to exist between State B and State C. State C is competent to act spontaneously—appraising events as they unfold—and it can do so whether the armed attack against State B is kinetic or electronic.

The Supervision of the Security Council

Article 51 of the Charter sets forth that the right of self-defense may be exercised until the Security Council has taken the measures necessary to maintain international peace and security. Under the article, a State invoking self-defense must immediately report to the Council what steps it has taken, and these steps do not diminish from the authority of the Council to take any action it deems necessary. As the International Court of Justice enunciated in the *Nuclear Weapons* Advisory Opinion, the "requirements of Article 51 apply whatever the means of force used in self-defence."[95] There is thus no difference between kinetic and electronic counter-measures.

Three thorny aspects of the Security Council's supervisory powers deserve to be mentioned. First, as a matter of fact, "[r]elatively few communications have been circulated expressly to meet the Charter obligation to report immediately to the Council on measures taken in the exercise of the right of individual or collective self-defence after an armed attack has occurred (Article 51)."[96] As a matter of law, however, a failure to report to the Security Council about engaging in self-defense against a CNA may be perilous. In its Judgment in the *Nicaragua* case, the majority of the Court implied that a State may be precluded from relying on the right of self-defense if it fails to comply with the requirement of reporting to the Council.[97] Judge Schwebel dissented, holding that the reporting

duty is a procedural matter and that therefore nonfeasance must not deprive the State concerned of its substantive cardinal right to self-defense.[98] The dissent is quite persuasive, but the majority's position cannot simply be disregarded.

Second, the Security Council's record since its inception is not such as to instill much confidence in the likelihood of its taking the necessary remedial action for the maintenance of international peace and security, thus avoiding any further need of unilateral self-defense against an armed attack. Once the Council's inaction was largely due to the Cold War and the abuse of the veto power by Permanent Members, each voting in tandem with the political interests of the bloc which it led or to which it belonged. Regrettably, even recent permutations in Big Power politics have not revived the faith in the Security Council's role as an above-the-fray arbiter of all armed conflicts in the international community.

Third, it is by no means clear what sort of resolution adopted by the Security Council would divest States of the right to embark upon unilateral use of force in self-defense against an armed attack. Surely, the Council is fully empowered to override specious claims to self-defense and adopt a legally binding decision to the effect that allegedly defensive measures must stop forthwith. But this does not mean that "any measure" adopted by the Council "would preempt self-defense."[99] Short of an explicit decree by the Council to discontinue the use of force, the State acting in self-defense retains its right to do so until the Council has taken measures which have actually "succeeded in restoring international peace and security."[100] Only effective measures that would not leave the victim State defenseless can terminate or suspend the exercise of the right of self-defense.[101]

Conclusion

The introduction of any new weapon into the arsenal of inter-State conflict raises first and foremost the issue of its legality. Under Article 36 of Additional Protocol I (of 1977) to the Geneva Conventions, any State adopting (or even developing) a new weapon must first determine whether or not it is prohibited by international law;[102] this norm appears to reflect customary international law.[103] CNAs are not incorporated in any present list of proscribed weapons under the *lex lata*. Evidently, there is a separate issue *de lege ferenda* whether mankind would not be better off by legally banning them altogether. The dilemma will probably be debated with growing intensity as the incidence of CNAs leaves their mark on the evolution of armed conflict.

The novelty of a weapon—any weapon—always baffles statesmen and lawyers, many of whom are perplexed by technological innovations. It is perhaps natural to believe that a new weapon cannot easily intermesh with the

pre-existing international legal system. In reality, after a period of gestation, it usually dawns on belligerent parties that there is no insuperable difficulty in applying the general principles and rules of international law to the novel weapon (subject to some adjustments and adaptations, which crystallize in practice). It can scarcely be denied that, unless legally excluded in advance, CNAs are almost bound to play a pivotal role as a first-strike weapon in the commencement of future hostilities. The challenge is to study now the most efficacious means of response to this ominous prospect.

Notes

1. For a general treatment of the subject, see Y. DINSTEIN, WAR, AGGRESSION AND SELF-DEFENCE (3d. ed. 2001).

2. Charter of the United Nations, 1945, 9 INTERNATIONAL LEGISLATION 327, 332 (M.O. Hudson ed., 1950).

3. *See* the Judgment of the International Court of Justice in Military and Paramilitary Activities in and against Nicaragua (*Nicaragua v. United States.*), 1986 I.C.J. 14, 96–97 (merits).

4. Report of the International Law Commission, 18th Session, [1966] II YEARBOOK OF THE INTERNATIONAL LAW COMMISSION 172, 247.

5. Consult the text of Article 53 of the 1969 Vienna Convention on the Law of Treaties, [1969] UNITED NATIONS JURIDICAL YEARBOOK 140, 154.

6. *Nicaragua* Judgment, *supra* note 3, at 100.

7. *Id.* at 153 (President Singh), 199 (Judge Sette-Camara).

8. J. Mrazek, *Prohibition of the Use and Threat of Force: Self-Defence and Self-Help in International Law,* 27 CANADIAN YEARBOOK OF INTERNATIONAL LAW 81, 90 (1989).

9. UN CHARTER, *supra* note 2, at 343–344.

10. *Id.* at 346.

11. *Id.* at 343.

12. *See* A. Randelzhofer, *Article 51, in* THE CHARTER OF THE UNITED NATIONS: A COMMENTARY 661, 664 (B. Simma ed., 1995).

13. *Id.*

14. *Cf.* Article 2 of the consensus Definition of Aggression adopted by the UN General Assembly in 1974. General Assembly Resolution 3314 (XXIX), 29(1) RESOLUTIONS ADOPTED BY THE GENERAL ASSEMBLY 142, 143 (1974).

15. *Cf.* B. Broms, *The Definition of Aggression,* 154 RECUEIL DES COURS 299, 346 (1977).

16. In the *Nicaragua* case, the majority of the International Court of Justice envisaged legitimate counter-measures "analogous" to but less grave than self-defense in response to use of force which is less grave than an armed attack (without ruling out the possibility that these counter-measures would involve the use of force by the victim State). *Nicaragua* Judgment, *supra* note 3, at 110. However, absent an armed attack, the only counter-measures available to the victim State are short of force; self-defense is ruled out even by analogy.

17. Unless there exists a treaty between the two countries calling for periodic consultations between their respective Heads of States. In such an instance, refusal to allow the visit might rise above mere unfriendliness and be branded as a breach of the treaty.

18. Such a notification is permissible at any time—without any need to explain the decision—under Article 9 of the 1961 Vienna Convention on Diplomatic Relations, 500 UNITED NATIONS TREATY SERIES 95, 102.

19. *See* [1976] DIGEST OF UNITED STATES PRACTICE IN INTERNATIONAL LAW 577–578 (E.C. McDowell ed., 1977).

20. "*Clandestine agents: spies* ... are not official agents of states for the purpose of international relations:" the home State usually disavows them, although—if caught in the act—the State upon whom they spied is likely to punish them severely under its domestic law. 1(2) OPPENHEIM'S INTERNATIONAL LAW 1176–1177 (R. Jennings & A. Watts eds., 9th ed. 1992).

21. *See* J.P. Partsch, *Retorsion, in* 9 ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW 335, 336 (R. Bernhardt ed., 1986).

22. As prescribed in Article 31 of the Vienna Convention on Diplomatic Relations, *supra* note 18, at 112.

23. *See* Part V (Articles 55–75) of the 1982 United Nations Convention on the Law of the Sea, Official Text, 18–27.

24. International Law Commission, Draft Articles on State Responsibility [Article 42(1)], 37 INTERNATIONAL LEGAL MATERIALS 440, 454 (1998).

25. UN CHARTER, *supra* note 2, at 341.

26. *Id.* at 342.

27. It is important to distinguish between the function of the Security Council in recommending appropriate methods of adjustment [under Article 36(1)] and its authority to legally bind Member States to comply with such procedures (or other measures) pursuant to Chapter VII of the Charter (Article 39 *et seq.*). *See* V. Gowlland-Debbas, *Security Council Enforcement Action and Issues of State Responsibility,* 43 INTERNATIONAL AND COMPARATIVE LAW QUARTERLY 55, 83 (1994).

28. The International Law Commission calls reprisals "countermeasures" and subjects them to certain conditions. *See* Articles 47–50 of the Draft Articles, *supra* note 24, at 456–458.

29. *See* O. SCHACHTER, INTERNATIONAL LAW IN THEORY AND PRACTICE 185 (1991).

30. See J.R. Sculley, *Computers, Military Use of,* 2 INTERNATIONAL MILITARY AND DEFENSE ENCYCLOPEDIA 617 (T.N. Dupuy ed., 1993).

31. *See* M.N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework,* 37 COLUMBIA JOURNAL OF TRANSNATIONAL LAW 885, 888 (1999).

32. *See* M.N. Schmitt, *Future War and the Principle of Discrimination,* 28 ISRAEL YEARBOOK ON HUMAN RIGHTS 51, 78 (1998).

33. Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons, 1996, 35 INTERNATIONAL LEGAL MATERIALS 809, 822 (1996).

34. It is noteworthy that nowadays there is less to the distinction than meets the eye, inasmuch as a modern artillery battery is likely to be directed by a computer.

35. The term "terrorists," as used in this paper, includes not only political groups but also crime rings, esoteric cults, and any other violent non-State actors who may acquire the technological capability to engage in a CNA. *See* D.C. Gompert, *National Security in the Information Age,* 51(4) NAVAL WAR COLLEGE REVIEW 22, 33 (1998).

36. Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 4, 22 (merits).

37. *See* R. Ago, *Fourth Report on State Responsibility,* [1972] II YEARBOOK OF THE INTERNATIONAL LAW COMMISSION 71, 120.

38. L. Condorelli, *The Imputability to States of Acts of International Terrorism,* 19 ISRAEL YEARBOOK ON HUMAN RIGHTS 233, 234 (1989).

39. The quotation is from Article 8(a) of the International Law Commission's Draft Articles, *supra* note 24, at 444. *Cf.* G. Townsend, *State Responsibility for Acts of De Facto Agents,* 14 ARIZONA JOURNAL OF INTERNATIONAL AND COMPARATIVE LAW 635, 638 (1997).

40. *Nicaragua* Judgment, *supra* note 3, at 103.

41. *Id.* at 104.

42. *Id.* at 349, 543.

43. International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law Committed in the Territory of the Former Yugoslavia since 1991, Prosecutor v. Dusko Tadič, Appeals Chamber, Case No. IT-94-1-A (July 15, 1999), Judgment, para. 137.

44. *Id.*

45. *See* Q. Wright, *Legal Aspects of the U-2 Incident,* 54 AMERICAN JOURNAL OF INTERNATIONAL LAW 836, 850 (1960).

46. *See* E. Rauch, *Espionage, in* 3 ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW 171, 172 (R. Bernhardt ed., 1982).

47. *See* L.R. Beres, *On International Law and Nuclear Terrorism,* 24 GEORGIA JOURNAL OF INTERNATIONAL AND COMPARATIVE LAW 1, 28 (1994–1995).

48. *See* R.G. Hanseman, *The Realities and Legalities of Information Warfare,* 42 AIR FORCE LAW REVIEW 173, 191–195 (1997).

49. State B may recruit foreign professional "hackers" as mercenaries in its service. For a recent treatment of the intricate topic of mercenaries, see D. Kritsiotis, *Mercenaries and the Privatization of Warfare,* 22(2) FLETCHER FORUM OF WORLD AFFAIRS 11–25 (1998).

50. *See* H.B. Robertson, *The Principle of the Military Objective in the Law of Armed Conflict,* THE LAW OF MILITARY OPERATIONS: LIBER AMICORUM PROFESSOR JACK GRUNAWALT 197–223 (M.N. Schmitt ed. 1998) (Vol. 72, US Naval War College International Law Studies).

51. Barcelona Traction, Light and Power Company, Limited (Second Phase), 1970 I.C.J. 3, 42.

52. "The massively destructive bombings of the [US] embassies in Kenya and Tanzania [in 1998], with a horrific loss of life, were clearly 'armed attacks' that allowed forcible measures of self-defense, even under the most stringent reading of UN Charter requirements." R. Wedgwood, *Responding to Terrorism: The Strikes against Bin Laden,* 24 YALE JOURNAL OF INTERNATIONAL LAW 559, 564 (1999).

53. For international practice confirming that the protection and rescue of nationals abroad is carried out in the exercise of self-defense, see N. RONZITTI, RESCUING NATIONALS ABROAD THROUGH MILITARY COERCION AND INTERVENTION ON GROUNDS OF HUMANITY 30–44 (1985).

54. *See* DINSTEIN, *supra* note 1, at 204–207.

55. For "on-the-spot reaction," see *id.* at 192–194.

56. On this problem, see M.R. Shulman, *Legal Constraints on Information Warfare,* Air War College, Center for Strategy and Technology, Occasional Paper No. 7, at 6 (1999).

57. *See* Advisory Opinion, *supra* note 33, at 823.

58. *See* DINSTEIN, *supra* note 1, at 199–200.

59. The best illustration of a defensive armed reprisal (against State-sponsored terrorism) is the US air-raid on Libyan targets in 1986 (in response to a bomb, which exploded in Berlin, killing two American servicemen and wounding many others). *See* W.V. O'Brien, *Reprisals, Deterrence and Self-Defense in Counterterror Operations,* 30 VIRGINIA JOURNAL OF INTERNATIONAL LAW 421, 463–467 (1989–1990).

60. *See* P.C. JESSUP, A MODERN LAW OF NATIONS 163 (1948).

61. On the difference between State terrorism, State-assisted or State-encouraged terrorism, and State-tolerated terrorism, see S. Sucharitkul, *Terrorism as an International Crime: Questions of Responsibility and Complicity,* 19 ISRAEL YEARBOOK ON HUMAN RIGHTS 247, 256–257 (1989).

62. Wedgwood, *supra* note 52, at 565.

63. For the facts of this famous incident, see R.Y. Jennings, *The Caroline and McLeod Cases,* 32 AMERICAN JOURNAL OF INTERNATIONAL LAW 82, 82–89 (1938).

64. *See* DINSTEIN, *supra* note 1, at 213–221.

65. *See* O. Schachter, *The Lawful Use of Force by a State against Terrorists in Another Country,* 19 ISRAEL YEARBOOK ON HUMAN RIGHTS 209, 228–229 (1989).

66. *Nicaragua* Judgment, *supra* note 3, at 94.

67. Nuclear Weapons Advisory Opinion, supra note 33, at 822.

68. On immediacy, see DINSTEIN, *supra* note 1, at 183–184.

69. L. Stuesser, *Active Defense: State Military Response to International Terrorism,* 17 CALIFORNIA WESTERN INTERNATIONAL LAW JOURNAL 1, 31 (1987–1988).

70. *See* C.A. Fleischhauer, *Negotiation, in* 1 ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW 152, 153 (R. Bernhardt ed., 1981).

71. This was established already in 1928, in the well-known Arbitral Award in the *Naulilaa* case, 2 REPORTS OF INTERNATIONAL ARBITRAL AWARDS 1011, 1028 (French text). For a summary in English, see [1927–1928] ANNUAL DIGEST OF PUBLIC INTERNATIONAL LAW CASES 526, 527.

72. *See* N.M. Feder, *Reading the UN Charter Connotatively: Toward a New Definition of Armed Attack,* 19 NEW YORK UNIVERSITY JOURNAL OF INTERNATIONAL LAW AND POLITICS 395, 415–416 (1986–1987).

73. *See* J.F. Murphy, *Force and Arms, in* 1 UNITED NATIONS LEGAL ORDER 247, 260 (O. Schachter & C.C. Joyner eds., 1995).

74. *See* R. Ago, *Addendum to Eighth Report on State Responsibility,* [1980] II (1) YEARBOOK OF THE INTERNATIONAL LAW COMMISSION 13, 69–70.

75. There is no support in the practice of States for the notion [advocated by J.G. Gardam, *Proportionality and Force in International Law,* 87 AMERICAN JOURNAL OF INTERNATIONAL LAW 391, 404 (1993)] that proportionality remains relevant—and has to be constantly assessed—throughout the hostilities in the course of war.

76. Presumably, this is why R. Ago said in his Report to the International Law Commission that "the action needed to halt and repulse the attack may well have to assume dimensions disproportionate to those of the attack suffered." Ago, *supra* note 74, at 69.

77. *See* DINSTEIN, *supra* note 1, at 208–209.

78. Such confusion is apparent when redundant legitimation is sought for the American and British air campaign against Iraq since December 1998 [*see,* e.g., S.M. Condron, *Justification for Unilateral Action in Response to the Iraqi Threat: A Critical Analysis of Operation Desert Fox,* 161 MILITARY LAW REVIEW 115–180 (1999)]. The Gulf War, which started with an Iraqi armed attack against Kuwait in August 1990, is not over at the time of writing. The cease-fire of 1991 did not terminate the war.

79. K.C. Kenny, *Self-Defence, in* 2 UNITED NATIONS: LAW, POLICIES AND PRACTICE 1162, 1167 (R. Wolfrum ed., 1995).

80. D. Goldstone & B.E. Shave, *International Dimensions of Crimes in Cyberspace,* 22 FORDHAM INTERNATIONAL LAW JOURNAL 1924, 1941 (1998–1999).

81. The Gulf War is a prime example. The invasion of Kuwait by Iraq took place on August 2, 1990. The Security Council authorized the use of "all necessary means" as from January 15, 1991 (namely, after almost half a year). Security Council Resolution 678 (1990), 29 INTERNATIONAL LEGAL MATERIALS 1565, *id.* (1990).

82. For the Kashmir incident, see 45 KEESING'S RECORD OF WORLD EVENTS 42997 (1999).

83. *See* DINSTEIN, *supra* note 1, at 172.

84. *See* T.D. Gill, *The Forcible Protection, Affirmation and Exercise of Rights by States under Contemporary International Law,* 23 NETHERLANDS YEARBOOK OF INTERNATIONAL LAW 105, 111–112 (1992).

85. "Hindsight can be 20/20; decisions at the time may be clouded with the fog of war." G.K. Walker, *Anticipatory Collective Self-Defense in the Charter Era: What the Treaties Have Said,* THE LAW OF MILITARY OPERATIONS, *supra* note 50, at 365, 393. Although the statement is made about

anticipatory action (which is inadmissible in the opinion of the present writer), it is equally applicable to interceptive self-defense.

86. *See* W.G. SHARP, SR., CYBERSPACE AND THE USE OF FORCE 133 (1999).

87. *See* A.D. Softer, *Terrorism, the Law, and the National Defense,* 126 MILITARY LAW REVIEW 89, 98 (1989).

88. *See* J.P. Terry, *An Appraisal of Lawful Military Response to State-Sponsored Terrorism,* 39(3) NAVAL WAR COLLEGE REVIEW 59, 60–61 (1986).

89. That is to say, Greece may respond to an armed attack against Peru. *See* M. AKEHURST, MODERN INTRODUCTION TO INTERNATIONAL LAW 317–318 (P. Malanczuk ed., 7th ed. 1997).

90. *Nicaragua* Judgment, *supra* note 3, at 110.

91. *Id.* at 104.

92. *Id.* at 544–545.

93. On the different categories of collective self-defense treaties, see DINSTEIN, *supra* note 1, at 226–236.

94. North Atlantic Treaty, 1949, 34 UNITED NATIONS TREATY SERIES 243, 246.

95. Nuclear Weapons Advisory Opinion, *supra* note 33, at 822.

96. S.D. BAILEY & S. DAWS, THE PROCEDURE OF THE UN SECURITY COUNCIL 103 (3d ed. 1998).

97. *Nicaragua* Judgment, *supra* note 3, at 121–122.

98. *Id.* at 376–377.

99. *See* O. Schachter, *United Nations Law in the Gulf Conflict,* 85 AMERICAN JOURNAL OF INTERNATIONAL LAW 453, 458 (1991).

100. M. Halberstam, *The Right to Self-Defense Once the Security Council Takes Action,* 17 MICHIGAN JOURNAL OF INTERNATIONAL LAW 229, 248 (1996–1997).

101. *See* N.D. WHITE, KEEPING THE PEACE: THE UNITED NATIONS AND THE MAINTENANCE OF INTERNATIONAL PEACE AND SECURITY 56 (1993).

102. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), 1977, THE LAWS OF ARMED CONFLICTS: A COLLECTION OF CONVENTIONS, RESOLUTIONS AND OTHER DOCUMENTS 621, 645 (D. Schindler & J. Toman eds., 3d ed. 1988).

103. *See* C. Greenwood, *The Law of Weaponry at the Start of the New Millennium,* THE LAW OF ARMED CONFLICT: INTO THE NEXT MILLENNIUM, 185, 231 (M.N. Schmitt and L.C. Green eds., 1998) (Vol. 71, US Naval War College International Law Studies).

VIII

Self-Defense against Computer Network Attack under International Law

Horace B. Robertson, Jr.

In his opening remarks to the Symposium which was the occasion for the current consideration of the international-law constraints on computer network attack (CNA),[1] Vice Admiral A. K. Cebrowski, President of the US Naval War College, asked the conferees, *inter alia*, to pay attention to the question, "Does international law require us to wait until lives are lost or property damaged before we may engage in acts of self-defense?[2] This is a question that has troubled international decision-makers and legal scholars for centuries. It has given rise to numerous and diverse opinions as to the proper threshold for the moment at which a potential victim State may lawfully use armed force to protect itself before the national border has been crossed, or the bombs have begun to fall, or the missiles have been launched. Consideration of this subject has given rise to a number of theories denominated by scholars and others variously as "pre-emptive" strike, "anticipatory self-defense," "interceptive self-defense," and a variety of other terms. Determining the moment when a State may legally take armed defensive action as a matter of self-preservation is difficult enough in the arena of conventional armed attack, where military and political intent may be divined from concrete actions of the alleged aggressor State, such as mobilization of military and economic forces, movement of ground troops and/or air and naval forces, and military exercises which may be regarded as rehearsals for

armed action. But when an attack—i.e., computer network attack—can be initiated without warning and instantaneously by a few computer strokes or clicks of a mouse at a location remote from the target State,[3] determining the threshold criteria is even more difficult. Nevertheless, the harm to a target nation and its infrastructure can be equally or more devastating than if kinetic forces were used. The destruction or impairment of critical networks controlling such activities as domestic air control systems, electrical power systems and grids, national banking systems, etc., even if military command and control networks are unaffected, could cripple a nation's economy and create a public health crisis of immense proportions.

While a leading expert in the field of network security who addressed the symposium assured the participants that a successful penetration of secure systems was not as easy as some alarmists have made it out to be,[4] it is nevertheless generally accepted that a skilled and persistent "hacker" could penetrate and seriously damage many critical infrastructures. Assuming even that such an impending attack could be predicted with reasonable certainty, an issue which will be discussed at a later point in this chapter, the fact that the attack could be conducted by an individual or group that may or may not be a part of the armed forces or otherwise officially connected to a State, raises the additional questions of whether such an attack can be attributed to the State in which the attack is initiated and whether such an attack is an "armed attack" within the accepted meaning of that term. Or is it, in the nomenclature used by Professor Yoram Dinstein, only an "unfriendly act" or an "ordinary breach of international law,"[5] which, under the widely accepted view, does not come within the prohibition of a "threat or use of force" as that term is used in Article 2(4) of the United Nations Charter?[6] Categorization is particularly important in view of Article 51's mandate that authorizes resort to the "inherent" right of self-defense only "if an armed attack occurs against a Member of the United Nations."[7]

The principal paper on the subject of self-defense at the CNA Symposium was given by Professor Dinstein and is published in this commentary under the title, "Computer Network Attacks and Self-Defense."[8] As the moderator of a small group of symposium participants designated to discuss this subject following the presentation of the paper, I was asked to prepare additional comments on the subject. Rather than address all aspects of the doctrine of self-defense against computer network attack that were dealt with in Professor Dinstein's paper and in the small group discussion, I shall primarily focus in this commentary on the discussion which dealt with the issue raised by Admiral Cebrowski in his opening remarks—whether international law requires a State to wait until lives are lost or property damaged before it responds in self-defense. Professor Dinstein

answers this question in the negative by invoking a doctrine which he labels as "interceptive self-defense."[9] This subject provoked the most lively discussion in the small group and revealed substantial differences of opinion among the conferees. In essence, they appeared to be expressions of two schools of thought that find support in the legal literature on this subject. The first of these supports the "strict" interpretation of UN Charter Article 51, which would require that an armed attack have actually taken place before a victim State may respond in self-defense. Professor Dinstein's "interceptive self-defense" is a sub-set of this school, giving it some flexibility of interpretation by allowing counter-action to be taken in advance of the first blow being struck by an analysis of when the armed attack actually begins, that is, when the potential aggressor "embarks upon an irreversible course of action, thereby crossing the Rubicon."[10] The second school asserts that there exists an "inherent" right of self-defense pre-dating the Charter, which continues to exist alongside the law of the Charter, and permits, in some cases, "anticipatory" self-defense when an armed attack may not have actually occurred but, according to objective evidence, is imminent.

The "Strict" School

The intellectual foundation for a "strict" interpretation of Article 51 can be found either in a narrow or literal reading of Article 51 as suggested by a number of eminent authorities or in the interpretation elaborated by Professor Dinstein in his book, *War, Aggression and Self-Defence*, that there was no pre-existing law of self-defense prior to the adoption of the UN Charter, and thus the law of self-defense as expressed in Article 51 is the sole legal basis for exercising this right.

One of the earlier expressions of the narrow or literal reading of Article 51 is found in an article by Professor Josef Kunz, who stated in 1947 that:

> [T]his right [of self-defense under Article 51] does not exist against any form of aggression which does not constitute "armed attack." . . . [T]his term means something that has taken place. Art. 51 prohibits "preventive war." The "threat of aggression" does not justify self-defense under Art. 51. . . . The "imminent" armed attack does not suffice under Art. 51.[11]

Dr. Djura Nincic makes a similar argument, stating:

> [N]othing less than an armed attack shall constitute an *act-condition* for the exercise of the right of self-defense within the meaning of Article 51 . . . . It further

> stipulates that *the armed attack must precede the exercise of the right of self-defense*, that only an armed attack which has actually materialized, which has "occurred" shall warrant a resort to self-defense. This clearly and explicitly rules out the permissibility of any "anticipatory" exercise of the right of self-defense, i.e., resort to armed force "in anticipation" of an armed attack.[12]

Other adherents of this view include Hans Kelsen,[13] Louis Henkin,[14] Ian Brownlie,[15] Hersch Lauterpacht,[16] Andrew Martin,[17] and Robert Tucker.[18]

Professor Randelzhofer, who authored the Chapters on Articles 2(4) and 51 in Simma's exhaustive exegesis on the UN Charter,[19] also adopts, as the "prevailing view," the strict interpretation ascribed to the aforementioned scholars.[20] With respect to the specific question of whether a State has a right of anticipatory self-defense, he acknowledges that "[t]here is no consensus in international legal doctrine over the point."[21] But he goes on to conclude that "Art. 51 has to be interpreted narrowly as containing a prohibition of anticipatory self-defence. Self-defence is thus permissible *only after the armed attack has already been launched.*"[22] His rationale for this conclusion is that since

> the (alleged) imminence of an attack cannot usually be assessed by means of objective criteria, any decision on this point would necessarily have to be left to the discretion of the state concerned. The manifest risk of an abuse of that discretion which thus emerges would *de facto* undermine the restriction to one particular case of the right of self-defence.[23]

Professor Dinstein also adheres to the view that a literal interpretation of Article 51 is required, arguing, in essence, that a right of self-defense exists if, and only if, an armed attack occurs.[24] He reaches that conclusion by a different route, however. In *War, Aggression and Self-Defence*, he argues, in effect, that there was no legally-recognized right of national self-defense prior to the adoption of the UN Charter. In support of that view he states:

> From the dawn of international law, writers sought to apply this [domestic law] concept [of self-defense] to inter-State relations, particularly in connection with the just war doctrine. . . . But when the freedom to wage war was countenanced without reservation (in the nineteenth and early twentieth centuries), concern with the issue of self-defence was largely a metajuridical exercise. As long as recourse to war was considered free for all, against all, for any reason on earth—including territorial expansion or even motives of prestige and grandeur—States did not need a legal justification to commence hostilities. The

> plea of self-defence was relevant to the legality of forcible measures short of war, such as extra-territorial law enforcement . . . . Still, logically as well as legally, it had no role to play in the international arena as regards the cardinal issue of war. Up to the point of the prohibition of war [i.e., adoption of the UN Charter], to most intents and purposes, "self-defence was not a legal concept but merely a political excuse for the use of force."[25]

Further developing this theme, Professor Dinstein argues that the right of self-defense cannot be justified under either natural law or as an element of the sovereignty of States. With respect to the natural law he states:

> [A] reference to self-defence as a "natural right", or a right generated by "natural law", is unwarranted. It may be conceived as an anachronistic residue from an era in which international law was dominated by ecclesiastical doctrines.[26]

With respect to reliance on the principle of sovereignty as a basis for an "inherent" right of self-defense, he acknowledges that the series of identical American notes accompanying the invitations to a number of States to become parties to the Kellogg-Briand Pact lends some support to that theory. Those notes stated, *inter alia*, that the right of self-defense "is inherent in every sovereign state and is implicit in every treaty."[27] Professor Dinstein states, however, that:

> [T]he principle of State sovereignty sheds no light on the theme of self-defence. State sovereignty has a variable content, which depends on the stage of development of the international legal order at any given moment. The best index of the altered perception of sovereignty is that, in the nineteenth (and early twentieth) century, the liberty of every State to go to war as and when it pleased was also considered "a right inherent in sovereignty itself" . . . . Notwithstanding the abolition of this liberty in the last half-century, the sovereignty of States did not crumble. The contemporary right to employ inter-State force in self-defence is no more "inherent" in sovereignty than the discredited right to resort to force at all times.[28]

While it is clear from Professor Dinstein's analysis that he regards a State's right of self-defense not to be activated until an armed attack actually occurs, he avoids the catastrophic consequences that might result from such a rigid doctrine by walking back the time that an attack actually begins to the point where the incipient attacker "embarks upon an irreversible course of action, thereby

crossing the Rubicon."[29] He labels this as "interceptive" self-defense, which he distinguishes from "anticipatory" self-defense in that it requires that the other side "has committed itself to an armed attack in an ostensibly irrevocable way," rather than that the attack is merely "foreseeable."[30]

While it is true that the self-defense doctrine owes its origin to theological and natural-law sources, which were the foundations of the concept of the "just war,"[31] and while Professor Dinstein is undoubtedly correct that during the positivist era of the 19th and early 20th centuries, any State was free to make war as an element of sovereignty, States nonetheless often continued to plead self-defense as a legal as well as a political or moral justification. This practice was more than a vestigial remnant of ecclesiastical law. States regarded it as inherent in their statehood; it is therefore not surprising that the term "inherent" found its way into Article 51 of the Charter.

Although Professor Randelzhofer states that the literal or strict interpretation of Article 51 with its denunciation of anticipatory self-defense is the "prevailing view" among recognized scholars, he nevertheless admits that there is substantial scholarly opinion *contra*. He states:

> There is no consensus in international legal doctrine over the point in time from which measures of self-defence against an armed attack may be taken. Thus, in particular those authors who interpret Art. 51 as merely confirming the pre-existing right of self-defence consider anticipatory measures of self-defence to be admissible under the conditions set up by Webster in the *Caroline* case, i.e. when "the necessity of that self-defence is instant, overwhelming and leaving no choice of means, and no moment for deliberation."[32]

The adherents of this opposing view are both numerous and distinguished. They include, among others, such publicists as Oscar Schachter, Myres McDougal, Robert Jennings, Humphrey Waldock, and Antonio Cassese.

Sir Humphrey Waldock was one of the earliest critics of the highly restrictive interpretation of Article 51 by the literalists. In his Hague lectures of 1952, Sir Humphrey stated:

> If an armed attack is imminent within the strict doctrine of the Caroline, then it would seem to bring the case within Article 51. To read Article 51 otherwise is to protect the aggressor's right to the first stroke. To cut down the customary right of self-defense beyond even the *Caroline* doctrine does not make sense in times when the speed and power of weapons of attack has enormously increased.[33]

Professor Myres McDougal and Florentino Feliciano, focusing primarily on the Kunz and Nincic readings of the Charter text, argue that the objections to such readings are twofold. First, Kunz and Nincic attempt to interpret the meaning of the text from an analysis of the words alone, attempting to divine a single clear and unambiguous meaning, and Kunz, in addition, "casually de-emphasize[s]" the preparatory work on the document. The second major flaw in their argument is that they seriously underestimate the potentialities of modern military weapons systems and the contemporary techniques of non-military coercion.[34]

With respect to arguments that allowing a State to respond in an anticipatory manner would vest too much discretion in individual States, McDougal and Feliciano point out that the claim to the right of self-defense "remains subject to the reviewing authority of the organized community."[35]

One of the more cogent criticisms of the conclusions reached by the literalists was made by Professor David Linnan in a recent article in which he applied the interpretive principles of the Vienna Convention on the Law of Treaties to an interpretation of Article 51 of the Charter. He states:

> Under the Vienna Convention, the textual exegesis or ordinary meaning approach enjoys primacy in the absence of inherent ambiguity or manifestly absurd result. Publicists employing the ordinary meaning approach, but dismissing Article 51's inherent right-*droit naturel* language as mere infelicitous drafting (viewing the natural law approach as generally discredited) violate its most basic canon. . . . [U]nder an ordinary meaning approach the use of the natural law terminology indicates the adoption by reference of its scheme of self-defense (without reaching or expressing an opinion on the validity of the natural law approach itself, which is a national view of international law not shared by all states). Regarding the scheme of self-defense adopted, U.S. views expressed in the notes accompanying the Kellogg-Briand Pact are representative.[36]

Professor Linnan goes on to argue that if, however, the use of the term "inherent right" creates an ambiguity, it brings into play the secondary rule of interpretation, which authorizes resort to supplementary materials under Article 32 of the Vienna Convention, at which point the "legislative history" of Article 51 comes to the fore. As he and many other publicists have pointed out,[37] the drafting history shows clearly that Article 51 was inserted to clarify the point that the new Security Council system would not displace contemporaneous efforts involving the creation of regional security systems.[38]

But international law is not just a creature of treaty text. It is at least equally a product of State practice. Analyzing State practice since the adoption of the

Charter, Sir Robert Jennings and Sir Arthur Watts, while cautioning that anticipatory self-defense should be regarded as unlawful under most circumstances, state that:

> [I]t is not necessarily unlawful in all circumstances, the matter depending on the facts of the situation including in particular the seriousness of the threat and the degree to which pre-emptive action is really necessary and is the only way of avoiding that serious threat.[39]

Proceeding on that basis, they conclude:

> The development of the law, particularly in the light of more recent state practice, in the 150 years since the *Caroline* incident, suggests that action, even if it involves the use of armed force and the violation of another state's territory, can be justified as self-defence under international law where (a) an armed attack is launched *or is immediately threatened*, against a state's territory or forces (and probably its nationals); (b) there is an urgent necessity for defensive action against that attack; (c) there is no practicable alternative to action in self-defence . . .; (d) the action taken by way of self-defence is limited to what is necessary to stop or prevent the infringement, i.e., to the needs of defence; and (e) in the case of collective self-defence, the victim of an armed attack has requested assistance.[40]

The severe restraints that Jennings and Watts would apply to the exercise of "anticipatory" self-defense reflect their concern that the right could be abused with enormously serious consequences. Professor Rosalyn Higgins has expressed the same concern. She has contrasted two cases in which Israel asserted this doctrine to justify resort to pre-emptive strikes to illustrate her view of what may or may not constitute a justified anticipatory exercise of the right of self-defense. The first was the Six Days War of 1967. Recall the events leading up to Israel's pre-emptory attack: President Nasser summarily ejected the UN Emergency Force from Sinai and the Gaza strip; he closed the Straits of Tiran, a vital seaway link for Israel to the outside world; both Syria and Egypt massed troops on Israel's border; and Syria and Egypt unleashed a barrage of bellicose statements. As Professor Higgins points out, neither the UN Security Council nor the UN General Assembly condemned Israel's action. On the contrary, there was a general feeling, "certainly shared by the Western states, that taken in context, this was a lawful use of anticipatory self-defence."[41] The second case was that of the Israeli air strike against the Iraqi nuclear reactor in 1981.

There, the Security Council, with the concurrence of the United States and the Common Market's "Group of Ten," "*strongly condemn[ed]*" Israel's actions.[42] Not only was the *building* of a nuclear reactor not a *use* of force; the timing of the strike lacked the temporal element of urgency required by the *Caroline* criteria.[43]

Professor Cassese, in the same collection of essays, agrees with Professor Higgins and, in addition, appears to go further by relaxing somewhat the rigorous criteria of the *Caroline* case.

> One might perhaps draw the conclusion that consensus is now emerging that under Art. 51 anticipatory self-defence is allowed, but on the strict conditions that (i) solid and consistent evidence exists that another country is about to engage on a large-scale armed attack jeopardizing the very life of the target State and (ii) no peaceful means of preventing such attack are available either because they would certainly prove useless to the specific circumstances, or for lack of time to resort to them, or because they have been exhausted.[44]

One of the most vocal critics of the strict interpretation theory has been the late Professor McDougal. He urged that in the age of the ballistic missile, to postpone action in self-defense until after the "last irrevocable act" reduces the right of self-defense to a right of retaliatory response.

> It is precisely this probable effect that gives to the narrowly restrictive construction of Article 51, when appraised for future application, a strong air of romanticism.[45]

Professor Schachter has written on the subject of self-defense on several occasions. While his writings reflect a profound commitment to the principles of Article 2(4) of the UN Charter, he nevertheless concludes that Article 51 cannot be so narrowly construed as to require a State to forego the right to respond when, based on persuasive evidence, an attack appears imminent. As he stated most eloquently in 1986:

> On the level of principle, it makes sense to support a norm that opposes the preemptive resort to force but acknowledges its necessity when an attack is so immediate and massive as to make it absurd to demand that the target state await the actual attack before taking defensive action. Webster's statement in the *Caroline* case is probably the only acceptable formulation at the present time to meet this situation.[46]

Finally, one must consider the judgment of the International Court of Justice in the *Nicaragua* case, as well as Judge Schwebel's dissenting opinion. In the jurisdictional phase of the case, the United States had argued that its multilateral treaty reservation divested the court of jurisdiction since the customary law of self-defense had been "subsumed" or "supervened" by treaty law, that is, Article 51 of the Charter. At that stage, the Court, in refusing to dismiss the case, stated:

> The fact that the above-mentioned principles [including *inter alia* the principle of self-defense] . . . have been codified or embodied in multilateral conventions does not mean that they cease to exist and to apply as principles of customary law, even as regards countries that are parties to such conventions.[47]

During the Merits stage, the Court further concluded that even if the customary law and treaty principles were identical in content, the customary-law rule may apply separately and independently.[48] Since, however, the parties to the case placed their reliance as to the applicability of the right of self-defense only on the case of an armed attack which had already occurred, the issue of the lawfulness of an armed response to an imminent threat of attack was not raised nor addressed by the majority opinion.[49]

Judge Schwebel, in his dissent, while also acknowledging that the issue was not before the Court, and while recognizing that "the issue is controversial and open to more than one substantial view," opined, *ex abundi cautela*, that he disagreed with a construction of Article 51 as if it read, "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if, and only if, an armed attack occurs."[50]

While the foregoing discussion admittedly constitutes only a partial review of the many scholarly writings on the use of force and the right of self-defense, I believe it constitutes a fair representation of the various positions taken by the leading commentators who have addressed this issue. From this review it would appear safe to conclude that there is a deep division between those who argue for a literal interpretation of Article 51 and those who argue that such an interpretation is inconsistent with the true meaning of the Article, particularly in the post-nuclear age. To conclude that one view or the other is the "prevailing" view, as Randelzhofer has done, is, I believe, too strong a conclusion to draw given the number and eminence of the scholars that are represented in the opposing camp.

In view of the foregoing, I do not consider it to be unreasonable that the United States takes the position that anticipatory self-defense against an

imminent attack is permitted under Article 51. This position is articulated in the relevant military operational manuals and in the Joint Chiefs of Staff (JCS) Standing Rules of Engagement. The Navy's Manual, for example, provides as follows:

> Anticipatory Self-Defense. Included within the inherent right of self-defense is the right of a nation (and its armed forces) to protect itself from imminent attack. International law recognizes that it would be contrary to the purposes of the United Nations Charter if a threatened nation were required to absorb an aggressor's initial and potentially crippling first strike before taking those military measures necessary to thwart an imminent attack. *Anticipatory self-defense involves the use of armed force where attack is imminent and no reasonable choice of peaceful means is available.*[51]

The JCS Standing Rules of Engagement authorize the exercise of the right of anticipatory self-defense against forces displaying "hostile intent," which is defined, *inter alia*, as follows:

> **Hostile Intent**. The threat of imminent use of force against the United States, US forces, and in some circumstances, US nationals, their property, US commercial assets, and/or other designated non-US forces, foreign nationals and their property.[52]

Having concluded that it would not be unreasonable for a State to take the position that anticipatory self-defense against an imminent armed attack is lawful, and having found that the United States has adopted this position, the question remains as to what are the criteria for determining when an attack is "imminent." The classic formulation is US Secretary of State Daniel Webster's dictum that an armed response is lawful when the necessity of action is "instant, overwhelming, and leaving no choice of means, and no moment for deliberation."[53] This is the test adopted by many eminent scholars and has been repeated often in legal and diplomatic arguments. It was adopted in the US Navy's operational manual prior to its current iteration.[54] A number of scholars have concluded, however, that this articulation is much too restrictive in the present age, particularly in the light of the possibility of devastating nuclear attack. McDougal and Feliciano have stated, for example, that:

> [T]he standard of required necessity has been habitually cast in language so abstractly restrictive as almost, if read literally, to impose paralysis.[55]

In their own extensive analysis of the required degree of necessity, McDougal and Feliciano are unable to provide tests that are less abstract, finally concluding that the requirement of necessity "can only be subjected to that most comprehensive and fundamental test of all law, reasonableness in particular context."[56] Analyzing the particular context of the Cuban Missile Crisis of 1962, Professor McDougal concluded that the US quarantine of Cuba was a lawful application of the doctrine of self-defense.[57] Central to his analysis was that the United States' action was an exercise of "initial discretion," which was then backed up by mustering the support of the members of the Organization of American States and reporting its action to the Security Council.[58]

Sally and Thomas Mallison have analyzed the criteria for the lawful employment of self-defense against an imminent armed attack in several of their writings, most recently in volume 64 of the Naval War College's "Blue Book" series (1991), where they, like McDougal and Feliciano, concluded that the Webster formulation was too restrictive, "since a credible threat may be imminent without being 'instant' and more than a 'moment for deliberation' is required to make a lawful choice of means."[59] Like McDougal and Feliciano, they also assert that whether an anticipatory resort to armed force in self-defense is lawful can only be determined in the context of the facts of the specific case.[60] They emphasize that where anticipatory self-defense is claimed, the criteria for lawfulness must be applied with greater stringency than when an actual attack has occurred.[61]

Computer Network Attacks as "Armed Attacks"

It is important that what is under discussion here is not what may be lawful in an ongoing armed conflict (*jus in bello*) but rather actions by a hostile individual, group, or State against another State while the target State and the State of origin of the actions are not yet engaged in armed conflict (*jus ad bellum*). In an ongoing armed conflict (war), it is unquestionably legitimate for a State to attack its enemy's military telecommunications infrastructure, including military computer networks.[62] Attacks on other telecommunications and network facilities which serve both military and civilian clientele may also be legitimate military objectives, provided that the international humanitarian law of armed conflict is observed with respect to proportionality, including limiting collateral damage.[63] It is a matter of indifference whether the mode of attack is kinetic or electronic, although the former may be more objectionable since it is more destructive and may cause more long-lasting effects.

In examining whether a computer network "attack" may constitute an "armed attack," Article 51 cannot be construed in isolation but rather must be read in the context of other articles of the Charter, particularly Articles 2(4), 39, 41 and 42. Article 2(4) provides:

> All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.

Article 39 empowers the Security Council to determine the existence of "any threat to the peace, breach of the peace, or act of aggression" and to make recommendations or decide on "measures" to be employed under Article 41 or Article 42. Article 41 provides a non-exhaustive list of measures "not involving the use of armed force" which the Security Council may take including "complete or partial interruption of . . . telegraphic, radio, and other means of communication." Article 42, in turn, provides for actions "by air, sea, or land forces" when the measures provided for in Article 41 are inadequate. Since the actions in Article 41 are described as "measures not involving the use of armed force,"[64] whereas those in Article 42 involve the use of armed forces, it would appear that, at least as an initial presumption, a computer network attack would not be regarded as an "armed attack." Giving effect to such an initial presumption, however, ignores the significance of the drastic consequences that such an attack can have on the social, economic and military structure of a State. As will be discussed *infra*, whether an attack is to be considered as an armed attack depends on the consequences of the attack rather than the modality.

The various terms used in the Charter, including the Preamble—"war" (Preamble), "armed force" (Preamble), "acts of aggression" (Article 1), "threat or use of force" (Article 2(4)), "act of aggression (Article 39), and "armed attack" (Article 51)—differ in scope and content. Though related in content "they differ considerably in their meaning."[65] None of them is further explained in the Charter.

This lack of definition has led to several attempts, primarily by the General Assembly, to give further content to the terms, particularly "act of aggression." Article 3 of the 1974 General Assembly's "Definition of Aggression" Resolution provides the following non-exhaustive list of acts which qualify as acts of aggression:

> (a) The invasion or attack by the armed forces of a State of the territory of another State, or any military occupation, however temporary, resulting from such

invasion or attack, or any annexation by the use of force of the territory of another State or part thereof;

(b) Bombardment by the armed forces of a State against the territory of another State or the use of any weapons by a State against the territory of another State;

(c) The blockade of the ports or coasts of a State by the armed forces of another State;

(d) An attack by the armed forces of a State of the land, sea or air forces, marine and air fleets of another State;

(e) The use of armed forces of one State, which are within the territory of another State with the agreement of the receiving State, in contravention of the conditions provided for in the agreement or any extension of their presence in such territory beyond the termination of the agreement;

(f) The action of a State in allowing its territory, which it has placed at the disposal of another State, to be used by that other State for perpetrating an act of aggression against a third State;

(g) The sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to the acts listed above, or its substantial involvement therein.[66]

While the term "act of aggression" is broader than "armed attack," it is apparent that most of the acts listed in the General Assembly's resolution would also constitute an "armed attack" and would, if of sufficient scale and effect, invoke the victim's right to respond under its right of self-defense.

As several recent articles and monographs have revealed, analyzing the novel and still-developing concept of computer network attack under either the customary law of self-defense or Article 51 of the Charter presents both theoretical and practical difficulties.[67] The principal difficulty flows from the fact that both traditionally and under the Charter, the discussion and codification of what constitutes an act of aggression or an armed attack generally involve the use of *armed* force—either in the form of employment of military weapons or hostile acts by members of the armed forces. It is now clear that the "armed force" involved does not have to be a part of the organized military forces of a State. As indicated above, the General Assembly's "Definition of Aggression"

Resolution, after listing certain acts involving the "armed forces of a State," also includes, as an act of aggression, the sending by or on behalf of a State of "armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State" or the substantial involvement of a State in such actions provided they reach a certain level of gravity.[68] The judgment of the International Court of Justice in the *Nicaragua* case likewise held that the "arming and training of the *contras* [by the United States] can certainly be said to involve the threat or use of force against Nicaragua."[69] It also held, however, that the "mere supply of funds . . . does not in itself amount to a use of force."[70]

Those publicists who have grappled with the problem of determining when a computer network attack constitutes an armed attack, have two possible avenues of approach–either the instrumentality or the consequences test. Nearly 40 years ago, Professor McDougal and Mr. Feliciano, though not visualizing cyber warfare, were critical of focusing on the instrumentality as the "precipitating event" for lawful self-defense, stating that to do so

> is in effect to suppose that in no possible context can applications of nonmilitary types of coercion (where armed force is kept to a background role) take on efficacy, intensity, and proportions comparable to those of an "armed attack" and thus present an analogous condition of necessity. Apart from the extreme difficulty of establishing realistic factual bases for that supposition, the conclusion places too great a strain upon the single secondary factor of modality–military violence.[71]

Michael Schmitt points out, however, that:

> At least since the promulgation of the Charter, [the] use of force paradigm has been instrument-based; determination of whether or not the standard has been breached depends on the type of the coercive *instrument*–diplomatic, economic, or military–selected to attain the national objectives in question. The first two type of instruments might rise to the level of intervention, but they do not engage the normatively more flagrant act of using force.[72]

While admitting that an instrument-based approach provides a relatively easily-applied test for calculating lawfulness of an act of intervention,[73] he ultimately concludes that it does not provide a useful test for computer network attack.

> Computer network attack challenges the prevailing paradigm, for its consequences cannot easily be placed in a particular area along the community

> values threat continuum. The dilemma lies in the fact that CNA spans the spectrum of consequentiality. Its effects freely range from mere inconvenience (e.g., shutting an academic network temporarily) to physical destruction (e.g., as in creating a hammering phenomenon in oil pipelines so as to cause them to burst) to death (e.g., shutting down power to a hospital with no back-up generators). It can affect economic, social, mental, and physical well-being, either directly or indirectly, and its potential scope grows almost daily, being capable of targeting everything from individual persons or objects to entire societies.[74]

Professor Schmitt recognizes, however, the weakness of a system of analysis which attempts to apply a system developed to regulate kinetic activities to account for non-kinetically based harm.[75] He calls for a new normative architecture.[76] Recognizing also, however, that there is no current consensus as to the need for developing such an architecture, he articulates an "appropriate normative framework"[77] under current international law as framed within the UN Charter, that relies on the "consequences" theory.

> To constitute an armed attack, the CNA must be intended to directly cause physical damage to tangible objects or injury to human beings. . . . States, acting individually or collectively, may respond to a CNA amounting to armed attack with the use of force pursuant to Article 51 and the inherent right of self-defense.[78]

The Institute for National Strategic Studies of the National Defense University has also adopted a "consequences" test as to whether a CNA rises to the level of an armed attack, stating:

> [I]t appears likely that an "armed attack" would include some level of actual or potential physical destruction, combined with some level of intrusion into its target's borders, or violation of its sovereign rights. . . . [A]ttacks that are sufficiently destructive may qualify as "armed attacks," no matter what their level of intrusion, and vice versa.[79]

Likewise, Professor Dinstein adopts a consequences test. He offers as examples of CNAs that would constitute armed attacks the following:

> Fatalities caused by loss of computer-controlled life-support systems; an extensive power grid outage (electricity blackout) creating considerable deleterious

> repercussions; a shutdown of computers controlling waterworks and dams, generating thereby floods of inhabited areas; deadly crashes deliberately engineered (e.g., through misinformation fed into aircraft computers), etc. The most egregious case is the wanton instigation of a core-meltdown of a reactor in a nuclear plant, leading to the release of radioactive materials that can cause countless casualties if the neighboring areas are densely populated. In all these cases, the CNA would be deemed an armed attack.[80]

Walter Gary Sharp, Sr., would lower the threshold substantially.

> [T]he mere penetration by a state into sensitive computer systems such as early warning or command and control systems, missile defense computer systems, and other computers that maintain the safety and reliability of a nuclear stockpile, should by their very nature be presumed a demonstration of hostile intent. Individually, these computer systems are so important to a state's ability to defend itself that espionage into any one of them should be presumed to demonstrate hostile intent.[81]

It is to be recalled that under the JCS Standing Rules of Engagement, demonstration of a hostile intent is the determinant for permitting an armed response to an imminent armed attack.[82] Invoking such a low threshold for triggering the right to respond by armed force in self-defense seems to be establishing a dangerous standard, especially when it is often difficult to determine whether a computer network attack has occurred at all. In some instances, malfunctions which appear at first to be the result of computer network attack have been determined, after more thorough investigation, to be the result of faulty software or operator error.[83]

If one agrees that computer network attacks of some degree of severity and under some circumstances may constitute "armed attacks," then one must apply some criteria for determining when such attacks cross the threshold from interventions that do not warrant responses under the right of self-defense to those that do. As has been mentioned, the closest the UN Charter itself comes to describing anything remotely resembling CNA is in Article 41, where it lists "complete or partial interruption . . . of telegraphic, radio, and other means of communication" as a measure "not involving the use of armed force" which the Security Council may take against threats to the peace, breaches of peace, or acts of aggression.[84] Presumptively, computer networks would fall under a broad definition of "telegraphic, radio, and other means of communication," but in today's environment of almost total dependence on

the proper functioning of computer networks for control of vital societal functions, as well as critical national-security systems, the "complete or partial interruption" of such systems would have a much more drastic effect than anything that could have been envisaged by the framers of the Charter in 1945. Article 41, therefore, cannot be said to require the categorization of computer network attacks as actions "not involving the use of armed force." As Professor Schmitt has suggested, it would be desirable for a normative architecture specifically tailored to CNA to emerge. For the present, however, until a consensus develops for the need for a new normative architecture, it would appear that the most rational and practical test of whether a computer attack can be the precipitating event for the exercise of lawful self-defense is whether the consequences are major damage to or destruction of vital military or civilian infrastructures or the loss of human life.

Anticipatory Self-Defense against Computer Network Attack

As discussed earlier, there is substantial legal support for the proposition that where there is persuasive evidence that an armed attack is imminent, the potential victim State is not required to stand idly by until the actual attack has occurred—it may respond with proportional force to ward off the attack. The difficulty with the application of this principle is in determining that in fact an attack is imminent. In the case of an attack by kinetic means, there are usually (but certainly not always) intimations of an impending attack. Some may be ambiguous, such as a step-up in propaganda or bellicose statements; others may carry a clearer threat—movement of troops to the border, mobilization of forces, increased aerial and electronic surveillance, deployment of naval and air forces, and clandestine infiltration of intelligence agents. While a computer network attack may also be preceded by acts that suggest an attack is imminent (or it may itself be a part of the pre-attack build-up for an attack by kinetic means), the capability of an attacker to cause almost instantaneous harm suggests that the first notice that a victim State may have that a computer network attack is underway is to experience the harmful effects themselves. If the consequence of the CNA is serious harm to vital infrastructure or loss of human life, then under the principles previously discussed, a proportional response is lawful. But difficult questions remain. Response against whom? Can the attacker be identified? The originator of the attack may have sent his electronic attack through multiple switches and servers in several different countries. Is the attacker acting on behalf of a foreign government, or is he merely a teen-age "hacker" engaged in what is to him a prank?[85] If the hacker is not a direct agent of a foreign government, is

the foreign government aware of his actions and impliedly consenting to them? The permutations and combinations of situations under which attacks may occur number in the millions. Professor Schmitt has reported that today over 120 countries are in the process of establishing information warfare competence[86] and by the year 2002 some "nineteen million individuals will have the know-how to launch cyber attacks."[87]

Obviously, not every probing of a presumably secure network, whether one controlling vital civilian infrastructure or a military network controlling critical defense functions, such as air defense, atomic weapons, satellite communications, or intelligence gathering, can be considered as a prelude to a full-scale network attack. Professor Schmitt has reported that the Defense Information Systems Agency identified 53 attacks on defense systems in 1992.[88] By 1995 the number had increased to 559 and was expected to reach 14,000 in 1999.[89] Figures supplied by the Defense Information Systems Agency reports are even more unsettling. That agency reported that the Defense Department may have experienced as many as 250,000 attacks in 1994.[90] Although each of these "attacks" required investigation and appropriate action, none of them presumably were of sufficient gravity either to indicate that they were themselves an "armed attack" that would have authorized a resort to armed force in response nor were they regarded as indicators that such an armed attack was imminent.

It would seem, then, that the most likely application of the doctrine of anticipatory self-defense to computer network attacks would be in the case of such attacks that in and of themselves do not constitute an armed attack but rather are evaluated as precursors of an armed attack by kinetic means and/or further, more severe cyber attacks. In modern warfare, the electronic battlefield will play a crucial role, and any steps that a prospective attacker can take to neutralize or destroy its enemy's electronic command and control, intelligence, communications, or weapons-control networks prior to a kinetic attack would gain enormous advantage. While these preliminary CNAs may not themselves rise to the level of armed attack, they may, if combined with other evidence of an impending attack, be sufficient to authorize armed measures of self-defense—not against the CNAs themselves, but rather as an exercise of the right of anticipatory self-defense against the impending kinetic or more serious cyber attack.

Professor Schmitt, who also visualizes the most likely scenario to be the use of CNA to soften up the battlespace,[91] proposes a three-prong test for determining when a State may respond to a CNA that itself does not constitute an armed attack.

1. The CNA is part of an overall operation culminating in armed attack;

2. The CNA is an irrevocable step in an imminent (near-term) and probably unavoidable attack; and

3. The defender is reacting in advance of the attack itself during the last possible window of opportunity available to effectively counter the attack.[92]

This formulation appears to be an application of Secretary Webster's dictum in the *Caroline* case, adapted to computer network attack. As we have seen, the *Caroline* standard has been found by many publicists to be too narrowly drawn to apply in all circumstances. "The last possible window" may be too late to avoid catastrophic results. The problem does not lend itself to a specific formula. I suggest that whatever the formula used, in the final analysis, the decision maker must apply "that most comprehensive and fundamental test of all law, reasonableness in particular context."[93]

Concluding Remarks

In this chapter I have attempted to defend the proposition that a State's right to exercise its "inherent" right of self-defense by armed force is not limited to the situation in which an attack has actually occurred, but may also apply when a State has persuasive evidence that such an attack is imminent (anticipatory self-defense). The State exercising the right of *anticipatory* self-defense, however, bears a heavy burden of proof that the evidence upon which it acted was indeed persuasive and must withstand *ex post facto* examination by the international community, primarily through the Security Council. I have also attempted to demonstrate that the term "armed attack" may also include attacks upon computer networks solely by electronic means if the *consequences* of such attacks include either substantial harm to vital civil or military networks, or loss of human life, or both. Although the first of these propositions is admittedly controversial, and some have labeled it a minority view, I believe that there is distinguished scholarly support for that position, as well as substantial support in State practice. The adoption of this position by the United States, as reflected in its military manuals and Standing Rules of Engagement is therefore justifiable. As to the second proposition, that is, that the test of whether an action constitutes an armed attack is the consequence of the attack, there does not seem to be any other choice, since an instrumentality-based criterion is wholly impractical in view of the capability of an innocuous instrument—the computer—to become

a lethal weapon in the hands of a skilled and persistent "hacker" determined to invade and attack another's computer network.

When I attempt to apply the doctrine of anticipatory self-defense to computer network attack, I find myself in waters difficult to navigate. The most likely scenario for CNA is that it will occur suddenly, without warning. It also seems likely that a true hostile CNA reaching the level of an "armed attack" will not be an isolated incident, but rather will occur as part of the preliminary softening-up of the battlespace preceding an attack by kinetic weapons or a more serious cyber attack. Professor Schmitt apparently visualizes this same scenario since he shifts the focus of his section on anticipatory self-defense to use of "computer network attack operations executed to prepare the battlespace."[94] Under these circumstances, it becomes even more important for a State facing what may appear to be an imminent CNA carefully to utilize all its resources in its analysis of all the surrounding events, political and military, to aid in its determination of whether an armed response may be made under the right of self-defense. Only in this way can it meet its heavy burden of establishing the justification for initiating the first resort to the use of armed force.

Notes

1. US Naval War College Symposium, Computer Network "Attack" and International Law, convened at the Naval War College, Newport, Rhode Island, June 22–25, 1999.

2. Vice Admiral A. K. Cebrowski, USN, CNE and CNA in the Network Centric Battlespace: Challenges for Operators and Lawyers, Welcoming Address to the Conferees, June 22, 1999.

3. Michael E. Ruane, *New Computer Technology Makes Hacking A Snap*, WASHINGTON POST, March 10, 1999, at 1.

4. Remarks of Dr. Mark Gembicki, Chief Technical Officer of WarRoom Research, Inc., to the Symposium, June 22, 1999.

5. Yoram Dinstein, *Computer Network Attacks and Self-Defense*, published in this volume.

6. UN CHARTER, art. 2, para. 4.

7. *Id.*, art. 51. As we shall discuss later, the meaning of the term "armed attack" is not identical with the term "threat or use of force" used in Art. 2, para. 4.

8. Dinstein, *supra* note 5.

9. *Id.* Professor Dinstein has elaborated this doctrine more fully in his book, WAR, AGGRESSION AND SELF-DEFENCE 172–173 (3d ed. 2001) [hereinafter DINSTEIN].

10. DINSTEIN, *supra* note 9, at 172.

11. Josef L. Kunz, *Individual and Collective Defense in Article 51 of the Charter of the United Nations*, 41 AMERICAN JOURNAL OF INTERNATIONAL LAW, 872, 878 (1947). It is interesting to note that Professor Kunz's literal interpretation of Article 51 leads him to conclude that the language of the article, which codifies the one requirement of necessity ("armed attack") frees the defending State from the requirements of reasonableness and proportionality, which, along with "immediacy," have traditionally been regarded as requirements for the exercise of the right in both domestic and international law. He even suggests that a minor border incident would justify a full-scale war. *Id.* at 876, 878.

12. Djura Nincic, *Reply, in* International Law Association Committee on the Charter of the United Nations, Report on Some Aspects of the Principle of Self-Defense in the Charter of the United Nations and The Topics Covered by the Dubrovnik Resolution 68 (Georg Schwarzenberger ed., 1958) (emphasis in original).

13. HANS KELSEN, THE LAW OF THE UNITED NATIONS 797 (1950) ("It is of importance to note that Article 51 does not use the term 'aggression' but the much narrower concept of 'armed attack,' which means that a merely 'imminent attack' or act of aggression which has not the character of an attack involving the use of armed force does not justify resort to force as an exercise of the right established by Article 51" (emphasis supplied). Kelsen reiterates this view in the supplement to the 4th printing of his book in 1956. It should also be noted that Kelsen states that the inclusion of the word "inherent" in Article 51 is a superfluity. "The effect of Article 51 would not change if the term 'inherent' were dropped." *Id.* at 792).

14. LOUIS HENKIN, HOW NATIONS BEHAVE 141–44 (2d ed. 1979) ("The fair reading of Article 51 permits unilateral use of force only in a very narrow and clear circumstance, in self-defense if an armed attack occurs." *Id.* at 141).

15. IAN BROWNLIE, INTERNATIONAL LAW AND THE USE OF FORCE BY STATES 264–80 (1963) ("It can only be concluded that the view that Article 51 does not permit anticipatory action is correct and that the arguments to the contrary are either unconvincing or based on inconclusive pieces of evidence." *Id.* at 278).

16. HERSCH LAUTERPACHT, 2 OPPENHEIM'S INTERNATIONAL LAW 156 (7th ed. 1952) ("[T]he Charter confines the right of armed self-defense to the case of an armed attack as distinguished from anticipated attack.") It should be noted that in the Jennings and Watts 9th edition of this authoritative treatise, the authors partially disavow the statement in the earlier version, stating that "while anticipatory action in self-defence is normally unlawful, it is not necessarily unlawful in all circumstances, the matter depending on the facts of the situation including in particular the seriousness of the threat and the degree to which pre-emptive action is really necessary and is the only way of avoiding that serious threat." ROBERT JENNINGS AND ARTHUR WATTS, 1 OPPENHEIM'S INTERNATIONAL LAW 417 (1992). For further elaboration of the Jennings and Watts views, *see infra* notes 39 and 40 and accompanying text.

17. ANDREW MARTIN, COLLECTIVE SECURITY 169 (UNESCO Paris, 1952) ("Under the Charter they no longer have this latitude [to respond to an apprehended attack]: the attack must be actual and armed.")

18. Robert Tucker, *The Interpretation of War Under Present International Law*, 4 INTERNATIONAL LAW QUARTERLY 11, 29–30 (1951).

19. THE CHARTER OF THE UNITED NATIONS (Bruno Simma ed., 1994).

20. Albrecht Randelzhofer, *Article 51, in id.* at 661, 666.

21. *Id.* at 675.

22. *Id.* at 676 (emphasis supplied).

23. *Id.* It should be noted that Professor Randelzhofer rejects the conclusion of the International Court of Justice in the *Nicaragua* case that the customary law of self-defense corresponds "almost completely to the right of self-defence under Art. 51 of the Charter," but regards this as of little moment, since, in his view the customary law could apply only to the few non-UN members. "As regards UN Members, it stands that Art. 51, including its restriction to the armed attack, supersedes and replaces the traditional right to self-defence." *Id.* at 678.

24. DINSTEIN, *supra* note 9, at 168.

25. *Id.* at 160, quoting, in part, E. Jimenez de Arechaga, *International Law in the Past Third of a Century*, 159 RECUEIL DES COURS DE L'ACADÉMIE DU DROIT INTERNATIONAL 1 at 96 (1978) [other citations omitted].

26. *Id.* at 163.

27. United States Identical Notes, reproduced in 22 AMERICAN JOURNAL OF INTERNATIONAL LAW (Supp.) 109 (1928).

28. DINSTEIN, *supra* note 9, at 164, quoting in part from A. S. HERSHEY, THE ESSENTIALS OF INTERNATIONAL PUBLIC LAW 349 (1912) [other footnotes omitted].

29. *Id.* at 172.

30. *Id.* Compare Professor Dinstein's theory with that suggested by Professor M. Nagendra Singh more than three decades earlier. Professor Singh also insisted that the actual occurrence of an armed attack was a condition precedent to the exercise of self-defense, but he too would authorize resort to self-help when the potential aggressor "has taken the last proximate act on its side which is necessary for the commission of the offence of an armed attack." M. Nagendra Singh, *The Right of Self-Defence in Relation to the Use of Nuclear Weapons*, 5 INDIAN YEARBOOK OF INTERNATIONAL LAW 3, 25 (1956).

31. *See* D. W. BOWETT, SELF-DEFENSE AND INTERNATIONAL LAW 2–3 (1958), and sources cited therein.

32. Randelzhofer, *supra* note 20, at 675.

33. C. Humphrey M. Waldock, *The Regulation of the Use of Force by Individual States in International Law*, ACADÉMIE DE DROIT INTERNATIONAL, RECUEIL DE COURS 455, 498 (1952) (footnote omitted).

34. MYRES S. MCDOUGAL & FLORENTINO P. FELICIANO, LAW AND MINIMUM WORLD ORDER 234–41 (1961).

35. *Id.* at 237.

36. David Linnan, *Self-Defense, Necessity and U.N. Collective Security: United States and Other Views*," 1 DUKE JOURNAL OF COMPARATIVE & INTERNATIONAL LAW 57, 81 (1991).

37. *See*, in particular, MCDOUGAL & FELICIANO, *supra* note 34, at 235; O. Schachter, *The Right of States To Use Armed Force*, 82 MICHIGAN LAW REVIEW 1620, 1633–34 (1982); Waldock, *supra* note 33 at 497.

38. MCDOUGAL & FELICIANO, *supra* note 34, and authorities cited therein.

39. ROBERT JENNINGS & ARTHUR WATTS, 1 OPPENHEIM'S INTERNATIONAL LAW 421 (9th ed. 1992).

40. *Id.* at 422 (emphasis supplied).

41. Rosalyn Higgins, *The Attitude of Western States towards Legal Aspects of the Use of Force*, *in* THE CURRENT LEGAL REGULATION OF THE USE OF FORCE 435, 442–43 (Antonio Cassese ed., 1986). But in the same volume, *see contra*, Ian Brownlie, *The U.N. Charter and the Use of Force, 1945–1985*," *id.* at 491, 498–99. Professor Dinstein, in his analysis of these cases under his doctrine of "interceptive self-defense," reaches the same conclusion as Professor Higgins with respect to the two Israeli actions. DINSTEIN, WAR, AGGRESSION AND SELF-DEFENCE, *supra* note 9, at 44 and 191.

42. U.N. SCOR (2288th mtg.), U.N. Doc. S/RES/487 (1981), *reprinted in* 75 AMERICAN JOURNAL OF INTERNATIONAL LAW 724 (1981).

43. Higgins, *supra* note 41, at 443. Other commentators have reached the same conclusion. *See, e.g.*, William T. Mallison and Sally V. Mallison, *The Israeli Aerial Attack of June 7, 1981, Upon the Iraqi Nuclear Reactor: Aggression or Self-Defense?*, 115 VANDERBILT JOURNAL OF TRANSNATIONAL LAW 417 (1982); DINSTEIN, *supra* note 9, at 45 and 169; Antonio D'Amato, *Israel's Air Strike Upon the Iraqi Reactor*, 77 AMERICAN JOURNAL OF INTERNATIONAL LAW 584 (1983). *Contra:* TIMOTHY L. H. MCCORMACK, SELF-DEFENSE IN INTERNATIONAL LAW: THE ISRAELI RAID ON THE IRAQI NUCLEAR REACTOR 302 (1996).

44. Antonio Cassese, *Return to Westphalia? Considerations on the Gradual Erosion of the Charter System*, *in* Cassese, *supra* note 41, 505, 515–16.

45. MCDOUGAL & FELICIANO, *supra* note 34, at 240.

46. Oscar Schachter, *In Defense of International Rules on the Use of Force*, 53 UNIVERSITY OF CHICAGO LAW REVIEW 113, 136 (1986).

47. Military and Paramilitary Activities (*Nicaragua v. United States*) (Jurisdiction), 1984 I.C.J. 424 (Nov. 26).

48. Military and Paramilitary Activities (*Nicaragua v. United States*) (Merits), 1986 I.C.J. 96 (June 27) [hereinafter *Nicaragua* case].

49. *Id.* at 103.

50. *Id.* at 347, quoting Waldock, *supra* note 33, at 496–97, and citing BOWETT, MCDOUGAL & FELICIANO, and SCHACHTER (dissenting opinion of Judge Schwebel).

51. Department of the Navy, The Commander's Handbook on the Law of Naval Operations (NWP 1-14M/MCWP 5-2.1/COMDTPUB P5800.1), para. 4.3.2.1 (1995) (emphasis supplied). This publication was formerly designated as NWP-9 (Rev. A) [hereinafter cited as NWP 1-14M and NWP-9 (Rev.A) respectively].

52. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3121.01A, Standing Rules of Engagement for US Forces, para 5h (2000) [hereinafter JCS SROE].

53. Secretary of State Daniel Webster to Mr. Fox, British Minister at Washington, April 24, 1841, *quoted in* 2 JOHN BASSETT MOORE, A DIGEST OF INTERNATIONAL LAW 412 (1906).

54. NWP-9 (Rev. A), para. 4.3.2., *supra* note 51, which provided that the necessity must be "instant, overwhelming, and leaving no reasonable choice of means."

55. MCDOUGAL & FELICIANO, *supra* note 34, at 217.

56. *Id.* at 218. In the course of their analysis, McDougal and Feliciano conclude that the standard of necessity under Article 51 is not less restrictive than the customary-law standard, which required a "high degree of necessity—a 'great and immediate' necessity [citing Westlake], 'direct and immediate' [citing Lawrence], 'compelling and instant' [citing Schwarzenberger]," to be characterized as "legitimate self-defense." *Id.* at 231, 232-41 [citations omitted].

57. MYRES S. MCDOUGAL, *The Soviet-Cuban Quarantine and Self-Defense*, 57 AMERICAN JOURNAL OF INTERNATIONAL LAW 597 (1963).

58. *Id.* Professor Brunson MacChesney, in a companion piece, agreed that under the conditions that prevailed at the time [nuclear stand-off], "A threatened state must retain some discretion in its initial judgment of necessity. Subsequent review will determine its validity." Brunson MacChesney, *Some Comments on the 'Quarantine' of Cuba*, 57 AMERICAN JOURNAL OF INTERNATIONAL LAW 592, 595–96 (1963).

59. William T. Mallison and Sally Mallison, *Naval Targeting: Lawful Objects of Attack*, *in* THE LAW OF NAVAL OPERATIONS 241, 263 (Horace B. Robertson, Jr. ed., 1991) (Vol. 64, US Naval War College International Law Studies).

60. *Id.*

61. *Id.* at 263. The three applicable criteria which they identify are: "(l) A good faith attempt to use peaceful procedures; (2) actual necessity (as opposed to a sham or pretense) in the context of either an existing armed aggression or a threat of armed aggression against the defending state which is both credible and imminent; and (3) proportionality in responding defensive measures." *Id.* at 262.

62. NWP 1-14M, *supra* note 51, para. 8.1.1. *See*, in particular, the notes to para. 8.1.1 in the Annotated Supplement to the Manual. ANNOTATED SUPPLEMENT TO THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS 402–03 (A. Ralph Thomas & James C. Duncan eds., 1999) (Vol. 73, US Naval War College International Law Studies).

63. *Id. See*, in particular, note 11 to para. 8.1.1 for a listing of the so-called "target sets" for the offensive air campaign of Operation DESERT STORM against Iraq.

64. UN CHARTER, art. 41.

65. Randelzhofer, *supra* note 20.

66. Annex, G.A. RES. 3314 (XXIX) 1974), adopted without a vote on December 14, 1974.

67. *See* WALTER GARY SHARP, SR., CYBER SPACE AND THE USE OF FORCE, Ch. 6; LAWRENCE T. GREENBERG ET AL., NATIONAL DEFENSE UNIVERSITY INSTITUTE FOR

NATIONAL STRATEGIC STUDIES, INFORMATION WARFARE AND INTERNATIONAL LAW, ch. 2; Sean P. Kanuck, *Information Warfare: New Challenges for Public International Law*, 37 HARVARD INTERNATIONAL LAW JOURNAL 272, 288-89 (1996); Michael Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUMBIA JOURNAL OF TRANSNATIONAL LAW 885 (1999).

68. "Definition of Aggression" Resolution, *supra* note 66.

69. *Nicaragua* case, *supra* note 48, at 119.

70. *Id.*

71. MCDOUGAL & FELICIANO, *supra* note 34, at 240–41.

72. Schmitt, *supra* note 67, at 909 (emphasis in original).

73. *Id.* at 911.

74. *Id.* at 912.

75. *Id.* at 917.

76. *Id.*

77. *Id.* at 934.

78. *Id.* at 935.

79. LAWRENCE T. GREENBERG ET AL., *supra* note 67, at 85–87.

80. Dinstein, *Computer Network Attack*, *supra* note 5.

81. SHARP, *supra* note 67, at 130.

82. *See* JCS SROE, *supra* note 52.

83. *See* examples in the NDU study, *supra* note 67 at 59–64.

84. UN CHARTER, art. 41.

85. In a 1999 article in the Washington Post, Michael Ruane reported that the Internet contains a vast number of "easy, ready-to-use computer hacking programs" and that for many kids, computer hacking just "seems kind of cool." Ruane, *supra* note 3, at 1.

86. Schmitt, *supra* note 67, at 898, citing Jack L. Brock *in* Information Security: Computer Attacks at Department of Defense Pose Increasing Risks: Testimony Before the Permanent Subcomm. On Investigations of the Senate Comm. On Governmental Affairs, 104th Cong. (1996) (statement of Jack L. Brock, Director, Defense Information and Financial Management Systems Accounting and Information, General Accounting Office).

87. Schmitt, *supra* note 67, at 898, citing President's Commission on Critical Infrastructure Protection, Critical Foundations: Protecting America's Infrastructures A-48 (Oct. 1997).

88. Schmitt, *supra* note 67, at 893.

89. *Id.*

90. Jack L. Brock, Jr., Director, Defense Information and Financial Management Systems, GAO, Report to Congressional Requesters (May 22, 1996). The report noted that only about 1 in 150 attacks is detected and an estimated 65 per cent of the attacks penetrated Defense systems. Michael Ruane reports that the Department of Defense undergoes 80 to 100 attacks every day. Ruane, *supra* note 3, at 1.

91. Schmitt, *supra* note 67, at 932.

92. *Id.* at 933. It should be noted that Professor Schmitt, in his formulation, closely follows the nomenclature of Professor Dinstein's "interceptive self-defense" doctrine. *Id.* at 931–33.

93. MCDOUGAL & FELICIANO, *supra* note 34, at 218.

94. Schmitt, *supra* note 67, at 932.

IX

Computer Networks, Proportionality, and Military Operations

James H. Doyle, Jr.

A Computer Network Attack (CNA) has been defined as operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computer networks themselves.[1] Whether CNA operations are employed in offense or countered in defense, there are complex issues of proportionality, just as there are in conventional or kinetic attack situations. This chapter explores some of the proportionality judgments an operational military commander must make. But first, it is useful to consider the capabilities, limitations, and vulnerabilities of the computers and computer networks that are revolutionizing high-tech military forces.

Operational Proliferation

During the war in Kosovo and Yugoslavia, targets for NATO aircraft were developed and reviewed by a computerized network that linked, in real time, commanders, planners, intelligence officers, and data specialists on both sides of the Atlantic.[2] Simultaneously, Tomahawk cruise missiles launched from surface ships and submarines were planned and directed using computer programs. Inside an aircraft, tank, or the lifelines of a warship, there are computer chips at the heart of every weapons system. For example, to track Chinese M-9 missiles fired

into the Taiwan Straits in 1996, USS BUNKER HILL (CG-52) loaded a theater ballistic missile surveillance and tracking program into the Aegis weapon system.[3] Computer watchstations acquire, process, display, and disseminate data from sensors simultaneously. In air defense, the new Cooperative Engagement Capability (CEC) uses a network of microprocessors and a data distribution system to share unfiltered radar measurements for composite tracking by dispersed aircraft, ships, and ground batteries.[4] Electronic, acoustic, infrared, and optical systems have many lines of computer code. Satellites and unmanned aerial vehicles, carrying sensors, communication, and data transfer links, are controlled by computer programs. National satellite imagery, when netted, enables precise geo-positioning for accurate targeting of standoff weapons, as well as mission planning, battle assessment, and intelligence support.[5] Precision guided munitions depend on sophisticated computer programs for processing weapon engagement data, such as those embedded in the Low Altitude Navigation and Infrared-for-Night (LANTIRN) and the Joint Surveillance Target Attack Radar (JSTARS) systems. Commercial off-the-shelf (COTS) technology is being exploited so that redesigns and updates in military computers can keep pace with the rapid commercial development in home and business computers.

Webbing and Netting

The computing power in transistors mounted on microprocessors has increased dramatically for combat systems in individual aircraft, ships, and battlefield units. However, it is in the *netting* and *webbing* of computers associated with command and control, surveillance, targeting, and gathering intelligence that is adding a new dimension to warfare.[6] In a computer web, commanders at all levels can simultaneously view the same battlespace. The synergism of several networks, such as the Joint Planning Network, Joint Data Network, and Joint Composite Tracking Network, enhance defense against ballistic and cruise missiles. In both offense and defense, decision-making is speeded up. Innovative tactics and "self-synchronization" at the warrior level are facilitated. Coordination and rapid maneuver among widely dispersed units are enhanced. There is a greater opportunity to get inside an adversary's observe, orient, decide, act (OODA) loop. Secure video teleconferencing, data base connectivity, direct downlink, and broadcast/receive capabilities provide access to intelligence, logistic, and essential support data, including weather, mapping, terrain, and oceanographic predictions.[7] The correlation and fusion of data from sensors in satellites, aircraft, ships, and battlefield units enable sensor-to-shooter connectivity and precision targeting. A soldier or Marine equipped with a Situational

Awareness Beacon with Reply (SABER) has access to thousands of friendly force positions every hour, which greatly minimizes fratricide in battle.[8] The emerging global infrastructure of communication networks, computers, data bases, and consumer electronics provides the National Command Authorities and military commanders with new opportunities to gather intelligence and, most importantly, to get indications and warning of a crisis or threat of attack.

Capabilities, Limitations, and Vulnerabilities

But with all the high-tech capabilities and potential, computers and their networks are only tools of warfare. Humans must make judgments, often based on insufficient or ambiguous data. Identification and discrimination regarding military targets and civilian casualties are difficult issues and cannot be resolved entirely by computer networks. In Kosovo, for example, restrictions on minimum altitudes and the types of authorized targets made it difficult for NATO forces to destroy an enemy who had no requirement to shoot, move, or expose himself.[9] Then there is the reality that computer networks are not always available or fully operable. Hard drives jam, memories fail, adapters burn out, cables sever, and servers saturate.[10] Difficult challenges of configuration control, standard computer language, reliability, and interoperability abound.[11] The Office of Management and Budget places the number of Defense Department computer systems at 8,145, of which 2,096 are deemed critical to military operations.[12] Furthermore, it is not easy to move "zeros" and "ones" where needed when bandwidth is constrained. There is also the ever-present problem of recruiting and retaining trained personnel to operate and maintain the sophisticated computer networks. In addition, data is not information. It is raw material that needs to be processed to obtain ground truth and avoid saturation. Since all data when displayed looks equally valid, computer-aided tools and filters are required to assign confidence levels to the accuracy of the information.[13]

For high-tech military forces, the capabilities of computers and their networks far outweigh the limitations. But technical issues need to be vigorously addressed. Systems must be designed with greater robustness, redundancy, and the ability to degrade gracefully.[14] Security systems (firewalls, shielding, intrusion detection devices, personnel checks, motion sensors, encryption, anti-virus software, and training) are required. But firewalls and intrusion detection devices can be bypassed, and all software is inherently flawed.[15] It must be recognized that command and control, communications, intelligence, surveillance, and reconnaissance systems have become much more vulnerable in information warfare.[16] This is especially true in communication systems, which rely on a

combination of military and civilian satellite networks and transponders. War games, modeling and simulation, and actual incidents reveal a number of methods to attack computer networks. These include physical disruption of hardware and software, insertion of a virus, worm, or logic bomb into a computer program, flooding networks with false data, buffer overflows, malformed data, and e-mail attachments, as well as unsophisticated jamming.[17] Intelligence gathering satellites, military communication networks, sensor downlinks, and precision targeting could be disrupted or defeated. But low-tech military forces, while less dependent on computer networks, may, in some cases, be just as vulnerable to CNA. Command and control may be a single path network without redundancy and fall-back alternatives. Satellite communications may be completely unprotected. In addition to the vulnerabilities of information systems, computer network technology employed offensively has the potential of producing devastating effects on both military support (fuel, spare parts, transportation, mobilization, and medical supplies) and the civilian infrastructure (air traffic control, electrical generation, water distribution, hospital life support, emergency services, currency control, and, ominously, nuclear reactor operations). Thus, both high and low-tech military commanders and their national command authorities need to thoroughly analyze the legal and policy implications before resorting to CNA operations, either in offense or defense. Then, there are the unfriendly "hackers" and terrorist groups eager to exploit vulnerability asymmetries at whatever risk and at relatively low cost. Cyberspace is a highly competitive environment world-wide. The long term effectiveness of computer networks may be less about technology and more about the ability to organize and innovate.

CNA and Consequences

As indicated in the lead-off definition, a CNA can either be an attack on the information resident in computers and computer networks or a direct attack on the computers and their networks. Whether a CNA constitutes an "armed attack"[18] depends not on the means and methods used, but on the resulting consequences.[19] The means and methods of attack may be similar to other offensive information operations, such as psychological or electronic warfare, but the consequences may be severe injury, suffering, death, or destruction of property, and amount to or rise to the level of an armed attack. On the other hand, the consequences may be intrusive, annoying, or disruptive, but not an imminent threat to life or limb, or intended to cause direct damage or injury. In both offense and defense, US military commanders are guided by the Standing Rules of Engagement (SROE) for US military forces. The SROE bridge the transition

between *jus ad bellum* and *jus in bello* by implementing the inherent right of self-defense and providing guidance for the application of force to accomplish the mission.[20] They are based on national policy, operational requirements, and US domestic and international law, including the law of armed conflict. The elements of self-defense and mission accomplishment are necessity and proportionality, although the meanings in the self-defense context are much different than when applied under the law of armed conflict for mission accomplishment. The SROE make no distinction in the guidelines for self-defense and mission accomplishment between an attack with conventional weapons and a computer network attack. Thus, the same general criteria would apply, with supplemental measures for a specific operation that might well include guidance on CNA operations.

Self-Defense (*Jus ad Bellum*)

A military force on a post-Cold War mission (humanitarian, peacekeeping, crisis control) could well be confronted with a computer network attack. The attacker could be a malicious hacker, terrorist group, or foreign armed force. Under the US SROE, necessity requires that the military commander must first determine whether the CNA is in fact either a hostile act or a clear demonstration of hostile intent before he decides that it is necessary to respond. An armed attack, such as sinking a ship, firing on troops, invading territory, blockading ports, or mining harbors would in most circumstances be regarded as hostile acts. A physical or kinetic attack against the computer networks that are vital for command and control, surveillance, targeting, or early warning could well preclude or impede the mission and thus also be considered a hostile act. On the other hand, a cyberspace intrusion into these same computer networks may or may not be a hostile act, although a disruption of the satellite network that provides indications of an ICBM launch might, per se, be a hostile act since active defenses are not yet available, and in any event, cueing information is so crucial.

Although the CNA may not rise to the level of a hostile act, the consequences may demonstrate hostile intent, that is, placing the military force in imminent danger. Hostile intent, however demonstrated, has always been a difficult judgment call. The determination is both objective and subjective, influenced by up-to-date intelligence on an adversary and his prior conduct. One military writer has described the concept as an "expression of the national right of anticipatory self-defense at the unit level."[21] Locking on an aircraft with fire control radar, approaching on an attack profile, massing tanks and troops on the border, or mobilizing the military and civilian infrastructure for war can all be evidence

of hostile intent. In cyberspace, there are a wide variety of methods of attack previously mentioned that could adversely affect a military commander's computer networks. However, the means of attack and the consequences may not be tangibly present—no "see and touch" evidence. Besides, since cyberspace attacks are inherently anonymous, covert, seamlessly interconnected, and travel across international boundaries via relay points, it is difficult to identify and trace the source, and establish attribution. Is the perpetrator military or civilian, State-sponsored, a rogue organization, or an individual acting on his own? Absent a conventional attack component, manipulation or intrusion by itself does not automatically indicate hostile intent. A CNA intrusion into the communications network could be just an intelligence probe for future operations. But a CNA to disrupt the air defense and targeting networks could be the critical step before launching an armed attack. There are many examples on both sides of the ledger, and critical questions to ponder. Do the consequences of a particular CNA place the military force in imminent danger? Is an adversary attempting to prepare the battlefield for an armed attack that is likely, imminent, or unavoidable? Is this the last opportunity for the military commander to counter the threat?[22] If so, the ingredients are there for hostile intent and the necessity to act.

In a CNA situation, just as in a conventional attack, the response to counter the threat must be proportional, whether in anticipatory or actual self-defense. That is, under the US SROE, "the force used must be reasonable in intensity, duration, and magnitude, based on all the facts known to the commander at the time, to decisively counter the hostile act or hostile intent and to ensure the continued safety of US forces."[23] In self-defense "proportionality points at a symmetry or approximation in 'scale and effects' between the unlawful force and the lawful counter-force. . . . A comparison must be made between the quantum of force and counter-force used, as well as the casualties and damage sustained."[24] A military commander must decide what weapons, means of delivery, countermeasures, and tactics are the most appropriate for the situation. For example, the Doctrine for Joint Operations in operations other than war provides that "military force be applied prudently. . . . Restraints on weaponry, tactics, and levels of violence characterize the environment."[25] The objective is to respond with just enough force to control the threat and protect the forces. The response need not be in kind or executed on the spot, if time permits due consideration. For example, in Operation EARNEST WILL (reflagging and protecting Kuwaiti tankers during the Iran-Iraq Tanker War), after the USS SAMUEL B. ROBERTS (FFG-58) hit an Iranian-laid mine, the appropriate and proportional response selected by the National Command Authorities was to attack Iranian oil platforms, attacking Iranian ships only if they fired on US ships.[26] On the other

hand, a theater ballistic missile fired at the military force or a facility under its protection requires action within minutes to acquire, track, and engage the missile. Also guiding a military commander in responding to an attack, CNA or conventional, will be a nation's policy objectives. US policy, as stated in the SROE, is to maintain a stable international environment and provide an effective and credible deterrent to armed attack. If deterrence fails, in addition to being proportional, the response should be designed to limit the scope and intensity of a conflict, discourage escalation, and achieve political and military objectives.[27] Finally, the use of force is normally the last resort. When time and circumstances permit, the potentially hostile force should be warned and given the opportunity to withdraw or cease threatening actions.[28]

During the Naval War College symposium, "Computer Network Attack and International Law," the Proportionality Working Group discussed various approaches for developing a response to a CNA.[29] One such framework would be to analyze the attack in categories of consequences, such as a network attack with only network effects, a network attack with network and conventional effects, and a conventional attack with network and conventional effects. For each category evaluated, a military commander could consider various options for a proportional response: computer network only, both computer network and conventional, or conventional only. In reaching a judgment, a military commander, guided by the SROE, might pose a series of questions to be resolved for each option, matched against each category: Is there time for a warning to cease threatening actions and an opportunity for the adversary to withdraw? Does the CNA place the military force in imminent danger? Is the CNA the final stage in preparing the battlefield for an attack? Is this the last opportunity for a military commander to protect his force? Is the response contemplated reasonable in intensity, duration, and magnitude? Will the response effectively counter the threat and remove his force from danger? Is a computer network response or a conventional response the most appropriate, or a combination of both? If a computer network response, is there an ability to accurately assess the consequences? Does a computer network response involve a cross-border intrusion? Will the response assist in stabilizing the immediate crisis? Is the response designed to limit the scope and intensity of an impending conflict? Does it discourage escalation? Is the response consistent with maintaining a credible deterrent to further CNAs? What will be the effects, intended or unintended, on civilians, their property and infrastructure? Can these effects be distinguished from effects on military personnel, equipment, and infrastructure?

In the case of a CNA with only network effects, the consequences, although degrading a particular computer network, may not place the force in imminent

danger or be evidence of an impending attack. The appropriate response might be to shift to an alternate network, use computer countermeasures to expel the intruder, sanitize the system, and report to higher authority. This situation would be analogous to tolerating an aircraft tracking radar, but not a locked on fire control radar. Higher authority, with the requisite technical expertise and network connections, could trace the intrusion, identify the perpetrator, and take appropriate action, such as a complaint to the relay State, if the CNA appears to be State-sponsored. Or, if the intrusion is an intelligence probe, higher authority might choose to play the game and "grab the hacker," feeding him false information covertly. If, however, the network effects disable the air and missile defense network and are judged as the overriding evidence of armed attack, the immediate response might be to launch a conventional attack against the most threatening military targets—tanks and troops, aircraft on runways, missile sites, command headquarters, and the like. Such a response would be timely and might discourage an adversary from attacking or, at least, indicate that there will be a high cost to proceeding. This would not rule out a follow-up computer network response against, for example, the adversary's military command and control network, executed at the appropriate level by trained network experts. In either situation of a CNA with network effects only, the proportionality set-point to trigger a response in kind should be high since the intrusion may be ambiguous and non-threatening or the response would not be timely, effective, or within the capability of the operational commander to execute.

In a crisis situation, an adversary may choose to initiate a CNA that has both network and conventional effects, such as manipulating the air traffic control network of an aircraft carrier that causes collisions or near misses of aircraft in the approach and landing pattern. This attack would be less risky than attacking the carrier or its air wing. The overall effect is to raise the level of hostility and resolve some of the ambiguity in identifying the source. Obviously the situation cannot be tolerated. If overall intelligence plus the conventional effects can presumptively attribute the CNA to a particular adversary, the initial response might be a stern warning to cease the hazardous computer operations, in addition to shifting to an alternate control mode, attempting to expel the perpetrator, and sanitizing the system. If, despite the warning and opportunity to cease, the disruption continues, the military commander might respond with a conventional, precision attack against the most appropriate military target that would reinforce the warning with force. Such targets might be a facility for the production of nuclear, chemical, and biological weapons, ballistic missile launchers that are not yet mobile, or a new warship about to be launched. This would be analogous to the response when the USS SAMUEL B. ROBERTS

hit the Iranian mine which was laid arbitrarily to hazard both warships and merchant ships. That response was neither in kind nor executed immediately. If the computer specialists also have the capability to intrude and disrupt one of the adversary's vital military computer networks, this would also be an appropriate and timely response. All of these responses are intended to control the crisis, discourage escalation, and avoid collateral damage and incidental injury to civilians.

In the case of a physical attack against a computer network asset itself, such as destroying a satellite (communications, navigation, imagery) or damaging a command and control (C2) node, the conventional effects are tangible and serious. The source and location can probably be pinpointed. Destruction of a satellite without other evidence of hostile intent would not warrant an immediate physical or CNA response. But such an extraordinary act would have implications and effects world-wide, and would merit immediate attention at the highest levels of government, as well as the United Nations Security Council. If the destruction of the satellite or damage to the C2 facility is the prelude to armed attack, a robust and direct conventional response to blunt the attack would probably be the most effective. All military targets that are part of or supporting the attack would be fair game. The objective would be to protect the force, control the threat, discourage escalation, and, at the same time, avoid collateral damage and incidental injury to civilians. A parallel CNA response to degrade, manipulate, or destroy information resident in the adversary's C2 computer networks might effectively complement the conventional response. This response might target networks that support the armed attack, taking care to avoid unintended network effects that injure or kill civilians or damage their property. Here, the problem is sorting out the network effects that may be inextricably linked in the military and civilian infrastructure.

There are numerous examples of network and/or conventional consequences and responses to a CNA that can be analyzed in the categories postulated. The most appropriate and proportional response will depend on a careful consideration of the facts, context, and intelligence in each particular case, whatever method of determination is pursued.

Mission Accomplishment (*Jus in Bello*)

A military force involved in a crisis or action in self-defense that develops into a low intensity conflict or prolonged war could be authorized to conduct CNA operations, that is, attack the information resident in computers and computer networks, or attack the computers and their networks directly. In applying force to accomplish a mission, the SROE provides that US forces will be governed by

the law of armed conflict[30] and rules of engagement. Also, as mentioned previously, the elements of mission accomplishment are necessity and proportionality. Hostile acts and intent are presumed. Necessity means that attacks must be limited to military objectives,[31] and that force has to be constrained to that required to accomplish the mission.[32] Proportionality in mission accomplishment, however, unlike self-defense, is not a comparison and symmetry between the quantum of force and counterforce used.[33] The objective is to defeat the enemy as rapidly as possible. Disproportionate force may be, and often is, required. But in applying counterforce, the law of armed conflict requires that a military commander observe the principle of distinction between combatants and noncombatants,[34] precautions in attack,[35] and the law of targeting.[36] Although it is not unlawful to cause incidental injury to civilians, or collateral damage to civilian objects, incidental or collateral damage must not be excessive in the light of the military advantage anticipated by the attack.[37] In applying this proportionality balancing test, a military commander must take all reasonable precautions, based on information available at the time, to keep civilian casualties and damage consistent with mission accomplishment. He must also consider alternative methods of attack to reduce civilian casualties and damage. In addition to *jus in bello* proscriptions, a military commander will be guided by supplemental measures in the ROE that "define the limits or grants of authority for the use of force for mission accomplishment."[38]

The Proportionality Working Group[39]also explored approaches for analyzing CNA offensive operations. For example, the CNA might be a network attack against a network target, a network attack against a non-network target, or a conventional (kinetic) attack against a network target. These categories, while overlapping and arbitrary, are intended to assist in focusing on the effects and consequences of a CNA. For each option evaluated in terms of effects and consequences, a military commander, guided by the SROE and battle plan, might pose a series of questions to be resolved: Will the CNA capture important enemy intelligence? Does it assist in getting inside the enemy's OODA loop? Can the CNA disrupt, control, or destroy the enemy's computer networks for intelligence collection and targeting? Will it contribute to establishing information dominance, air and maritime superiority, and space control? Does the CNA provide the military commander with new options for favorably controlling the rhythm of the battle? Will it influence the enemy to terminate military action and alter policy? Does the CNA degrade an enemy's supporting infrastructure? Is it essential in protecting own forces, equipment, and facilities? Overall, does the CNA contribute to the partial or complete submission of the enemy with the least expenditure of life, time, and resources? In coalition warfare, does it

preserve unity of effort and consensus in waging war? Does the CNA respect the inviolability of neutrals and their commerce? Is the CNA consistent with United Nations Security Council enforcement action, if any? Does the CNA involve cross-border intrusions? Is it compatible with diplomatic and political efforts to achieve a cease-fire, suspension of hostilities, armistice agreement, peace treaty, or other termination of the war? What are the effects of the CNA on protected persons (civilians; wounded, sick, and shipwrecked; medical personnel and chaplains; and prisoners of war)? What incidental injury to civilians or collateral damage is anticipated from the CNA, based on the best means to accurately assess the primary and secondary effects of a CNA? Can the military effects be distinguished from the civilian effects? Is the incidental injury or collateral damage likely to be excessive in the light of the military advantage anticipated? Will it cause unnecessary suffering or be indiscriminate in nature? Are there alternative means and methods of attack that will reduce civilian casualties and damage from that considered likely from the CNA? Will a decision to withhold *network attacks* against network or non-network targets influence an enemy to also refrain from similar network attacks, and can this restraint be relied upon? Finally, pertinent to each of the questions, does the network or non-network target by its nature, purpose, or use make an effective contribution to the enemy's military action, and thus constitute a lawful military objective of the CNA.

In the category of a network attack against a network target, the intention is to adversely affect the *information* resident in the enemy's computer network. Examples include introducing information or disinformation (not perfidious) into the computer network to influence or mislead behavior, intruding with a data device or technique to degrade the military C2 network, disrupting vital links in the integrated air defense (IAD) network, or manipulating the military communication network to confuse the timing of a maneuver or attack. In these and similar offensive computer operations, the ultimate consequences are neither intended nor anticipated to involve incidental injury or collateral damage. Psychologically, the civilian population may, as intended, be influenced, but the effects would not be physical. A computer intrusion into the enemy's intelligence network to capture vital information, or indications and warning, would be a necessary step in preparing the battlespace, and probably would not even fall within the definition of a CNA. In any event, a network attack on the information in a computer network that is tailored to produce limited physical consequences may prove to be an effective non-lethal tool of warfare against military objectives. An alternative conventional attack calculated to degrade the C2 and IAD networks, for example, could result in civilian casualties and damage.

However, in most cases, these effects would probably not be considered excessive in the light of the military advantage anticipated.

In the case of a network attack against a non-network target, the intention is to damage or destroy military objectives through the medium of a CNA operating on the information resident in the enemy's computer network. Examples would include disrupting the military air traffic control system to induce collisions or crashes, causing a military satellite to lose control and implode, disabling the electrical system in the enemy's C2 facility, and manipulating the computer network that manages vital military support. For these and other military targets, and assuming an ability to accurately assess the primary and secondary effects, CNA operations may prove to be an effective method of prosecuting the war at less risk to one's own forces. However, network attacks on the civilian infrastructure, even though it supports the enemy's military effort, raises difficult issues. It may not be possible to distinguish the military from the civilian effects because of the inextricable linkage between the two. Even if that is possible, the CNA may set off a chain of effects that cascades beyond the military and into civilian institutions. This could raise questions of whether the CNA was indiscriminate and not directed at a valid military objective. Furthermore, a cascading CNA might result in disastrous consequences on essential services for the civilian population (electrical power, water distribution, life support, nuclear power operations). Even assuming, for example, a CNA against an electrical power grid that supports the military effort, and is therefore a valid military objective, there must be no indiscriminate cascading effects, and under the proportionality and balancing test, any incidental injury and collateral damage must not be excessive in view of the military advantage anticipated. The point is not to rule out CNAs in this category, but to urge caution in their use in view of the uncertainty in predicting effects.

An attack against an enemy's computers and computer networks with missiles, bombs, or artillery shells is the traditional means of attack. A military commander must insure that the various computer network sites and facilities are valid military targets and that incidental injury and collateral damage are kept to a minimum. Damage or destruction of C2 war rooms and command posts, for example, would contribute significantly to defeating the enemy. Air defense sites, microwave stations, data relay facilities, and communication satellites can also be electronically jammed from aircraft, ground stations, and warships. Damage or destruction of a dual-use military and civilian satellite would raise serious issues for high-tech military forces that are becoming extraordinarily dependent on satellites for both military and commercial purposes. Should the commander refrain from attacking the satellite in the hope that the enemy will also exercise restraint? Is the dual-use satellite a valid military target when the bandwidth used

by the military is relatively minor? Disruption, damage, or destruction of computer network facilities that provide essential civilian services, as well as support the military effort, such as electrical power grids, may be unavoidable in prosecuting the war. But difficult proportionality judgments must be made even though there may not be the unpredictable cascading effects produced by a CNA. An assessment must be made that the civilian injury and damage will not be excessive in the light of the military advantage anticipated. Temporarily disabling the power grids by attacking with carbon chaff, for example, may reduce casualties and avoid more serious consequences, as well as influencing behavior. Attacking computers and computer networks serving primarily the civilian infrastructure, such as banking systems, stock exchanges, water management, and research centers, would be difficult to justify in terms of a military advantage and would probably result in excessive civilian injury and damage.

Just as in the *jus ad bellum* situation, there are many examples of actual or potential CNA offensive operations. While mission accomplishment proportionality takes on a different meaning from that in self-defense, the balancing test of military advantage versus excessive incidental injury and collateral damage must consider both the actual and cascading effects of a CNA, whatever method of analysis is used.

Observations

CNA operations as part of information warfare or network-centric warfare are in their infancy, with far-reaching implications for law, policy, and rules of engagement. The ability to predict and assess the damage from executing a CNA in offense or defense, similar to a precision strike weapon, is far from assured. CNAs may well prove to be invaluable in defeating the enemy and countering an attack, provided that trained and experienced computer network experts can accurately "hit" the target, control the effects, and avoid unintended cascading consequences. This assumes that CNA operations are authorized at the appropriate level. All this adds to the complexity of proportionality judgments. However, the basic rules in *jus ad bellum* and *jus in bello* still apply. An analysis of the targeting must be conducted for a CNA just as it is conducted for attacks using conventional weapons. On the defense side, the old adage of the best defense is a good offense may be turned on its head in the case of CNA operations. There is no question that a high-tech military force with significant network vulnerabilities must have a robust, passive protection against CNA. This requires increased awareness, training, technical support, hardware and software improvements, greater redundancy, and an ability to degrade gracefully in computer network

equipment and systems. It also means that military commanders must plan and train to "work-around" network attacks that disrupt, deny, or destroy critical information resident in their computers and computer networks. This is particularly important since rogue and terrorist groups without asymmetrical vulnerabilities can wage network war on the cheap with little regard for the risk.

Notes

1. Chairman of the Joint Chiefs of Staff, Joint Publication 3-13, Joint Doctrine for Information Operations, at GL-5 (1998) [hereinafter Joint Pub 3-13].

2. *See* Michael Ignatieff, *The Virtual Commander: How NATO Invented a New Kind of War*, THE NEW YORKER, Aug. 2, 1998, at 33.

3. *See* Gary W. Schnurrpusch, *Asian Crisis Spurs Navy TBMD*, NAVAL INSTITUTE PROCEEDINGS, Sept. 1999, at 46–49.

4. *See The Cooperative Engagement Capability*, 16:4 JOHNS HOPKINS APPLIED PHYSICS LABORATORY TECHNICAL DIGEST 377–396 (1995).

5. *See* Austin G. Boyd and David G. Simpson, *Satellite Communications: C4I Link into the 3rd Millennium*, 21:5 SURFACE WARFARE, Sept./Oct. 1996, at 11–16.

6. For a discussion of the present and future potential of computer networks in warfare, see Arthur K. Cebrowski and John Garstka, *Network-Centric Warfare: Its Origins and Future*, NAVAL INSTITUTE PROCEEDINGS, Jan. 1998, at 28–35; James J. Kuzmich and Christopher P. McNamara, *Land Attack from the Sea*, NAVAL INSTITUTE PROCEEDINGS, Aug. 1999, at 52–55; Andrew F. Krepinevich, *Calvary to Computer: The Pattern of Military Revolutions*, in STRATEGY AND FORCE PLANNING 582 (Naval War College Faculty eds., 1995); William K. Lescher, *Network-Centric: Is it Worth the Risk?*, NAVAL INSTITUTE PROCEEDINGS, July 1999, at 58-63; Arthur K. Cebrowski, *Network-Centric Warfare and C2 Implications*, NAVAL WAR COLLEGE REVIEW, Spring 1999, at 4–11.

7. *See* David G. Simpson, *Using Space for a Battlefield Advantage*, 21:5 SURFACE WARFARE, Sept./Oct., 1996, at 7–9.

8. *See* Austin Boyd, *Rapid Response Through Space: Reducing Battlefield Fratricide*, *id.* at 27–28. Similarly, the new Joint Expeditionary Digital Information System (JEDI) is a briefcase-size command and control system with an Iridium satellite handset. It contains a personal digital assistant and a Global Positioning System (GPS) receiver, and can interface with the Global Command and Control System, displaying GCCS-like tracks. *See* Rupert Pengelley, *JEDI Returns for JSCOPE'S Mini C2 System*, JANE'S INTERNATIONAL DEFENSE REVIEW, Oct. 1994, www.janes.com.

9. *See* Phillip C. Tissue, *21 Minutes to Belgrade*, NAVAL INSTITUTE PROCEEDINGS, Sept. 1999, at 38–40.

10. *See* Michael Keehn, *Is the Navy Heading for a Crash?*, NAVAL INSTITUTE PROCEEDINGS, July 1999, at 88–89.

11. *See* Letitia Austin, *Linking Acquisition to the Fleet*, 21:5 SURFACE WARFARE, Sept./Oct. 1996, at 8–9.

12. *See Pentagon Report: Pentagon Seeks to Boost Public Confidence in Y2K Readiness*, NATIONAL DEFENSE, Sept. 1999, at 10.

13. *See* Alan D. Zimm, *Human-Centric Warfare*, NAVAL INSTITUTE PROCEEDINGS, May 1999, at 28–31.

14. *See* Robert F. James, *The Guts Behind the Glory*, 21:5 SURFACE WARFARE, Sept./Oct.1996, at 2–7.

15. *See* Perry G. Luzwick, *What's a Pound of Your Information Worth?: Constructs for Collaboration and Consistency*, 20:4 NATIONAL SECURITY LAW REPORT, AUG. 1999, at 1, 6.

16. *See* Joint Pub 3-13, *supra* note 1, at III-1-15; Office of General Counsel, Department of Defense, An Assessment of International Legal Issues in Information Operations (Nov., 1999) (The paper is appended to this volume as the Appendix).

17. For a description of the effects of a "logic bomb," "worms," and a "sniffer," see Steve Lohr, *Ready, Aim, Zap*, NEW YORK TIMES, Sept. 30, 1996, at D-1. *See also* David Tubbs, *Exploits: How Hackers Hack*, 20:4 NATIONAL SECURITY LAW REPORT, Aug., 1999 at 14–16.

18. For a discussion of the macro issues in the international law of information warfare, see LAWRENCE GREENBERG, SEYMOUR GOODMAN, AND KEVIN SOO HOO, INFORMATION WARFARE AND INTERNATIONAL LAW (1998) and WALTER G. SHARP, SR., CYBERSPACE AND THE USE OF FORCE (1999).

19. For an innovative framework to analyze a CNA in *jus ad bellum* situations, see Michael N. Schmitt, *Computer Network Attack and Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUMBIA JOURNAL OF TRANSNATIONAL LAW 885–937 (1999).

20. Joint Chiefs of Staff Standing Rules of Engagement (SROE), Chairman, Joint Chiefs of Staff Inst. 3121.01, Oct. 1, 1994 [hereinafter SROE] (The current version of the SROE was promulgated on Jan. 15, 2000, as CJCS Instruction 3121.01A.) For an excellent discussion of the US Rules of Engagement, see James C. Duncan, *The Commander's Role in Developing Rules of Engagement*, NAVAL WAR COLLEGE REVIEW, Summer 1999, at 76–89.

21. Duncan, *supra* note 20, at 82.

22. *See* Schmitt, *supra* note 19.

23. SROE, *supra* note 20, at A-5.

24. YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENCE 231 (3d ed. 2001).

25. Chairman Joint Chiefs of Staff, Joint Publication 3-0, Doctrine for Joint Operations, at V-3 (1995).

26. WILLIAM J. CROWE, THE LINE OF FIRE 187–211 (1993).

27. SROE, *supra* note 20, at A-2.

28. SROE, *supra* note 20, at A-6.

29. Symposium on Computer Network "Attack" and International Law, Naval War College, June 1999.

30. SROE, *supra* note 20, at A-2.

31. "Military objectives are limited to those objects which by their nature, purpose, or use make an effective contribution to military action and whose total or partial destruction, capture, or neutralization, in the circumstances ruling at the time, offers a definite military advantage." Additional Protocol I to the Geneva Conventions of Aug. 12, 1949, and relating to the Protection of Victims of International Armed Conflicts, June 8, 1977, *reprinted in* Documents on the Laws of War 419 (Adam Roberts and Richard Guelff eds., 3rd ed. 2000).

32. The Commander's Handbook on the Law of Naval Operations, NWP 1-14M/MCWP 5-2.1/ COMDTPUB P5800.1, para 5.2 (1995) [hereinafter NWP 1-14M].

33. *See* DINSTEIN, *supra* note 24, at 231–235.

34. Protocol I, art. 51, *supra* note 31, at 448–49.

35. Protocol I, art. 57, *supra* note 31, at 452–453.

36. NWP 1-14M, *supra* note 32, at para 8.1.

37. NWP 1-14M, *supra* note 32, at para. 8.1.21. *See also* Protocol I, art. 57 2(a)(iii), *supra* note 31, at 453; SAN REMO HANDBOOK ON INTERNATIONAL LAW APPLICABLE TO ARMED CONFLICTS AT SEA (Louise Doswald-Beck ed., 1995), para. 46, at 16; and William Fenrick, *The Rule of Proportionality and Protocol I in Conventional War*, 98 MILITARY LAW REVIEW 91, 125 (1982).

38. Duncan, *supra* note 20, at 83.

39. *See* Symposium, *supra* note 29.

X

Some Thoughts on Computer Network Attack and the International Law of Armed Conflict

Louise Doswald-Beck*

Introduction

It seems one has to accept as inevitable that when something useful for the improvement of man's life has been invented, thoughts will either turn to how to weaponize or destroy it, or, in the case of computer network technology, both.

The task of the international lawyer in the face of a new weapon or intended military activity is to establish how existing law applies and with what effect. Would existing law prohibit the weapon or activity or restrict it in any particular way? Would it be appropriate, for one or more policy reasons, to impose prohibitions or restrictions that do not already apply? Might it be the case, on the contrary, that the new weapon or method might be an improvement from both a policy and humanitarian point of view?

The purpose of this short chapter is to explore certain aspects of how computer network attack (CNA) could be affected by international humanitarian law (IHL), including the law of neutrality, based on the knowledge generally available so far on the military possibilities presented by computer networks. It

may be that these possibilities are overstated, but the chapter will base itself on the premise that a variety of the indicated effects would be possible.

Applicability of the International Law of Armed Conflict (International Humanitarian Law)[1]

It is perfectly reasonable to assume that CNA is subject to IHL just as any new weapon or delivery system has been so far when used in an armed conflict. The only real difficulty in this regard would arise if the first, or only, "hostile" acts were conducted by these means. Would this amount to an armed conflict within the meaning of the 1949 Geneva Conventions and other IHL treaties? This question is close to, but not necessarily identical with, whether the behavior amounts to an armed attack within the meaning of Article 2(4) of the UN Charter. The ICRC Commentary to the 1949 Geneva Conventions indicates that in the case of a cross-border operation, the first shot suffices to create an international armed conflict,[2] which can therefore be of very short duration.[3] There are, of course, other views which would require a threshold of intensity or time,[4] but this approach would lead to the need for evaluations that would create inevitable uncertainties and ultimately to the same problems faced when establishing whether "war" existed without a formal declaration; this issue led to the abandonment for the need for a "war" for the "law of war" to apply. The problem is still with us, however, in non-international armed conflicts where there remain many cases of uncertainty (or denial) as to whether the threshold and nature of violence has reached that of an armed conflict, rather than "just" internal violence requiring "police" operations.[5] If the first or only "hostilities" that occur in a non-international situation were computer network attacks, the degree of doubt would be even greater.

The problem is, of course, that so far hostilities have involved weapons which launch projectiles, or other types of energy transfer, that lead to visible physical damage. In the case of IHL, the motivation for the application of the law is to limit the damage and provide care for the casualties. This would militate in favor of an expansive interpretation of when IHL begins to apply. The likelihood of this threshold being linked with the perception that an armed attack within the meaning of Article 2(4) has occurred in the case of a cross-border CNA is, of course, high, given the historical development of the *jus ad bellum* and the *jus in bello*. This would not be problematic if it had a restraining effect on the commencement of hostilities through CNA, either because of the Article 2(4) prohibition, or because the Security Council decided the CNA amounted to a threat to the peace and dealt with it in a way that avoided more damage.

However, the danger lies in the possibility of the CNA being perceived as an armed attack justifying measures of self-defence, for such a characterization might escalate the situation further than would otherwise have been the case. Whether or not these linkages occur, there is an argument to be made in favor of the implementation of IHL when CNA is undertaken by official sources and is intended to, or does, result in physical damage to persons, or damage to objects that goes beyond the bit of computer program or data attacked. CNA alone in non-international contexts is even more problematic—it is far more likely to be seen solely as criminal behavior, although the potential for damage could be enormous and the groups undertaking this could be at least as well organized as "armed" groups. Once "normal" weapons are used, there is no problem at all. CNA will be an attack (in the sense of the *jus in bello*) as any other. Whether CNA alone will ever come to be seen as amounting to an armed conflict for the purposes of IHL implementation will probably be determined through practice, rather than a formal decision by the international community in the abstract, although the latter should not be ruled out. It will probably also depend on the degree of damage that CNA causes (the more it creates, the more likely it will be treated in the same way as an armed conflict). Perhaps even the term "armed" conflict will one day start sounding as outdated as "*jus in bello*!"

How the Existing Law of Armed Conflict Would Affect the Use of Computer Network Attack

As indicated earlier, one can safely assert that the whole body of IHL applies to the use of CNA. Three areas of this law seem, however, particularly pertinent: the principle of distinction and all the rules that flow from it, the use of ruses of war and the prohibition of perfidy, and whether the rules relating to combatant status could be affected. In addition, some thought needs to be given to the law of neutrality during armed conflict.

The Principle of Distinction

Whereas in the eighteenth and nineteenth centuries methods of warfare meant that civilians were only directly affected by sieges and otherwise only indirectly by the general economic advantages or misfortunes caused by war, the advent of air and missile warfare in the 20th century brought the need for special protection for civilians against attack to the fore. The principle of distinction has therefore taken on an importance, and led to detailed treaty and customary law, that goes well beyond the few rules articulated in the 1899 and 1907 Hague

Conventions. Although heartily derided by the "realists," those persons who strove to ban the dropping of bombs from the air[6] were obviously far-seeing people who realized the potential for massive destruction that this new method represented. Even restrictions on air warfare were slow to come about, only being accepted, in the form of the 1977 Protocols Additional to the Geneva Conventions, once the potential military utility of air warfare had been thoroughly explored.[7]

Although the form and probable effect of warfare is quite different, the same pattern may be showing itself in relation to CNA. Here is a new tool that in civilian life opens up access to the world through rapidity and ease of communication in a way that has been heretofore unseen. Moreover, it allows technological development that could lead to all kinds to extraordinary steps in human development. One suggestion that has been made is to consider banning at least some forms of CNA;[8] however, it has been rejected, probably because of the desire to further explore CNA's military potential. As always, there are those who argue that "progress" cannot be stopped, that new means and methods of warfare are inevitable, and that therefore there is really no point in trying to stop or regulate anything. Others prefer to see which new methods are useful in that they are more accurate, militarily more effective, do not cause unnecessary damage, and are not more trouble than they are worth. Needless to say, IHL in general, and the principle of distinction in particular, are based on the latter premise. It is hoped that, unlike bombardment from the air, careful thought will be given to CNA before launching into experimentation.

The principle of distinction involves a number of rules that will be of particular relevance for CNA: (i) the evaluation that objects considered for attack are indeed "military objectives" within the meaning of IHL; (ii) the prohibition of indiscriminate attacks; (iii) the need to minimize collateral damage and to abstain from attacks if such damage is likely to be disproportionate to the value of the military objective to be attacked; and (iv) the need to take the necessary precautions to ensure that the above three rules are respected. From what is known at present, there are potential problems as regards all of these rules in relation to CNA.

Only Military Objectives May Be Attacked

The definition of military objective contained in Additional Protocol I[9] is not only that accepted by the 155 States party to the treaty, but was also referred to as being the appropriate one to use by the representatives of several major non-party States at the recent diplomatic conference that adopted the Second Protocol to the Hague Convention for the Protection of Cultural Property of 1954.[10] In order for something to be a military objective, it must meet two cumulative conditions: it must make an effective contribution to the military

action of the adversary and, in the circumstances ruling at the time, its attack must offer a definite military advantage to the attacker. It is clear that this definition does presuppose a plan to be followed with a view to achieving a particular military result. It also presupposes a knowledge of what the adversary is using, and how it is being used, for its military action. The terminology was chosen carefully to prohibit certain behaviors of the Second World War, specifically, it addressed the attack of persons and objects on the basis that they are "quasi-combatants" or in one way or another help the "war effort." Such reasoning leads sooner or later to no restraints, for anything can be justified this way. Indeed, it rapidly led to the United Kingdom deciding that "civilian morale" was to be a target[11] and, as a result, to the wholesale destruction of cities.

The specification that the object must effectively help the "military action" of the adversary means that the link to the military operations must be a close and obvious one. The reference to the "circumstances ruling at the time" requires that the military advantage to the attacker be equally clear and obvious in the context of the attacker's military plan to achieve the particular military aim. During the negotiation of the Additional Protocols, this was considered to represent both economy of force and military professionalism, thereby leading to the military result needed while moving away from generally attacking anything in the hope that in due course the adversary would surrender. The decision not to adopt a list of "military objectives" was part of the same reasoning. Any list could either exclude something that in the circumstances could be of great importance in achieving the particular military mission, or alternatively include things of little or no importance in the particular circumstances. It is for this reason that any "list" in a textbook or manual can never offer more than examples of what have at one point or another been considered to be military objectives in past conflicts—they will not necessarily be so in any particular future one.

It is to be hoped that planning and precision will not be lost. Computer networks can easily be seen as "communications." Many manuals refer to "means of communication" as typical military objectives—a simple reference to existing lists could lead to the appalling result that any computer network used by the adversary State and its citizens could be attacked. Quite apart from the fact that this would almost certainly hit protected objects, and in addition amount to an indiscriminate attack, it would not result from the necessary process of evaluation described above. In order to amount to a military objective, either the piece of network being affected or the object that the network is controlling must meet the two conditions.

There could also be the temptation to try to totally remove the technological framework which the whole of society bases itself on (although this may well be

technically impossible through CNA), on the reasoning that this would make that society's life so generally unpleasant that surrender would surely follow. The temptation is likely to be all the greater because military networks will probably be better protected from hacking than a number of civilian networks. It could also be asserted that this method would be more "humanitarian" than sending bombs. It is clear that this reasoning is quite different from that underlying the Protocols, which stress choices of target for the specific desired military goals. Is there a possibility that sophisticated military practice (which was the basis for the rules in the Protocols) will change? What would happen to the principle of distinction? An approach based on technological siege warfare would in effect make it disappear, or at least radically change its characteristics. It could require that specially protected objects, e.g., hospitals, organize themselves so that they are not within the normal computer network (if this were practicable) in order to be protected. In effect, this would represent a return to the reasoning behind the rules of Geneva Convention IV of 1949[12] and the Hague Convention of 1954,[13] which rely on the concept of the creation of various safe areas because they assumed that the practices of World War II would prove inevitable. Such reasoning would amount to abandoning the approach of the Protocols and present customary law, i.e., that all objects that are not military objectives are safe from being deliberately targeted.

Careful thought should be given before going down the road of technological siege warfare. Quite apart from the fact that it would be contrary to present customary and treaty law, the presumptions that such a practice would be based on are dubious for at least two totally separate reasons. First, society is increasingly becoming so dependent on modern technology that computer systems failure for a lengthy period would not be just "unpleasant"—it could easily lead to mass disease, starvation and other catastrophes[14] (it is probable that such a scenario could not be accomplished by CNA alone, but it may well be possible when undertaken in conjunction with other methods). On the other hand, and despite the recent example, it would not necessarily lead to surrender in a short period of time. Both reasons lead to the conclusion that surgical technological strikes, to the degree that this is technically possible, would make more sense.

The Prohibition of Indiscriminate Attacks

Additional Protocol I defines indiscriminate attacks in Article 51(4).[15] An attack is indiscriminate when it either is not carefully aimed at each military objective (through carelessness or use of inappropriate weapons) or when its effects on a military objective are uncontrollable and unpredictable (an obvious and

uncontroversial example would be the use of a bacteriological weapon against a group of soldiers).

From what has been written so far on CNA, this appears to be potentially the most serious problem, i.e., aiming accurately at what the intended target is and, even if one manages to strike it with precision, not at the same time creating a host of unforeseen and unforeseeable effects.[16]

The Problem of Collateral Damage

The need to avoid, or at least minimize, damage to civilians and civilian objects is reflected in Article 57(2)(a)(ii) of Protocol I, which indicates that "those who plan or decide upon an attack shall . . . take all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event to minimizing, incidental loss of civilian life, injury to civilians and damage to civilian objects." An attack only becomes in itself illegal, however, if it violates the rule of proportionality, a long-standing rule of customary law. The wording used in Article 51(5)(b) of Protocol I is "an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated."

The evaluation as to whether likely civilian damage would be disproportionate has an inherent difficulty in that one is comparing two different things. Whereas the need to avoid or at least minimize collateral injury is a straightforward rule relating to the choice of means or methods that should be preferred, an evaluation as to possible illegality is fraught with difficulty. A certain subjectivity seems inevitable, but as an anticipated result could be illegal, there ought to be some objective factors to follow. State practice in this regard is scant—just a few examples have been given on when such attacks have been desisted from—and they have usually been when either the possible target was something that was military in nature but in the circumstances unusable or where the object's value as a military objective could not be verified.[17] To complicate matters, certain statements of understanding indicate that the attack is to be considered as a whole when making the evaluation.[18] However, these statements should not be interpreted as meaning proportionality of the civilian damage caused during the entire campaign compared with military advantages obtained during a specific attack. Such an interpretation is impossible because the only evaluation that could be possible would be at the end of the conflict, whereas the rule requires the evaluation to be done *before* the attack concerned. Proportionality evaluations pursuant to the *jus in bello* should also not be confused with proportionality in self-defence, which is the *jus ad bellum* rule that requires the military action as a

whole to be limited to what is necessary to restore one's territorial integrity.[19] Rather, based on a number of sources, the statements of understanding can only be logically interpreted as referring to the fact that the military value of attacking an object (which has to be weighed against the likely civilian casualties) will obviously be assessed taking into account its role in the broader strategic purpose of a particular military operation that may consist of various individual actions.[20]

There could be, of course, a temptation to consider that whatever collateral damage was caused by CNA, it would surely be proportional to the military advantage gained. This would be an abuse of the rule, as it requires a careful *advance* evaluation of the likely effects on the civilians. If the likely effects are quite unclear and unforeseeable (which appears to be the technical situation at present), the attack would be an indiscriminate one and therefore illegal as such—the rule of proportionality would not even be relevant.[21]

Precautions in Attack

It is obvious that in order to respect the rules relating to the principle of distinction, a certain amount of thought and planning is necessary. Such precautions are therefore nothing more than the expression of a *bona fide* implementation of the law.[22] The advance evaluations indicated above are of particular importance, but it also ought to be possible to call off an attack once it becomes clear that what was thought to be a military objective is not one after all or ceases to be one, or if it becomes clear that the consequent collateral damage would be excessive.[23] This would be particularly relevant in cases of CNA methods that would not have an immediate effect on the target.

The other aspect of great importance, in order to evaluate military objective or incidental damage, is that of sufficient intelligence information. The advantage of computer operations is that they can be conducted from the comparative security of a computer terminal far from the actual military operations. Computer network exploitation (CNE) could help gain maximum information on an adversary's situation, provided that such data is available on reachable networks and that the data is not itself deliberate misinformation. However, although it is a valuable tool for gaining intelligence and does not pose the risks of physical presence, CNE cannot totally replace intelligence gathering by other means, especially the most reliable one, direct observation.[24] CNE combined with other intelligence sources could well provide for the possibility of good precautions being taken in attack.

On the other hand, CNA conducted from a distance poses two particular problems in relation to precautions in attack. First, if one suspects that one is the object of such an attack, taking out the attacker is likely to prove to be very

difficult because of the immense difficulty of being sure where the attack originated. The likelihood, therefore, of attacking back in quite the wrong place is high.

Second, lack of physical presence near the object to be affected means that the likelihood of making mistakes as to whether something really is at that moment a military objective is high. Protocol I speaks in terms of the attacker doing "everything feasible" to verify that the target is a military objective. The word "feasible" clearly indicates that perfection is not expected. It is a matter of common sense and good past military practice that commanders take into account the need to reduce exposure of their own armed forces (an eliminated army cannot win an armed conflict). However, it is only a recent practice that so much care is given to avoiding *any* military casualties on one's own side, and one can see how tempting CNA would be in such an endeavor. The law requiring precautions in attack cannot be simply eliminated if such precautions involve some physical risk to the attacker. Although not articulated anywhere as such, when such a practice means that there are many more civilian casualties than military, the concept of the principle of distinction is badly battered, perhaps even turned on its head. Once again, apart from amounting to a violation of existing law, such inaccuracy gives rise to concern as to the effectiveness of the intended military operation.

Ruses of War and Perfidy

Computer data provides new avenues for practicing ruses of war. The more CNE is undertaken, the more likely it is that misinformation will be deliberately planted to confuse the adversary. Such misinformation about one's own affairs is perfectly lawful, for it is analogous in principle to any other vehicle for misinformation. Moreover, it is clear from traditional sources that ruses of war need not be limited to creating misinformation about oneself.[25] However, it must also be true that computer generated attacks cannot be undertaken whilst giving the impression that they come from the adversary's own side. This would be the equivalent to attacking while wearing the enemy's uniform, which is clearly illegal.[26] As with all ruses of war, care must be taken that they do not cross the line into perfidy. Therefore, misinformation implicating protected persons or objects would be unlawful, as would CNE amounting to a breach of good faith, such as pretending to surrender or to create a truce.[27]

Combatants and CNA

It is most likely that CNA and CNE would be carried out by specialized personnel. What would be the legal situation of such persons? Could they be

attacked by any means and in any place? What would be their status if captured? There is probably no reason why the rules should be any different than in traditional armed conflict.

If incorporated into the armed forces, such personnel would have all the rights and liabilities of combatants. Therefore, they certainly could be attacked like any other combatant and should endeavor to be in uniform if captured. The narrow exception in Article 44(3) of Protocol I (for those party to it), which would allow POW status if captured without uniform, may well not apply to such persons, as this provision is generally interpreted as applying only to combatants in occupied territory, and only then in certain situations.[28] Persons captured in the adversary's territory without uniform carrying out CNE would also qualify as spies. If conducted from outside the territory, however, the situation should be no different from someone gathering data from a spy satellite.

Technicians that act for the military, but are not part of it, pose more of a problem. The persons listed in Article 4(4) of Geneva Convention III of 1949[29] are entitled to prisoner of war status if captured, but the type of persons listed are more analogous to computer technicians that keep the machines in order, and not ones that actually undertake the attacks. It could well be, therefore, that persons who actually undertake CNA would be considered civilians who would have no POW status if captured. They would also be subject to attack, as they would be taking a "direct part in hostilities."[30] Whether those undertaking CNE are in exactly the same situation is less clear, and this is because State practice is not consistent as to whether intelligence collection falls into the category of taking a "direct" part in hostilities. However, there is no reason why gathering intelligence by this means should be treated any differently from intelligence gathering by other means. The possibility of being treated as a spy would only occur if the CNE were carried out clandestinely in the territory of the adversary. The Hague Regulations of 1907, in particular Article 21, do not exclude the possibility that civilians could be spies for the purposes of IHL, although Article 46 of Protocol I only refers to members of the armed forces. However, both treaties conceptually indicate the need to be caught in the act in the territory controlled by the adversary, although this is not the exact wording used.[31] However, if the civilian undertaking CNA or CNE is not "claimed" by the army using him, he could be simply treated as an individual breaking national law and therefore be subject to criminal law should he be captured on return to the country; the rule that he cannot be treated as a spy once he returns to his own army would not apply and there is no reason why POW status would be considered either.

The Effect on Neutral States

Although there are a number of discussions on whether there is a formal difference between "non-belligerent" and "neutral" States, and a resulting difference of legal regime,[32] this author believes that there is insufficient basis in State practice to support such an assertion. Therefore, for the purposes of this chapter, all States not party to a conflict will be treated as "neutral."

As many networks link up and/or are owned by different countries or their private citizens, and given that it is the general view that the effect of any CNA might not be limited to the intended target, the law relating to neutral States is of particular significance. The law of neutrality in cyberspace poses difficulties, beyond those of other aspects of IHL, because neutrality law has led to legal regimes that differ depending on the region of operations. Thus, there are significant differences between the law applicable to land, sea (which is subdivided into different maritime areas), and outer space operations. It is not self-evident what the regime should be in relation to cyberspace. To suggest that it should vary depending on whether the data affected are supposed to be at any particular moment in a country's territory, passing via a satellite, or being conducted through an underwater cable would create a factual and legal nightmare.

One could, of course, simply wait to see what happens and deduce customary law based on practice, rather like what initially happened in relation to the law of outer space, which began to take shape when the first satellites were actually put into orbit. However, this new area of activity did not escape formal regulation through a series of international instruments that began to be adopted after only a few years, initially in the form of UN resolutions and later a number of treaties which confirmed the practice that outer space and other planets could not be acquired by any nation nor be used to base certain weapons.[33] Therefore, the likelihood of CNA being left entirely to practice without more formal international legal regulation is somewhat slim. It would make sense at this stage to consider the kind of regime that would be appropriate, and, rather than be totally inventive, see whether basic principles of the law of neutrality could provide some answers.

The basic premise of the law of neutrality is that a neutral State should not, through its actions, deliberately affect the outcome of armed conflict between belligerents. In return, the neutral expects not to be drawn into the conflict. An excellent description of the concept of neutrality and the basic rules that flow from it is contained in Volume II of Oppenheim's *International Law*. Certain passages in this description remain of fundamental importance. After indicating that all States that are not drawn into the war are presumed neutral, it provides that:

> Since neutrality is an attitude of impartiality, it excludes such assistance and succour to one of the belligerents as is detrimental to the other, and, further, such injuries to the one as benefit the other. But it requires, on the other hand, active measures from neutral States. For neutrals must prevent belligerents from making use of their neutral territories, and of their resources, for military and naval purposes during the war. . . . Further, neutrals must, by all means falling short of becoming involved in hostilities or of abandoning their attitude of impartiality, prevent each belligerent from interfering with their legitimate intercourse with the other belligerent through commerce and the like, because a belligerent cannot be expected passively to suffer vital damage resulting to himself from the violation by his enemy of a rule, which, while it operates directly in favour of neutrals, indirectly operates in his favour as well.
>
> The required attitude of impartiality is not incompatible with sympathy with one belligerent, and disapproval of the other, as long as these feelings do not find expression in actions violating impartiality. . . . Moreover, acts of humanity on the part of neutrals and their subjects . . . can never be construed as acts of partiality, even if these comforts are provided for the wounded and the prisoners of one belligerent only.[34]

The same thought is put across even more succinctly by Professor Leslie Green:

> So long as the activities of these non-participants do not interfere with the legitimate activities of the belligerents or benefit one at the expense of the other, neutrals are entitled to have their territory and doings respected and unaffected because of the conflict.[35]

These passages indicate the importance of distinguishing between, on the one hand, the right of the neutral State to carry on its life, including commerce with belligerents, as normal, from, on the other hand, the prohibited behavior of actively favoring the outcome of the war through State acts. This is also the reasoning, cited in Oppenheim, behind some of the more detailed rules, including those that distinguish between State acts and the acts of a State's citizens:

> International Law is primarily a law between States. . . . In the first instance, neutral States are bound by certain duties of abstention, e.g., in respect of supply of loans and munitions to belligerents, which they are not bound to exact from their nationals. Secondly, neutral States are under a duty to prevent their territory

> from becoming a theatre of war as the result of passage of foreign troops or aircraft or of prolonged stay of belligerent men-of-war in their territorial waters. Thirdly, they are bound to control the activities of their nationals insofar as these may tend to transform neutral territory into a basis of war operations or preparations. At the same time, International Law renders unlawful certain activities of nationals of neutral States, like carriage of contraband or breach of blockade, without, however, imposing upon these States the duty to prevent or to penalise such acts. These are punished by the belligerent against whom they are directed.[36]

Oppenheim then recognizes the rather thin line between individual activity and State activity in regulated economies, but indicates that the rule still exists. Although this text was published 48 years ago, practice has not really changed significantly, especially in the light of the precision given on export licences:

> From the case of actual governmental responsibility for the production of and trade in certain articles there must be distinguished that of governmental control over exports by the system of licensing and the like. The fact that the Government permits export which it could prevent by means of withholding the licence does not make it a party to the transaction. Its responsibility is engaged only when in thus acting it discriminates between the opposing belligerents. . . .
>
> . . . Apart from certain restrictions necessitated by impartiality, all intercourse between belligerents and neutrals takes place as before, a condition of peace prevailing between them in spite of the war between the belligerents. This applies particularly to the working of treaties, to diplomatic intercourse, and to trade.[37]

The same point is made by Professor Green:

> A neutral does not have to forbid the supply of war *matériel* by resident individuals or companies, nor is it required to stop the passage of such goods across its territory. It is under no obligation to forbid the use of privately-owned communication equipment on behalf of belligerents, but if it limits the freedom of its nationals to provide such facilities this restriction must operate against all the belligerents.[38]

This passage stresses the fact that neutral States have, for the most part, the right to carry on life as normal. Their specific duties are relatively narrow, concentrating primarily on preventing their territory from being used as a base

of operations by one belligerent or the other. If they choose to grant specific facilities (that must not directly concern military operations), they must be granted to all the belligerents equally, e.g,. if the neutral allows one belligerent to bring prizes to one of its ports, it must allow the other belligerent the same rights.[39] Therefore, any negative effect of the war on the neutral State would be indirect.

The specific rights of belligerents in relation to neutral merchantmen in this context are more in the character of an exception to the general rule than otherwise. They are based on the rather special combination of being acts that are carried out against individuals, in an area that is not national territory, and stem from very long and peculiar practice specific to naval warfare. Any analogy between computer networks and these special rules of neutrality relating to merchantmen on the high seas would be highly dubious; it would certainly not be based on the general principles which for the most part allow neutral citizens to carry on life as normal. State practice over the last 50 years is essentially consistent with this position. Arguments that most States are not really "neutral" because of the degree of relations that they and their citizens have with belligerents appear to be founded on an exaggerated interpretation of the degree of restrictions and duties that such States are supposed to have.[40] Therefore, a belligerent State would have to be very certain that a neutral State has indeed violated its duties of neutrality before considering self-help measures involving force to stop the violation. Such a violation of the duty of neutrality by the State cannot be easily asserted. In addition, the prohibition of the use of force in Article 2(4) of the UN Charter means that such a use of force by a belligerent could, if not clearly lawful, be not only a breach of the law of neutrality, but also a violation of the UN Charter.[41]

Returning specifically now to the question of computer networks, which are for the most part owned by companies that are more or less subject to a limited degree of State regulation, basic principles of neutrality law would militate in favor of their continuing to be used as normal, even if some States are in an armed conflict with each other. The nearest equivalent to computer networks in existing neutrality law is reflected in Article 8 of Hague Convention V of 1907:

> A neutral Power is not called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals.

In so far as much of the computer network does indeed use telephone lines, this provision is directly applicable. In other cases, both its implication and the basic principles of neutrality law would support application of the same rule. As far as transmission via satellite is concerned, there is no reason why the rule should be any different; freedom of the use of outer space in international law is extensive and the 1967 Outer Space Treaty does not contain any specific provisions that would prevent the use of neutrally owned satellites by belligerents or give the right to a belligerent to interfere with such satellites. Despite the indication in Article III that the use of outer space should be pacific, and in Article I that it should be in the interests of all countries, the prohibitions that are clearly enunciated are limited to weapons of mass destruction,[42] and, at any rate, use must be in conformity with international law.[43] Without taking a stand on whether any type of military use of satellites is in conformity with the letter or spirit of the 1967 treaty, it contains nothing that would change the law of neutrality as such, nor, to this author's knowledge, has it been interpreted as having done so. This brings us back to general neutrality law.

It would appear, therefore, that a breach of neutrality would only occur if a neutral State specifically allowed a network to be built on its territory for the purposes of supporting the armed conflict of one or more belligerents or if it specifically allowed a network to be devoted to this purpose, for doing so would be the equivalent of allowing its territory to become a base of operations. This conclusion mirrors Article 3 of Hague Convention V:

> Belligerents are . . . forbidden to
>
> (a) Erect on the territory of a neutral Power a wireless telegraphy station or other apparatus for the purpose of communicating with belligerent forces on land or sea;
>
> (b) Use of any installation of this kind established by them before the war on the territory of a neutral Power for purely military purposes, and which has not been opened for the service of public messages.

Article 5 of the same treaty indicates that neutral States must not allow any of these acts to occur on its territory.

So much for the use of computer networks by neutrals and belligerents. What would be the case if a CNA was directed at a target in a belligerent country but affected a neutral country. If such an effect was unforeseeable and unlikely, then it would be purely accidental. However, if such an effect was probable or even

possible, then the situation would not be the same. The law of neutrality is very strict in its prohibition of any violation of neutral territory. As Article 1 of the 1907 Hague Convention V puts it, "the territory of neutral Powers is inviolable." The fact that military operations must not adversely affect neutral territory is further reflected in the traditional rule that a blockade must not bar access to the ports and coasts of neutral States.[44]

State practice also indicates that all due precautions must be taken by belligerents to avoid any, even collateral, damage to neutral States. During the Second World War, US bombers unintentionally damaged a Swiss border town on April 1, 1944. Not only did Switzerland protest, but the US government also recognized that due precautions had not been taken, formally apologized for the incident, and promptly paid four million dollars in reparations. The US then issued directives prohibiting bombings within 50 miles of Switzerland.[45]

Such a clear and strict approach means that a computer network attack that could well have an adverse effect on neutral territory would be a violation of international law.

Conclusions and Further Considerations on Possible Future Legal Developments

It is clear that CNA could only be undertaken to the degree and in a fashion that would respect existing law. Certain uses would probably be not only violations of the law of armed conflict, but also amount to war crimes, in which case the individuals involved would be subject to punishment both at the national and international levels within the context of applicable international law. It should also not be forgotten that such breaches require payment of compensation, especially in the context of international armed conflicts, where compensation is a long-standing requirement.[46] In addition, the trend towards requiring reparation to be made to victims of international crimes is reflected in Article 75 of the Statute of the International Criminal Court.

In addition to these considerations, further steps deserve careful consideration. First, some thought needs to be given, after technical analysis, as to whether certain types of actions (for example, the introduction of worm viruses) would be inherently indiscriminate. If so, in principle they would automatically be illegal weapons[47] and ought to be formally banned as such. This is probably the reasoning behind part of paragraph 3 of the draft Russian resolution (that was presented to the First Committee of the 1998 General Assembly):

> *Invites* all Member States to inform the Secretary-general of their views and assessments concerning . . . :
> advisability of developing international legal regimes to prohibit the development, production or use of particularly dangerous forms of information weapons . . .[48]

This suggestion was not accepted by the United States which took the position that: "it is premature at this point to discuss negotiating an international agreement on information warfare" and that "there seems to be no particularly good reason for the United States to support negotiations for new treaty obligations in most of the areas of international law that are directly relevant to information operations."[49] The resolution finally adopted,[50] therefore, does not contain this proposal, but this does not make such a suggestion any less valid.

Second, given that there does appear to be more support for the idea of international cooperation to suppress unwelcome private actions,[51] there may well be a move towards creating universal jurisdiction for the punishment of certain hackers, either on the basis of permissive universal jurisdiction (based on the model of the customary law relating to piracy and most war crimes), or of compulsory universal jurisdiction (such as that created by treaty for grave breaches, torture, and certain types of terrorist acts). Even if universal jurisdiction as such is not created, it is likely that there will be arrangements to facilitate the extradition and punishment of such offenders.

Finally, a careful policy evaluation ought to be made as to the advantages and disadvantages of embarking on computer network attacks. On the one hand, if military advantages can be gained through this method which not only respect existing law but also reduce physical damage and casualties, then this would be a definite "plus." On the other hand, computer network attacks do have the potential to seriously mess up a wonderful new human achievement. In this regard, the most technologically advanced societies would be the most at risk. These anxieties are clearly reflected in the preambular paragraphs of the two General Assembly resolutions adopted in 1998 and 1999, which are virtually identical.[52] The operative paragraphs in effect only call on States to think about existing threats and what could be done about them, in particular the "Advisability of developing international principles that would enhance the security of global information and telecommunications systems and help to combat information terrorism and criminality."[53] The fact that military applications are possible is recognized in the first preambular paragraph which does not exclude as such this use but goes on the say that it is important to maintain and encourage civilian use. The policy question remains, therefore, "is CNA worth it?" Or would it be

more intelligent to outlaw this form of warfare before serious damage begins? It is hoped that we will not just "wait and see!"

Notes

* This chapter reflects the personal views of the author and in no way engages the responsibility of the International Commission of Jurists.

1. These terms are generally accepted as being interchangeable. Some might question whether aspects of the law of neutrality that are more concerned with the protection of the sovereign territory of neutral nations than humanitarian aspects could be properly characterised as "international humanitarian law." However, dividing up neutrality law for the purpose of making such a distinction would be awkward and unnecessary.

2. The ICRC Commentary to Article 2 of all four Geneva Conventions states that:

> Any difference arising between two States and leading to the intervention of members of the armed forces is an armed conflict within the meaning of Article 2. . . . It makes no difference how long the conflict lasts, or how much slaughter takes place. The respect due to the human person as such is not measured by the number of victims.

The ICRC Commentary to Geneva Convention Article 6, elaborates further:

> By using the words "from the outset of the conflict " the authors of the Convention wished to show that it became applicable as soon as the first acts of violence were committed, even if the armed struggle did not continue. Nor is it necessary for there to have been many victims. Mere frontier incidents may make the Convention applicable, for they may be the beginning of a more widespread conflict.

3. *Id.* at 59. Lieutenant Goodman, shot down by the Syrians on December 4, 1983, was held for one month, during which he was visited by the ICRC "in accordance with standard criteria" on the basis that the incident did amount to an armed conflict, albeit very short. 1983 ICRC ANNUAL REPORT 63.

4. For example, Howard Levie, *The Status of Belligerent Personnel "Splashed" and Rescued by a Neutral in the Persian Gulf Area*, ASIL PROCEEDINGS 597, 598, 609–610 (1988).

5. *See, e.g.*, JAMES E. BOND, RULES OF RIOT: INTERNAL CONFLICT AND THE LAW OF WAR, 51–52 (1974); George Abi-Saab, *Humanitarian Law and Internal Conflicts: The Evolution of Legal Concern*, *in* HUMANITARIAN LAW OF ARMED CONFLICT: CHALLENGES AHEAD 213, 215–216 (Astrid Delissen & Gerald Tanja eds., 1991).

6. Declaration (IV, 1) to Prohibit, for the Term of Five Years, the Launching of Projectiles and Explosives from Balloons and other Methods of Similar Nature, July 29, 1899, 1 AMERICAN JOURNAL OF INTERNATIONAL LAW 153 (Supp., 1907). *See also*, DAVID H.N. JOHNSON, RIGHTS IN AIR SPACE, 1965:

> It was to the Disarmament Conference in 1932 that the French Government submitted, in addition to a proposal to prohibit air attacks against civilians and indeed to abolish bombardment from the air altogether, a plan for the internationalisation of civil air transport under a regime organised by the League of Nations. The proposal came to nothing. (p. 38) . . . At the Disarmament Conference in 1932 four various proposals were put forward for the abolition of bombing, and even of air forces; but these came to nothing. (p. 45).

During discussions on the problem of aerial bombardment during this period, the ICRC also indicated its view that a total prohibition of bombardment from the air would be the best solution to protect civilians:

> Le Comité international estime que la seule manière de mettre les populations civiles à l'abri de certains des plus graves périls crées par l'état de guerre est l'interdiction pure et simple du bombardement aérien. . . . Il adresse dans ce sens un appel pressant à la Conférence.

DOCUMENTS RELATIFS À LA GUERRE CHIMIQUES ET AÉRIENNE PRÉSENTÉS AUX MEMBRES DE LA CONFÉRENCE POUR LA RÉDACTION ET LA LIMITATION DES ARMEMENTS PAR LE COMITÉ INTERNATIONAL DE LA CROIX-ROUGE 5 (Geneva, 1932) (the text of the appeal quoted is dated February 18, 1932).

7. A notable failed attempt was the drafting of the "Rules concerning the control of wireless telegraphy in time of war and air warfare" by a Commission of Jurists at The Hague, December 1922–February 1923 (see esp. arts. 22–24) [hereinafter Draft Resolution]. This Commission was constituted in accordance with a resolution of the Washington Conference (1922) on the limitation of armaments. These rules were never codified. Johnson (*supra* note 6, at 53) quotes military commanders as saying, in short, that in the past towns would have been besieged to win wars, which caused much more suffering than air raids during the Second World War. Johnson, who wrote in 1965, and therefore before negotiations for Additional Protocols to the Geneva Conventions, refers to Professor Georg Schwarzenberger, who

> concluded that under modern conditions the standard of civilisation has retreated before the necessities of war, that the traditional distinction between combatants and non-combatants has largely disappeared and that the only persons who may still expect immunity from acts of warfare are persons who are both unconnected with military operations or the production of war materials and reside in areas that are 'sufficiently remote' from likely target areas.

See also, J.M. SPAIGHT, AIR POWER AND WAR RIGHTS 244–258 (3rd ed. 1947) (*see, e.g.*, Proposals of 1923, Disarmament Conference of 1932, French proposals at 1932 Conference, British proposals at 1932 Conference, British proposals at 1933 Disarmament Conference, Resolution of July 22, 1932, proposed Air Pact between "Locarno Powers" of February 1935, German proposals of 1935–1936, etc.).

8. UN General Assembly, First Committee, Letter dated September 23, 1998, from the Permanent Representative of the Russian Federation to the United Nations to the Secretary General, concerning Agenda item 63, "Role of science and technology in the context of international security, disarmament and other related fields," A/C.1/53/3, Sept. 30, 1998.

9. Article 52(2), which reads as follows:

> In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action, and whose total or partial destruction, capture or neutralisation, in the circumstances ruling at the time, offers a definite military advantage.

10. This Protocol, adopted on March 26, 1999, repeats the same definition. The States that supported this definition as the appropriate one to use in the new Protocol, because of its articulation in Additional Protocol I, were the United States, India, Turkey, France and Israel.

11. JOHNSON, *supra* note 7, at 48–49. *See also*, Hays Parks, *The Protection of Civilians from Air Warfare*, 27 ISRAEL YEARBOOK ON HUMAN RIGHTS 77–82 (1997).

12. Convention (IV) Relative to the Protection of Civilian Persons in Time of War, August 12, 1949, art. 14, 6 U.S.T. 3516, 75 U.N.T.S. 287 [hereinafter GC IV]. GC IV relates to hospital and safety zones and localities. A hospital zone or locality is generally of a permanent character and is established outside the combat zone in order to shelter military or civilian wounded and sick from long range weapons, especially aerial bombardment. A safety zone or locality is generally of a permanent character and is established outside the combat zone in order to shelter certain categories of the civilian population, which, owing to their weakness, require special protection

(children, elderly people, expectant mothers, etc.) from long-range weapons, especially aerial bombardment. Article 15, GC IV, relates to neutralized zones, that are generally of a temporary character and are established in the actual combat zone to protect both combatant and non-combatant wounded and sick, as well as all members of the civilian population who are in the area and not taking part in the hostilities, from military operations in the neighborhood.

13. Convention for the Protection of Cultural Property in the Event of Armed Conflict, May 14, 1954, 249 U.N.T.S. 240. Article 2 states that the protection of cultural property shall comprise the *safeguarding* of and *respect* for such property. Article 3 states that the High Contracting Parties undertake to prepare in time of peace for the *safeguarding* of cultural property situated within their own territory against the foreseeable effects of an armed conflict, by taking such measures as they consider appropriate. Article 8, relating to Special Protection, makes it clear that this protection can only be given if the special shelters that are created or the monuments to be listed in a special list are not in any industrial center nor near any military objective, including communications lines. This restriction, which reflects the old system, has been remedied in the new Protocol II of the 1954 Convention, adopted in 1999, which reflects the new reasoning and therefore does not repeat these restrictions for property under "enhanced protection."

14. The problem of the increasingly integrated information society is noted in Daniel Kuehl, *The Ethics of Information Warfare and Statecraft*, www.infowar.com/mil_c4ij.html-ssi.

15. Which reads as follows:

> Indiscriminate attacks are: (a) those which are not directed at a specific military objective; (b) those which employ a method or means of combat which cannot be directed at a specific military objective; or (c) those which employ a method or means of combat the effects of which cannot be limited as required by this Protocol; and consequently, in each such case, are of a nature to strike military objectives and civilians or civilian objects without distinction.

Paragraph 5 refers to two other situations "to be considered as indiscriminate." In this author's view they are not, strictly speaking, indiscriminate, but rather behaviors that are outlawed for specific reasons. Paragraph 5(a) refers in effect to target area bombardments which deliberately treat as one target clearly separated and distinct military objectives even though civilians lie between them. This behavior is correctly outlawed because, in this author's view, it amounts to a deliberate targeting of civilians, i.e., those in between the military objectives. Paragraph (b) represents the customary rule that incidental damage (i.e., damage that is inevitable or likely, but not in itself intended) during attack may not violate the rule of proportionality. Once again, this is not really a description of an "indiscriminate" attack, but rather a prohibition on attacks on military objectives that, although as well aimed as possible, are still likely to create more civilian damage than the objective is worth. It is for this reason that the issue of proportionality is treated in the next section of this article.

16. Various "tools of the trade" are described in DEFENSE NEWS, August 9, 1999, at 6. The problems relating to predictability are referred to in a variety of writings, including Lawrence Downs, Jr., *Digital Data Warfare: Using Malicious Computer Code as a Weapon*, in XIII ESSAYS ON STRATEGY 43 (Mary Sommerville ed., 1996); Myron Cramer & Stephen Pratt, *Computer Viruses in Electronic Warfare*, www.infowar.com/survey/virus_ew.html; Matthew Devost, *The Digital Threat: United States National Security and Computers*, www.devost.net/mgd/documents/digitalthreat.asp; Roger Barnett, *Information Operations, Deterrence, and the Use of Force*, www.nwc.navy.mil/press/review/1998/spring/art1 - sp8.htm.

17. Burrus Carnahan, *Linebacker II and Protocol I: the Convergence of Law and Professionalism*, 31 AMERICAN UNIVERSITY LAW REVIEW 861, 865 (1981), in relation to a probable vehicle depot during the Vietnam war; *U.S. Defense Department Report on the Role of the Law of War in the Conduct*

of the Persian Gulf War, 31 INTERNATIONAL LEGAL MATERIALS 612, 626 (1992), in which reference is made to the decision not to attack two fighter aircraft next to the ancient temple of Ur:

> Commander in Chief Central Command . . . elected not to attack the aircraft on the basis of respect for cultural property and the belief that positioning of the aircraft. . . . effectively had placed each out to action, thereby limiting the value of their destruction . . . when weighed against the risk of damage to the temple.

Otherwise the same report refers rather vaguely to military targets not being attacked because of the risk to civilian persons or property:

> Coalition forces also chose not to attack many military targets in populated areas or in or adjacent to cultural . . . sites, even though attack of those military targets is authorised by the law of war.

Id. at 624.

18. Several countries have made interpretative declarations concerning Article 51(5)(b) of Additional Protocol I (1977) that references to the "military advantage" are intended to mean the advantage anticipated from *the military attack considered as a whole* and not only from isolated or particular parts of that attack. *See, e.g.*, declarations upon ratification by Australia (June 21, 1991), Canada (November 20, 1990), Italy (February 27, 1986), the Netherlands (June 26, 1986), and the United Kingdom (January 28, 1998).

19 There are different views as to whether, and if so what, other ends can be justified as needs of self-defence. This chapter does not intend to go into this issue.

20. See, in particular, an analysis of this question in the ICRC document on Elements of Crimes prepared for the Preparatory Commission for the International Criminal Court, UN Doc. PCNICC/1999/WGEC/INF.2/Add.1 at 29–32.

21. Unless, of course, the perpetrator were to be indicted as a war criminal under this rule. The fact that he or she was aware that an evaluation of likely results was not even possible would be an interesting test case, as Article 85(3)(b) of Protocol I and the ICC Statute both indicate that the accused needed to have knowledge of the extent of the civilian damage that would be caused.

22. They are spelled out in Article 57 of Protocol I

23. This is spelled out in Article 57(2)(b) of Protocol I

24. It is somewhat ironic that the most accurate intelligence, which is the best way to restrict attacks to clearly identified military objectives, is probably that collected directly by undercover agents. However, the price to be paid is that spies are not entitled to prisoner-of-war status. One could wonder whether this very long-standing custom is still appropriate.

25. *See, e.g.*, LASSA OPPENHEIM, II INTERNATIONAL LAW 429 (Hersch Lauterpacht ed., 1952), which offers the following examples: "the watchword of the enemy may be used, deceitful intelligence may be disseminated, the signals and bugle calls of the enemy may be mimicked to mislead his forces."

26. *Id.*

27. *Id.* and art. 37 of Protocol I.

28. Interpretative declarations upon ratification of Additional Protocol I (1977) by Australia (June 21, 1991), Belgium (May 20, 1986), Canada (November 20, 1990), Germany (February 14, 1991), Ireland (May 19, 1999), Republic of Korea (January 15, 1982), and United Kingdom (January 28, 1998) state that the situation described in the second sentence of paragraph 3 of Article 44 can exist only in occupied territory or in armed conflicts covered by paragraph 4 of Article 1. The interpretative declarations by Italy (February 27, 1986) and Spain (April 21, 1989) state that the situation described in the second sentence of paragraph 3 of Article 44 can exist only in occupied territory.

29. Which reads as follows:

> Prisoners of War, in the sense of the present Convention, are persons belonging to one of the following categories, who have fallen into the power of the enemy: . . . Persons who accompany the armed forces without actually being members thereof, such as civilian members of military aircraft crews, war correspondents, supply contractors, members of labour units or of services responsible for the welfare of the armed forces, provided that they have received authorisation from the armed forces which they accompany, who shall provide them for that purpose with an identity card. . . .

30. Article 51(3) of Protocol I, which represents long-standing customary law.

31. *See* arts. 29 and 31 of the Hague Regulations and art. 46(3) & (4) of Protocol I.

32. Discussions on this issue took place during one of the meetings of experts (Geneva 1993) that led to the SAN REMO MANUAL ON INTERNATIONAL LAW APPLICABLE TO ARMED CONFLICTS AT SEA (text and commentary published by Cambridge University Press, 1995) [hereinafter SAN REMO MANUAL]. Two papers were prepared on this issue, one by Wolff Heintschel von Heinegg entitled "Neutrality and Non-Belligerency" and the other by Dietrich Schindler on "Neutrality and Non-Belligerency in Armed Conflicts at Sea" (filed in the ICRC Archives). Both reach the conclusion that there is no such legal difference and the Manual treats equally all States not taking part in the conflict as "neutral." Reference is also made to this idea, but likewise rejected, in III ENCYCLOPAEDIA OF PUBLIC INTERNATIONAL LAW 552 (Jan Mayen ed., 1997).

33. In particular: G.A. Res. 1721(1961) and 1962 (1963); the 1967 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies; the 1972 Convention on International Liability for Damage Caused by Space Objects; the 1979 Agreement Governing the Activities of States on the Moon and Other Celestial Bodies; and the various telecommunications INTELSAT agreements

34. OPPENHEIM, *supra* note 25, at 654–655 (para. 294).

35. LESLIE GREEN, THE CONTEMPORARY LAW OF ARMED CONFLICT 268 (2d ed. 2000). *See also* ENCYCLOPAEDIA OF PUBLIC INTERNATIONAL LAW, *supra* note 32, at 551:

> A neutral State has the right to demand respect for its independence and above all for its territorial sovereignty, including its air space. It has the right to maintain relations with all other States, whether neutral or belligerent. . . .The supreme concept is that the neutral State may not, by governmental measures, intervene in the conflict to the advantage of one of the belligerents.

36. OPPENHEIM, *supra* note 25, at 656 (para. 296).

37. *Id.*, at 659 (paras. 296a and 297).

38. GREEN, *supra* note 35, at 262–63.

39. OPPENHEIM, *supra* note 25, at 675–76 (para. 316). *See also*, art. 9, Hague Convention XIII of 1907.

40. Oppenheim stresses over and over again the right of neutral States to continue their commerce with belligerents. *See, e.g.*, 674 (paras. 314 and 315), 675 (para. 316), 676 (para. 318), and 677 (para. 319).

41. This issue was hotly debated during the discussions leading to the San Remo Manual on International Law Applicable to Armed Conflict at Sea (*supra* note 32).The result in Paragraph 22 is more restrictive than the traditional right of self-help in such a circumstance.

42. Art. IV.

43. Art. III.

44. SAN REMO MANUAL, *supra* note 32, para. 99, which reflects art. 18 of the 1909 London Declaration. During the drafting of the San Remo Manual, this provision was totally uncontested.

45. J. Helmreich, *The Diplomacy of Apology—U.S. Bombings of Switzerland during World War II*, AIR UNIVERSITY REVIEW, May–June 1977, at 20, 21–23. The letter of apology, dated 4 April 1944, issued by the US Embassy in Berne, contained the following:

> Le profond regret de tous les Américains pour le tragique bombardment par les bombardiers américains de la ville suisse de Schaffhouse le 1er avril . . . un groupe de bombardiers . . . n'ont pas pris les larges précautions prévues pour éviter des incidents de ce genre. . . . Le Secrétaire de la Guerre . . . a demandé en même temps au Secrétaire d'Etat d'assurer votre Gouvernement que toutes précautions seront prises pour prévenir autant qu'il est humainement possible la répétition de pareil malheureux accident.

15 DOCUMENTS DIPLOMATIQUES SUISSES 1848–1945, at 315.

46. 1907 Hague Convention IV, art. 3, repeated in Additional Protocol I, art. 91.

47. *See, e.g.*, the articulation of basic rules of IHL in the Advisory Opinion of the International Court of Justice on the Legality of the Threat or Use of Nuclear Weapons, para. 95, July 8, 1996: "Thus, methods or means of warfare, which would preclude any distinction between civilian and military targets . . . are prohibited."

48. Draft Resolution, *supra* note 7.

49. Office of the General Counsel, Department of Defense, An Assessment of International Legal Issues in Information Operations (Nov. 1999) [hereinafter DoD/GC Paper]. The paper is appended to this volume as the Appendix.

50. G.A. Res. 53/70 (Jan. 4, 1999), Developments in the field of information and telecommunications in the context of international security, UN Doc. A/RES/53/70.

51. *E.g.*, "current U.S. efforts to improve mutual legal assistance and extradition agreements should continue to receive strong emphasis. Another idea that might prove fruitful is to negotiate a treaty to suppress information terrorism. . . ." DoD/GC Paper, *supra* note 49, at Appendix. This thought is also reflected in the final preambular paragraph of the resolution adopted (note 51): "*Considering* that it is necessary to prevent the misuse or exploitation of information resources or technologies for criminal or terrorist purposes." This provision is repeated in a resolution of the same name adopted the following year, UN Doc. A/54/558 which is essentially the same as the previous one, G.A. Res. 54/49 (Dec. 1, 1999) UN Doc. A/54/558.

52. *See supra* notes 9 & 51. Paragraphs 2, 3, and 7 of the 1999 resolution read as follows:

> *Noting* that considerable progress has been achieved in developing and applying the latest information technologies and means of communication;
>
> *Affirming* that it sees in this process the broadest positive opportunities for the further development of civilisation, the expansion of opportunities for co-operation for the common good of all States, the enhancement of the creative potential of mankind, and additional improvements in the circulation of information in the global community;
>
> *Expressing concern* that these technologies and means can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the security of States.

53. *Id.*, both resolutions operative para. 2(c).

XI

Wired Warfare: Computer Network Attack and the *Jus in Bello*

Michael N. Schmitt

Despite ongoing debates about the existence, or lack thereof, of a "revolution in military affairs," it is undeniable that 21st century warfare will differ dramatically from that which characterized the 20th. Perhaps most remarkable will be the maturation of "information warfare" as a tool of combat.[1] It will challenge existing warfighting doctrine, necessitate a reconceptualization of the battlespace, and expand the available methods and means of warfare. Of particular note will be the impact of information warfare on the principles of international humanitarian law . . . and vice versa.

Information warfare (IW), in particular computer network attack, has been described in detail in this volume and elsewhere. Therefore, only a brief explanation of the typology employed in this chapter is necessary. Information warfare is a subset of information operations (IO), i.e., "actions taken to affect adversary information and information systems while defending one's own information and information systems."[2] Such operations encompass virtually any nonconsensual measures intended to discover, alter, destroy, disrupt, or transfer data stored in a computer, manipulated by a computer, or transmitted through a computer. They can occur in peacetime, during crises, or at the strategic, operational, or tactical levels of armed conflict.[3] Information operations are distinguished by that which is affected or protected—information.

IW is narrower. It consists of "information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries."[4] Thus, information warfare is differentiated from other operations by the context in which it occurs—crisis or conflict. As an example, routine peacetime espionage is an example of an information operation that does not constitute information warfare unless conducted during a crisis or hostilities.

Computer network attacks (CNA), which may amount to IW or merely IO, are "operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."[5] The essence of CNA is that, regardless of the context in which it occurs, a data stream is relied on to execute the attack.[6] Thus, the *means* used set CNA apart from other forms of IO. These means vary widely. They include, *inter alia,* gaining access to a computer system so as to acquire control over it, transmitting viruses to destroy or alter data, using logic bombs that sit idle in a system until triggered on the occasion of a particular occurrence or at a set time, inserting worms that reproduce themselves upon entry to a system thereby overloading the network, and employing sniffers to monitor and/or seize data.

This chapter addresses the use of CNA during *international* armed conflict and is limited to consideration of the *jus in bello*, that body of law addressing what conduct is permissible, or impermissible, during hostilities, irrespective of the legality of the initial resort to force by the belligerents.[7] Discussion therefore centers on the use of CNA in the context of "State-on-State" armed conflict. Moreover, the chapter is an effort to explore the *lex lata*, rather than an exercise in considering *lex ferenda*. While setting forth *lex ferenda* is an especially worthy project as the nature of warfare evolves,[8] the goal here is simply to analyze the applicability of existing humanitarian law to computer network attack, and identify any prescriptive lacunae that may exist therein.

Applicability of Humanitarian Law to CNA

The threshold question is whether computer network attack is even subject to humanitarian law. To begin with, there is no provision in any humanitarian law instrument that directly addresses CNA, or, for that matter, IW or IO; this might suggest that CNA is as yet unregulated during armed conflict. Additionally, it could be argued that the development and employment of CNA post-dates existing treaty law, and thus, having not been within the contemplation of the Parties to those instruments, is exempt from the coverage thereof. A third possible argument for inapplicability is that humanitarian law

is designed for methods and means that are kinetic in nature; since there is little that is "physical" in CNA, attacks by computers fall outside the scope of humanitarian law.[9] Restated, humanitarian law applies to armed conflict, and computer network attack is not "armed."

The first two possibilities are easily dispensed with. The fact that existing conventions are silent on CNA is of little significance. First, the Martens clause, a well-accepted principle of humanitarian law, provides that whenever a situation is not covered by an international agreement, "civilians and combatants remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and from the dictates of public conscience."[10] By this norm, all occurrences during armed conflict are subject to application of humanitarian law principles; there is no lawless void. The acceptance of "international custom" as a source of law in Article 38 of the Statute of the International Court of Justice also demonstrates the fallacy of any contention of inapplicability based on the absence of specific *lex scripta*.[11]

Arguments focusing on the fact that CNA post-dates present prescriptive instruments are similarly fallacious. Precisely this line of reasoning was presented to the International Court of Justice in *Legality of the Threat or Use of Nuclear Weapons*. In its advisory opinion, the court summarily rejected the assertion that because humanitarian "principles and rules had evolved prior to the invention of nuclear weapons," humanitarian law was inapplicable to them. As the court noted, "[i]n the view of the vast majority of States as well as writers there can be no doubt as to the applicability of humanitarian law to nuclear weapons."[12] There being no reason to distinguish nuclear from computer weapons, at least on the basis of when they were developed vis-à-vis the entry into force of relevant humanitarian law norms, the same conclusion applies to CNA. Furthermore, a review of new weapons and weapon systems for compliance with humanitarian law is a legal, and often a policy, requirement.[13] Obviously, this would not be so if pre-existing law were inapplicable, *ab initio*, to nascent methods and means of warfare.

This analysis leaves only the third argument for inapplicability of humanitarian law to computer network attack—that it is not *armed* conflict, at least not in the absence of conventional hostilities. In exploring this prospect one might reflexively reach, as some have, for the UN Charter.[14] Article 2(4) of that constitutive instrument proscribes the "use of force," whereas Article 51 allows for forceful action in self-defense in the face of an "armed attack." If an act constitutes a "use of force" or an "armed attack" would it not logically be subject to the laws of "armed conflict," i.e., humanitarian law? If so, all that need be done is to determine what actions amount to a use of force or constitute an armed attack.[15]

Such an analysis confuses the *jus ad bellum* with the *jus in bello*. Articles 2(4) and 51, together with Chapter VII of the Charter, are the key prescriptive norms of the *jus ad bellum*. They govern when it is legitimate under international law (or at least Charter law) to resort to force, either as a tool of national policy or in the face of another State's decision to do so in pursuit of its own national interests. A State that has unlawfully resorted to force may subsequently carry out its operations in compliance with the *jus in bello*, which, as mentioned *supra*, governs the actual conduct of hostilities by the parties. For instance, during the Falklands/Malvinas conflict Argentina wrongfully invaded British territory, but generally abided by the rules of warfare. Similarly, many commentators urge that Operation ALLIED FORCE, NATO's 1999 Kosovo bombing campaign, violated the *jus ad bellum*, but was conducted in substantial compliance with the laws governing armed conflict.[16] Conversely, a State (or its military) that lawfully resorts to force may subsequently violate humanitarian law principles. As an example, it seems clear that Russia is entitled to maintain order in Chechnya; but it is equally clear that in doing so its forces have regularly violated both the law of non-international armed conflict and human rights law.[17] The point is that the *jus ad bellum* and *jus in bello* are normatively distinct. Professor Leslie Green has very pragmatically noted this distinction and its relevance to military personnel:

> Members of the armed forces are not concerned with the manner in which a conflict begins, nor whether it is legal or illegal. So far as they are concerned, the law of armed conflict comes into operation and they must abide by it from the moment that hostilities begin and they are required to participate therein.[18]

The task at hand, therefore, is to query when "hostilities" have begun. Tautologically, the answer is that hostilities commence once humanitarian law applies. Common Article 2 to the four 1949 Geneva Conventions provides that the conventions apply, aside from specific provisions that pertain in peacetime, "to all cases of declared war or of any other *armed conflict* which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them."[19] The 1977 Protocol Additional I, which, like the conventions pertains to international armed conflict, adopts the same "armed conflict" standard, one that has become an accepted customary law threshold for humanitarian law.[20] The fact that the 1977 Protocol Additional II also embraces the term "armed conflict,"[21] albeit in the context of *non*-international armed conflict, demonstrates that armed conflict is a condition determined by its nature, rather than its participants,[22] location,[23] or, as was formerly the case with "war," declaration of the belligerents.[24]

It seems relatively clear, then, that humanitarian law is activated through the commencement of armed conflict. But what is armed conflict? Commentaries published by the International Committee of the Red Cross to the 1949 Geneva Conventions and the 1977 Protocols Additional take a very expansive approach towards the meaning of the term. The former define armed conflict as "[a]ny difference arising between two States and leading to the *intervention of armed forces* . . . even if one of the Parties denies the existence of a state of war. It makes no difference how long the conflict lasts, or how much slaughter takes place."[25] Similarly, Protocol Additional I's commentary provides that "humanitarian law . . . covers any dispute between two States involving the *use of their armed forces*. Neither the duration of the conflict, nor its intensity, play a role. . . ."[26] Protocol Additional II's commentary describes armed conflict as "the existence of open *hostilities between armed forces* which are organized to a greater or lesser degree."[27] The *sine qua non* in all three cases is commitment of armed forces.

But a dispute or difference resulting in the engagement of armed forces cannot be the sole criterion. Military forces are used on a regular basis against adversaries without necessarily producing a state of armed conflict—consider aerial reconnaissance/surveillance operations as just one example. Further, it is now generally accepted that isolated incidents such as border clashes or small-scale raids do not rise to the level of armed conflict as that term is employed in humanitarian law.[28] Accordingly, State practice, supplemented by the writings of publicists, illustrates that Protocol Additional I's dismissal of intensity and duration has proven slightly overstated.

Instead, the reference to armed forces is more logically understood as a form of prescriptive shorthand for activity of a particular nature and intensity. At the time the relevant instruments were drafted, *armed* forces were the entities that conducted the contemplated activity at the requisite level of intensity; by focusing on the armed forces, the intended ends were achieved. Restated, the relevant provisions of the conventions and their commentaries were actor-based because citing the actors engaged in the undesirable conduct—armed forces—was, at the time, a convenient and reliable method for regulating it.

And what was that conduct? The logical answer is found in the underlying purposes of humanitarian law. A review of its instruments and principles makes clear that protecting individuals who are not involved in the hostilities directly, as well as their property, lies at their core.[29] Most notably, protected entities include civilians and civilian objects, as well as those who are *hors de combat* (e.g., wounded or captured personnel) or provide humanitarian services (e.g., medical personnel). As for the protection they are entitled to, it is usually framed in terms of injury or death or, in the case of property, damage or

destruction. These Geneva law purposes are complemented by Hague law norms intended to limit suffering generally through restrictions on certain weaponry and methods of warfare.[30]

This excessively abbreviated summarization of humanitarian law's fundamental purposes elucidates the term armed conflict. Armed conflict occurs when a group takes measures that injure, kill, damage, or destroy. Also included are actions intended to cause such results or in which they are the foreseeable consequences thereof. Because the issue is the *jus in bello* rather than *ad bellum*, the motivation underlying the actions is irrelevant. So too is their wrongfulness or legitimacy. Thus, for example, the party that commences the armed conflict by committing such acts may be acting in legitimate anticipatory (or interceptive) self-defense; nevertheless, as long as the actions were intended to injure, kill, damage, or destroy, humanitarian law governs them. It should be noted that given the current weight of opinion, actions that are sporadic or isolated in nature would not suffice. Additionally, because the issue is the law applicable to international armed conflict, the relevant actions must be attributable to a State.[31]

Returning to the topic at hand, and quite aside from *ad bellum* issues, humanitarian law principles apply whenever computer network attacks can be ascribed to a State, are more than merely sporadic and isolated incidents, and are either intended to cause injury, death, damage, or destruction (and analogous effects), or such consequences are foreseeable. This is so even though classic *armed* force is not being employed. By this standard, a computer network attack on a large airport's air traffic control system by agents of another State would implicate humanitarian law. So too would an attack intended to destroy oil pipelines by surging oil through them after taking control of computers governing flow,[32] causing the meltdown of a nuclear reactor by manipulation of its computerized nerve center, or using computers to trigger a release of toxic chemicals from production and storage facilities. On the other hand, humanitarian law would not pertain to disrupting a university intranet, downloading financial records, shutting down Internet access temporarily, or conducting cyber espionage because, even if part of a regular campaign of similar acts, if the foreseeable consequences would not include injury, death, damage, or destruction.

It should be apparent that, given advances in methods and means of warfare, especially information warfare, it is no longer sufficient to apply an actor-based threshold for application of humanitarian law; instead, a consequence-based one is more appropriate. This is hardly a jurisprudential epiphany. No one would deny, for instance, that biological or chemical warfare (which does not involve delivery by kinetic weapons) is subject to humanitarian law. A

consequence-based threshold is also supported by the fact that once armed conflict has commenced (and except for prohibitions relevant to particular weapons), the means by which injury, death, damage or destruction are produced have no bearing on the legality of the causal act. Intentionally targeting a civilian or other protected persons or objects is unlawful irrespective of the method or means used. Starvation, suffocation, beating, shooting, bombing, even cyber attack—all are subject to humanitarian law based on the fact that a particular consequence results. That this is so counters any assertion that, standing alone, cyber attacks are not subject to humanitarian law because they are not "armed" force. On the contrary, they may or may not be, depending on their nature and likely consequences.

Computer Network Attack Targets

As has been discussed, computer network attacks are subject to humanitarian law if they are part and parcel of either a classic conflict or a "cyber war" in which injury, death, damage, or destruction are intended or foreseeable. This being so, it is necessary to consider the targets against which computer network attacks may be directed.

A useful starting point is to frame the conduct that is subject to the prescriptive norms governing targeting. Because most relevant Protocol Additional I provisions articulate standards applicable to Parties and non-Parties (as a restatement of binding customary law) alike, that instrument serves as an apt point of departure.[33] Article 48, the basic rule governing the protection of the civilian population, provides that "Parties to the conflict . . . shall direct their operations only against military objectives."[34] On its face, Article 48 would seem to rule out *any* military operation, including CNA, directed against other than purely military objectives. In fact, it does not. In subsequent articles, proscriptions are routinely expressed in terms of "attacks." Thus, "the civilian population as such, as well as individual civilians, shall not be the object of attack"[35]; "civilian objects shall not be the object of attack"[36]; "indiscriminate attacks are forbidden"[37]; "attacks shall be limited strictly to military objectives"[38]; and so forth. The term is expressly defined in Article 49: "'Attacks' means acts of violence against the adversary, whether in offence or in defence." As a general matter then, the prohibition is not so much on targeting non-military objectives as it is on *attacking* them, specifically through the use of violence. This interpretation is supported by the text of Article 51, which sets forth the general principle that the "civilian population and individual civilians shall enjoy general protection against *dangers* arising from military operations," and which prohibits "acts or threats of *violence*

the primary purpose of which is to spread terror among the civilian population,"[39] as well as the commentary to Article 48, which notes that "the word 'operation' should be understood in the context of the whole of the Section; it refers to military operations during which *violence* is used."[40]

In light of this interpretation, does computer network attack fall outside the ambit of "attacks" because it does not employ violence? No, and for precisely the same reason that armed attacks can include cyber attacks. "Attacks" is a term of prescriptive shorthand intended to address specific consequences. It is clear that what the relevant provisions hope to accomplish is shielding protected individuals from injury or death and protected objects from damage or destruction. To the extent the term "violence" is explicative, it must be considered in the sense of violent *consequences* rather than violent *acts*. Significant human physical or mental suffering[41] is logically included in the concept of injury; permanent loss of assets, for instance money, stock, etc., directly transferable into tangible property likewise comprises damage or destruction. The point is that inconvenience, harassment, or mere diminishment in quality of life does not suffice; human suffering is the requisite criterion. As an example, a major disruption of the stock market or banking system might effectively collapse the economy and result in widespread unemployment, hunger, mental anguish, etc., a reality tragically demonstrated during the Depression of the 1930s. If it did cause this level of suffering, the CNA would constitute an attack, as that term is understood in humanitarian law.

Other articles within the section sustain this reading. For instance, the rules of proportionality speak of "loss of civilian life, injury to civilians, damage to civilians objects, or a combination thereof,"[42] those relating to protection of the environment refer to "widespread, long-term, and severe damage,"[43] and the protection of dams, dykes, and nuclear electrical generating stations is framed in terms of "severe losses among the civilian population."[44] Furthermore, during the negotiation of Protocol Additional I, the issue of whether laying landmines constituted an attack arose. Most agreed that it did because "there is an attack whenever a person is directly endangered by a mine laid."[45] By analogy, a computer network attack which foreseeably endangers protected persons or property would amount to an attack.

Return now to Article 48. In the context of computer network attack, and as a general rule (various other specific prohibitions are discussed *infra*), the article would prohibit those CNA operations directed against non-military objectives that are intended to, or would foreseeably, cause injury, death, damage, or destruction. Unless otherwise prohibited by specific provisions of humanitarian law, CNA operations unlikely to result in the aforementioned consequences are

permissible against non-military objectives, such as the population.[46] As a result of this distinction, the need to carefully assess whether or not an information warfare operation is or is not an "attack" is greatly heightened. In the past, analysis of this matter approximated a *res ipsa loquitor* approach. However, CNA is much more ambiguous than traditional military operations, thereby demanding a more challenging consequence-based consideration.

While CNA does dramatically expand the possibilities for "targeting" (but not attacking) non-military objectives, it is unfair to characterize this as a weakening of the prescriptive architecture. Instead, it simply represents an expansion of permissible methods and means resulting from advances in technology; existing norms remain intact. Recall, for example, that psychological operations directed against the civilian population that cause no physical harm are entirely permissible, so long as they are not intended to terrorize.[47] This is so whether the motivation for the operations is military in nature or not. Nevertheless, although the objective regime is a constant, the advent of CNA reveals a normative lacuna that, unless filled, will inevitably result in an expansion of war's impact on the civilian population.

Assuming a CNA operation is an "attack," what can be targeted? Analytically, potential targets can be classified into three broad categories: 1) combatants and military objectives; 2) civilians and civilian objects; and 3) dual-use objects. Moreover, particular types of potential targets enjoy specific protection. It is useful to address each grouping separately.

Combatants and military objectives: Combatants and military objectives are by nature valid targets and may be directly attacked as long as the method used, as discussed in the next section, is consistent with humanitarian law restrictions. Those who plan or decide on attacks have an affirmative duty to "do everything feasible" to verify that intended targets are legitimate, i.e., that they do not enjoy immunity from attack under humanitarian law.[48]

A combatant is a member of the armed forces other than medical personnel and chaplains; armed forces include "all organized armed forces, groups and units which are under a command responsible to [a Party to the conflict] for the conduct of its subordinates. . . . [They must] be subject to an internal disciplinary system which, *inter alia*, shall enforce compliance with the rules of international law applicable in armed conflict."[49] Directing computer network attacks against combatants, for instance by causing a military air traffic control system to transmit false navigational information in order to cause a military troop transport to crash, is clearly permissible.

Military objectives are defined in Article 52 of Protocol Additional I as "those objects which by their nature, location, purpose or use make an effective

contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite advantage."[50] Military equipment and facilities, other than medical and religious items, are clearly military objectives, and thereby subject to direct computer network attack. However, determining which objects are military objectives beyond these obvious exemplars is often difficult.[51] The problem lies in ascertaining the required nexus between the object to be attacked and military operations.

The crux of the dilemma is interpretation of the terms "effective" and "definite." Some, such as the International Committee of the Red Cross, define them very narrowly. In the ICRC commentary to the protocol, effective contribution includes objects "directly used by the armed forces" (e.g., weapons and equipment), locations of "special importance for military operations" (e.g., bridges), and objects intended for use or being used for military purposes.[52] As to "definite military advantage," the commentary excludes attacks that offer only a "potential or indeterminate" advantage.[53] By contrast, the United States, which does not dispute the wording of the definition, would include economic targets that "indirectly but effectively support and sustain the enemy's war-fighting capability," a particularly expansive interpretation.[54]

This difference has interesting implications for computer network attack. Can a banking system be attacked because wealth underpins a military's sustainability? What about the ministry responsible for taxation? The stock market? Are attacks on brokerage firms acceptable because they will undermine willingness to invest in the economy? If a country disproportionately relies on a particular industry to provide export income (e.g., oil), can computer network attack be used to disrupt production and distribution? The issue of striking economic targets is a particularly acute one because the operation of most is computer intense in nature, and thereby very appealing to information warfare targeteers.

The threshold issue, recalling the discussion *supra*, is whether or not the attack would cause injury, death, damage, or destruction. Once this determination is made, the differing interpretations of military objective would come into play, in all likelihood leading to disparate results on the legitimacy of striking the target. On the other hand, if the operation were designed to cause, e.g., mere inconvenience, it would not rise to the level of an attack and would thus be permissible regardless of the target's nexus, or lack thereof, to military operations. For instance, if the Serbian State television station had been targeted by CNA rather than kinetic weapons during NATO strikes on Belgrade in April 1999, there might well have been no consequent injury, death, damage, or destruction; in that circumstance, criticism on the basis that a civilian target had

been hit would likely have fallen on deaf ears, thereby probably avoiding the negative publicity that resulted, as well as the pending litigation in the European Court of Human Rights.[55]

Civilians and civilian objects: Civilians are those not considered combatants,[56] whereas a civilian object is one that is not a military objective.[57] The prohibition on attacking civilians and civilian objects is nearly absolute. Specifically, Protocol Additional I provides:

> Article 51.2. The civilian population, as such, as well as individual civilians shall not be the object of attack. Acts or threats of violence the primary purpose of which is to spread terror among the civilian population are prohibited.
>
> Article 52. Civilian objects shall not be the object of attack or of reprisals.[58]

Doubts as to the character of an object or individual are to be resolved in favor of finding civilian status.[59] Again, in the case of computer network attack, the threshold question is whether or not the attack is intended to, or forseeably will, cause injury, death, damage, or destruction; if so, the prohibitions set forth earlier, which undeniably restate existing customary law, apply.

Unfortunately, the norms, albeit clear on their face, are subject to interpretive difficulties. The differing standards for distinguishing civilian objects from military objectives have already been highlighted. Similar disparities surround when a civilian may be attacked. Protocol Additional I allows for this possibility only in the case of a civilian taking a "direct part in hostilities," a standard described in the commentary as "acts of war which by their nature or purpose are likely to cause actual harm to the personnel or equipment of the enemy armed forces."[60] This is the illegal combatant problem. Some would limit civilian immunity even more severely by, for instance, characterizing mission-essential civilians working at a base during hostilities, though not engaged directly in acts of war, as legitimate targets.[61]

In the context of information operations, the civilian issue is an important one. Some countries have elected to contract out information warfare functions, whether those functions involve the maintenance of assets or the conduct of operations. Moreover, computer network attack is a function that may be tasked to government agencies other than the military. In the event civilian contractors or non-military personnel are in a support role that is essential to the conduct of operations, for instance maintaining CNA equipment, by the latter interpretation they would be directly targetable. Further, because they are valid targets, any injury caused them would not be calculated when assessing whether

an attack is proportional (see discussion *infra).* On the other hand, narrowly applying the "direct part in hostilities" standard would preserve the protection they enjoy as civilians, though if captured they would be entitled to prisoner of war status as persons "accompanying the armed forces."[62]

Should civilians engage in computer network attack themselves, the problem becomes more complex. If the CNA results, or foreseeably could result, in injury, death, damage, or destruction, then the "perpetrators" would be illegal combatants. This status attaches because they have taken a direct part in hostilities without complying with the criteria for characterization as a combatant. As illegal combatants, they may be directly attacked, any injury suffered by them would be irrelevant in a proportionality calculation, and in the event of their capture they would not be entitled to prisoner of war status.

By contrast, if the civilians involved were conducting computer network operations that did not rise to the level of "attacks," they would not be illegal combatants because they would have committed no "acts of war that by their nature or purpose are likely to cause actual harm to the personnel or equipment of the enemy armed forces." Their civilian status and its corresponding protections would remain intact. Nevertheless, as with support personnel, if captured while attached to a military unit and accompanying that unit, these civilians would be classed as prisoners of war.[63] Of course, the facility and equipment being used to conduct the operations might well be valid military objectives and, as a result, be subject to attack; but the operators themselves could not be directly attacked.

As should be apparent, the use of civilians, whether contractors or government employees, is fraught with legal pitfalls. Clearly, a prudent approach would be to employ military personnel for information warfare purposes.

Dual-use objects: A dual-use object is one that serves both civilian and military purposes. Examples of common dual-use objects (or objectives) include airports, rail lines, electrical systems, communications systems, factories that produce items for both the military and the civilian population, and satellites such as INTELSAT, EUROSAT and ARABSAT. If an object is being used for military purposes, it is a military objective vulnerable to attack, including computer network attack. This is true even if the military purposes are secondary to the civilian ones.

Several caveats are in order. First, whether or not an object is a military objective may turn on whether the narrow or broad definition of the term, a matter discussed *supra*, is used. Second, whether an object is dual-use, and therefore a military objective, will depend on the nature of the specific conflict. An airfield may be utilized for logistics purposes in one conflict, but serve no military function in another. Third, an object that has the potential for military usage, but is

presently solely used for civilian purposes, is a military objective if the likelihood of use is reasonable and not remote in the context of the particular conflict underway. Finally, dual-use objects must be carefully measured against the requirements of discrimination and proportionality, discussed *infra,* because by definition an attack thereon risks collateral damage and incidental injury to civilians or civilian objects.

Specifically protected objects: In addition to the general rules regarding the protection of the civilian population, certain objects enjoy specific protection. A controversial category of specially protected objects is dams, dikes, and nuclear electrical generating stations. Because of their reliance on computer and computer networks, such facilities are especially vulnerable to CNA. Article 56 of Protocol Additional I, a provision opposed by the United States, forbids an attack on these facilities if the attack might "cause the release of dangerous forces [e.g., water or radioactivity] and consequent severe losses among the civilian population."[64] This prohibition applies even if they are military objectives. Interestingly, CNA offers a fairly reliable means of neutralizing such facilities without risking the release of dangerous forces, a difficult task when using kinetic weapons.

Conducting attacks that starve the civilian population or otherwise deny it "indispensable objects,"[65] even if enemy armed forces are the intended "victims," is prohibited.[66] Indispensable objects include such items as foodstuffs, crops, livestock, or drinking water. Applying this restriction, computer networks attacks against, for instance, a food storage and distribution system or a water treatment plant serving the civilian population would be impermissible even if military forces also rely on them.

Protocol Additional I further prohibits military operations likely to cause widespread, long-term, and severe damage to the environment,[67] although the United States does not recognize the provision as a restatement of customary law. Computer network attacks might conceivably cause such devastation. An attack on a nuclear reactor could result in a meltdown of its core and consequent release of radioactivity. Similarly, CNA could be used to release chemicals from a storage or production facility or rupture a major oil pipeline. Many other possibilities for the causation of environmental damage through CNA exist. It is important to note that the prohibition applies regardless of whether or not the attack is targeted against a valid military objective and even if it complies with the principle of proportionality. Once the requisite quantum of damage is expected to occur, the operation is prohibited.

There are a number of other objects, persons, and activities that enjoy special protected status, and which are susceptible to computer network attack, but which do not present unique CNA opportunities or challenges. For example,

military and civilian medical units and supplies are exempt from attack unless being used for military purposes;[68] the same is generally true of medical transport.[69] So too are cultural objects, places of worship,[70] and civil defense shelters, facilities, and material.[71] Additionally, humanitarian relief activities must not be interfered with.[72] By these prohibitions, for example, a computer network attack to alter blood type information in a hospital's data bank, deny power to a bomb shelter, or misroute humanitarian relief supplies would all be unlawful. Of course, misuse of protected items or locations for military purposes renders them valid military objectives that may be attacked.

Finally, there are limitations on striking certain objects or individuals in reprisal, including reprisals by computer network attack. Reprisals are otherwise unlawful actions taken during armed conflict in response to an adversary's own unlawful conduct. They must be designed solely to cause the adversary to act lawfully, be preceded by a warning (if feasible), be proportionate to the adversary's violation, and cease as soon as the other side complies with the legal limitations on its conduct. The right to conduct reprisals has been severely restricted in treaty law, much of which expresses customary law. There are specific prohibitions on reprisals conducted against civilians; prisoners of war; the wounded, sick, and shipwrecked; medical and religious personnel and their equipment; protected buildings, equipment, and vessels; civilian objects; cultural objects; objects indispensable for the survival of the civilian population; works containing dangerous forces; and the environment.[73] Essentially, this leaves only combatants and military objectives subject to reprisals. Of course, in most cases a computer network attack conducted against them would be lawful at any rate.[74]

In fairness, it should be acknowledged that certain countries argue that the Protocol Additional I restrictions on reprisals fail to reflect customary law. The United States, while accepting that most reprisals against civilians would be inappropriate (and illegitimate), asserts that the absolute prohibition thereon "removes a significant deterrent that presently protects civilians and other war victims on all sides of the conflict."[75] The United Kingdom issued a reservation on precisely the same point when it became a Party to the protocol.[76] For these and other countries that have adopted this position, reprisatory computer network attacks are issues of policy, not law.

Limits on Striking Legitimate Targets

The core prescriptions on striking legitimate targets are based in the principle of discrimination.[77] It is this principle which most clearly expresses humanitarian law's balancing of State-centric interests in resorting to force against the

more broadly based humanitarian interest in shielding non-participants from the effects of what is, at best, an unfortunate necessity.

Discrimination is bifurcated in nature. Applied to weapons, it limits the use of those that are incapable of distinguishing between combatants and military objectives on the one hand and civilians, civilian objects, and other protected entities on the other. Applied to tactics and the *use* of weapons, it requires an effort to distinguish between the two categories when conducting military operations. Protocol Additional I articulates this difference in Article 51.4:

> Indiscriminate attacks are: (a) those which are not directed at a specific military objective; (b) those which employ a method or means of combat which cannot be directed at a specific military objective; or (c) those which employ a method or means of combat the effects of which cannot be limited as required by this Protocol; and consequently, in each such case, are of a nature to strike military objectives and civilians or civilian objects without distinction.

Subparagraph (a) refers to indiscriminate use, whereas (b) and (c) describe indiscriminate weapons. The indiscriminate use aspect of discrimination consists of three related components—distinction, proportionality, and minimizing collateral damage and incidental injury.[78]

Indiscriminate weapons: Computer network attacks are mounted by a weapon system consisting of a computer, computer code, and a means by which that code is transmitted. Obviously, the computer itself is not indiscriminate for it can very discretely send code to particular computers and networks. The sending of e-mail is an apt example. By contrast, code can be written that is very, perhaps intentionally, indiscriminate. The classic example is a virus that passes from computer to computer free from the control of its originator. Because the code, even if an uncontrollable virus, can be targeted at particular military objectives, it is not indiscriminate on the basis that it cannot be directed. However, such code may be indiscriminate on the ground that its *effects* cannot be limited. In many cases, once viral code is launched against a target computer or network, the attacker will have no way to limit its subsequent retransmission. This may be true even in a closed network, for the virus could, as an example, be transferred into it by diskette. Simply put, malicious code likely to be uncontrollably spread throughout civilian systems is prohibited as an indiscriminate weapon.

One must be careful not to overstate the restriction. Note that Article 51.4 cites "methods and means of combat." A means of combat is defined in Protocol Additional I's commentary as a "weapon," whereas a method of combat is the way a weapon is used.[79] The plain meaning of "weapon" is something that

can be used to *attack* an adversary. Drawing on the analysis *supra* regarding the humanitarian law term "attacks," computer code is only part of a *weapon* system when it can cause the effects encompassed in that term—injury, death, damage, and destruction (including related effects like severe mental suffering, terror, suffering, etc.). In the event it cannot, it is not part of a weapon system, and thus would not be prohibited, at least not on the ground that it is indiscriminate.

Distinction: The principle of distinction, unquestionably part of customary humanitarian law, is set forth in Protocol Additional I, Article 48: "[T]he Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives." Whereas the prohibition on attacking civilians directly rendered a specific category of potential targets off-limits, the distinction requirement extends protection to cases in which an attack may not be directed against civilian or civilian objectives specifically, but in which there is a high likelihood of striking them nonetheless. An example would be firing a weapon, though capable of being aimed, blindly.

This is a particularly relevant prohibition in the context of computer network attack. For example, it would embrace situations where it is possible to discretely target a military objective through a particular means of CNA, but instead a broad attack likely to affect civilian systems is launched. Such an attack would be analogous to the Iraqi SCUD attacks against Saudi and Israeli population centers during the 1990–91 Persian Gulf War.[80] The SCUD is not an inherently indiscriminate weapon. Indeed, it is easily capable of being aimed with sufficient accuracy against, for instance, military formations in the desert. However, use of SCUDS against population centers was indiscriminate even if the Iraqi intent was to strike military objectives situated therein; the likelihood of striking protected persons and objects so outweighed that of hitting legitimate targets that the use was improper. Given the interconnectivity of computer systems today, computer network attacks could readily be launched in an analogous fashion.

Proportionality: Scienter distinguishes the principle of proportionality from that of distinction. Distinction limits direct attacks on protected persons or objects and those in which there is culpable disregard for civilian consequences. By contrast, proportionality governs those situations in which harm to protected persons or objects is the foreseeable consequence of an attack, but not its intended purpose. The principle is most often violated (sometimes in an unintended but culpably negligent fashion) as a result of: 1) lack of sufficient knowledge or understanding of what is being attacked; 2) an inability to surgically craft the

amount of "force" being applied against a target; and 3) the inability to ensure the weapon strikes precisely the right aim point.[81] All three pitfalls could surface in the context of computer network attack.

As set forth in Protocol Additional I, an attack is indiscriminate as violative of the principle of proportionality when it "may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated."[82] A concrete and direct advantage is "substantial and relatively close[;] . . . advantages which are hardly perceptible and those which would only appear in the long term should be disregarded."[83] Moreover, the advantage calculated is that resulting from the overall operation, not the individual attack itself.[84]

Basically, the principle of proportionality mandates a balancing test—one that is especially difficult to conduct because differing entities (suffering and damage v. military advantage) are being compared against each other in the absence of a common system of valuation. How should civilian passenger lives be weighed against military aircraft in a computer network attack on an air traffic control system? How much human suffering is acceptable when shutting down an electrical grid that serves both military and civilian purposes? Can computer network attacks be conducted against telecommunications if they result in degrading emergency response services for the civilian population? Complicating matters is the fact that the answers to these and similar questions, assuming there are any "right" answers, is contextual because the military advantage resulting from an attack always depends on the state of hostilities at the time.[85] Acknowledging the difficulty involved in making these types of determinations, the Protocol Additional I commentary notes that "[p]utting these provisions into practice . . . will require complete good faith on the part of the belligerents, as well as the desire to conform with the general principle of respect for the civilian population."[86]

Further complicating matters is the issue of reverberating effects, i.e., those effects not directly and immediately caused by the attack, but nevertheless the product thereof—it is the problem of the effects caused by the effects of an attack. The most cited example involves the attack on the Iraqi electrical grid during the 1991 Persian Gulf War. Although it successfully disrupted Iraqi command and control, the attack also denied electricity to the civilian population (a "first-tier" effect), thereby affecting hospitals, refrigeration, emergency response, etc. Similarly, when NATO struck at Yugoslavia's electrical supply network during Operation ALLIED FORCE, one consequence was shutting down drinking water pumping stations.[87] Such attacks set off "second-tier" suffering (a reverberating effect) of the population. Obviously, precisely the

same effects could have resulted had the attacks been conducted through CNA. Indeed, the problem of reverberating effects looms much larger in computer network than kinetic attacks due to the interconnectivity of computers, particularly that between military and civilian systems.

Reverberating effects bear on proportionality analysis because they must be considered when balancing collateral damage and incidental injury against military advantage. Unfortunately, and whether reverberating or direct, it is difficult to assess such damage and injury when caused by computer network attack absent an understanding of how the computer systems involved function and to which other systems they are linked. Despite this obstacle, planners and decision-makers have an affirmative duty to attempt to avoid collateral damage and incidental injury whenever feasible, a duty that necessarily implies an effort to ascertain the resultant damage or injury from an attack.[88] Given the complexity of computer network attack, the high likelihood of an impact on civilian systems, and the relatively low understanding of its nature and effects on the part of those charged with ordering the attacks, computer experts will have to be available to assess potential collateral and incidental effects throughout the mission planning process.[89] Additionally, modeling and simulation, like that already conducted for nuclear weapons, would prove invaluable in identifying possible reverberating effects; conducting them prior to the outbreak of hostilities—free from the fog, friction, and pace of war—would be well advised.

Minimizing collateral damage and incidental injury: Proportionality determinations establish whether a military objective may be attacked at all. However, even if the selected target is legitimate and the planned attack thereon would be proportional, the attacker has an obligation to select that method or means of warfare likely to cause the least collateral damage and incidental injury, all other things being equal (such as risk to the forces conducting the attack, likelihood of success, weapons inventory, etc.).[90] Additionally, whenever a choice is presented between military objectives that can be attacked to achieve a desired result, the attack which risks the least collateral damage and incidental injury must be chosen.[91]

The availability of computer network attack actually expands the options for minimizing collateral damage and incidental injury. Whereas in the past physical destruction may have been necessary to neutralize a target's contribution to the enemy's efforts, now it may be possible to simply "turn it off." For instance, rather than bombing an airfield, air traffic control can be interrupted. The same is true of power production and distribution systems, communications, industrial plants, and so forth. Those who plan and execute such operations must still be concerned about collateral damage, incidental injury, and reverberating

effects (consider the Iraqi electric grid example *supra*), but the risks associated with conducting classic kinetic warfare are mitigated significantly through CNA. Additionally, depending on the desired result, it may be possible to simply interrupt operation of the target. This tactic would be particularly attractive in the case of dual-use objectives. Consider an electrical grid. It might only be militarily necessary to shut the system down for a short period, for example, immediately preceding and during an assault. The system could be brought back up as soon as the pressing need for its interruption passed, thereby limiting the negative effects on the civilian population. Along the same lines, because targets are not physically damaged, and thus do not need to be repaired or rebuilt, the civilian population's return to normalcy at the end of the conflict would be facilitated.

There is, from a humanitarian point of view, one theoretical downside to the fact that CNA may sometimes cause less collateral damage and incidental injury than kinetic attacks—it might actually encourage attacks. This would be so in the case of an attack that could not pass the proportionality test if conducted kinetically, but could if accomplished by computer network attack. Should the CNA result in any collateral damage or incidental injury (albeit not enough to outweigh the resulting military advantage), the net result would be greater civilian suffering. While this is true, the better question from the humanitarian point of view is whether CNA causes more or less collateral damage and incidental injury overall, not merely as to a single operation. So long as the various limitations of the principle of discrimination are complied with, and without the benefit of a track record to draw on in making the assertion, it would seem that in humanitarian terms computer network attack is probably a step forward.

Perfidy: Although the core normative constraints on computer network attack derive from the principle of discrimination, several other related aspects of humanitarian law are implicated by this new means of warfare. One is the prohibition on perfidy. Perfidy is the feigning of protected status in order to take advantage of an adversary. Examples include pretending to be wounded or sick, to enjoy non-combatant status, or to surrender, and improperly displaying symbols that signify protected status, such as the red cross or red crescent. Perfidy is distinguished from ruses, which are acts intended to mislead an adversary and cause him to act recklessly, but which do not involve false claims of protected status. Ruses are lawful.

Information warfare, including computer network attack, opens many opportunities for ruses and perfidy. This is because both techniques are intended to convey false information. For instance, lawful ruses might include transmitting false data, meant to be intercepted by an adversary, regarding troop disposition

or movements. Alternatively, it might involve altering data in an adversary's intelligence databases, sending messages to enemy headquarters purporting to be from subordinate units, or passing instructions to subordinate units that appear to be from their headquarters.[92] All such activities would be perfectly legitimate.

On the other hand, any action intended to mislead the enemy into believing that one's forces enjoyed protected status in order to kill, injure, or capture the enemy would be illegitimate.[93] For instance, medical units and transports may use codes and signals established by the International Telecommunications Union, the International Civil Aviation Organization, and the International Maritime Consultative Organization to identify themselves.[94] Falsely transmitting such code/signals or, a more likely prospect in the computer network attack context, causing adversary systems to reflect receipt of such signals would be clear examples of perfidy. The Department of Defense has also opined that using "computer 'morphing' techniques to create an image of the enemy's chief of state informing his troops that an armistice or cease-fire agreement had been signed" would be a war crime if false.[95]

An interesting prospect would be routing a computer network attack through civilian systems, or otherwise feigning a civilian source. This might be done to later mask the source of attack or to inspire confidence in the target that the transmission was benign. Doing so would be prohibited both by the Protocol Additional I and customary law.[96] This is a very sensible restriction because a response to an attack apparently originating from a civilian source could be kinetic in nature.

It must be noted that the protocol's restriction on perfidy is limited to conduct calculated to facilitate killing, injuring, or capturing an adversary. The commentary thereto notes this limitation, but suggests that "there is more to an international treaty than the literal reading of all the words in the document may suggest; it represents one step forward in the ongoing evolution in relations between States."[97] Be that as it may, as the law stands today it would be permissible to disguise information warfare operations as civilian in origin if they were not related to killing, injuring, or capturing one's adversary. This standard is consistent with that employed *supra* regarding "armed" conflict and "attack." Moreover, the prohibition on misuse of protective codes and signals, such as those designed to identify medical facilities, are absolute, i.e., they apply regardless of the abuser's intent. As an example, usage merely to avoid attack is forbidden.

Civilian Shields: In theory, a computer attack might utilize a civilian network to shield itself against a response, either kinetic or through a counter-cyber attack. If the latter did not cause death or injury to civilians or damage

or destruction of protected objects, and therefore was not an "attack" in the humanitarian law sense, it would be permissible. On the other hand, if it might cause collateral damage or incidental injury, then any such effects on the civilian population would have to be considered in a proportionality analysis; civilians and civilian objects do not lose the protections of the law of armed conflict by the wrongful acts of others. Of course, the use of civilian shields is itself wrongful;[98] the party that subjects the civilian population or protected objects to risk by using them as shields is culpable under humanitarian law. This principle applies whether the attack is kinetic or computer in nature.

Mercenaries: Since computer network attacks can amount to both armed conflict and, in individual cases, an attack, restrictions on mercenaries may apply to those who conduct them. Mercenaries are specifically addressed in Protocol Additional I, although the restrictions contained therein are not customary in nature, a position strengthened by the absence of any mention of mercenaries in the Statute of the International Criminal Court.

By Article 47 of the protocol, a mercenary is any person who:

> (a) is specially recruited locally or abroad in order to fight in an armed conflict;
> (b) does, in fact, take a direct part in the hostilities;
> (c) is motivated to take part in the hostilities essentially by the desire for private gain and, in fact, is promised, by or on behalf of a Party to the conflict, material compensation substantially in excess of that promised or paid to combatants of similar ranks and functions in the armed forces of that Party;
> (d) is neither a national of a Party to the conflict nor a resident of territory controlled by a Party to the conflict;
> (e) is not a member of the armed forces of a Party to the conflict; and
> (f) has not been sent by a State which is not a Party to the conflict on official duty as a member of its armed forces.[99]

While Protocol Additional I does not actually prohibit mercenarism, because they are not combatants, mercenaries are not entitled to prisoner of war status. Therefore, like any other noncombatant who directly engages in hostilities, they may be tried under the domestic law of the State that captures them.[100]

Given the complexity of conducting computer network attacks, it is quite conceivable that States might hire non-nationals possessing the requisite expertise to mount them. If the CNA amount to an "attack," these individuals would be taking a "direct part in the hostilities." Assuming they met the other qualifying criteria for mercenaries, the Protocol Additional I provisions would apply. Interestingly, there is a financial incentive to outsource CNA because in

many cases hiring computer attack expertise would be far more cost-effective than hiring conventional attack mercenaries or even acquiring weapons for one's own forces.

Conclusion

By and large, as information warfare capabilities increase, existing humanitarian prescriptive norms will suffice to maintain the protection civilians, civilian objects, and other protected entities enjoy. However, certain novel aspects of CNA do pose new and sometimes troubling quandaries. The unease over the use of cyber warfare during NATO's campaign against Yugoslavia in 1999 is compelling evidence that the question of how humanitarian law bears on CNA remains unsettled.[101]

First, in order to apply extant norms to CNA, it is necessary to accept various interpretive premises. Most important are the consequence-based interpretations of "armed conflict" and "attack." Absent such understandings, the applicability, and therefore adequacy, of present-day humanitarian law principles would fall into question. Interestingly, consideration of computer network attack in the context of the *jus ad bellum* also leads to consequence-based interpretation.[102]

Second, even accepting the parameters resulting from the interpretations suggested, normative lacunae exist. Most notably, attacks against civilians and civilian objects that do not injure, kill, damage, or destroy (or otherwise produce the requisite level of suffering) are by and large permissible. Given that kinetic attacks usually have such effects, civilians and civilian objects enjoy broad protection during conventional military operations. However, computer network attack, because it may not amount to an *attack,* opens up many possibilities for targeting otherwise protected persons and objects. The incentive for conducting such operations grows in relation to the extent to which the "war aims" of the party conducting the CNA are coercive in nature; the desire to, e.g., "turn out the lights" to a civilian population in order motivate it to pressure its leadership to take, or desist from taking, a particular course of conduct (a step suggested by NATO's air commander during Operation ALLIED FORCE) will grow as the means for doing so expand.[103] This is an especially negative reality in humanitarian terms.

Third, and more encouraging, is the fact that CNA may make it possible to achieve desired military objectives with less collateral damage and incidental injury than in traditional kinetic attacks. Indeed, in certain cases, military commanders will be obligated to employ their cyber assets in lieu of kinetic weapons

when collateral and incidental effects can be limited.[104] That said, it will be critically important to carefully analyze the effects of such operations, particularly their reverberating effects, when assessing an attack's compliance with the principle of proportionality. This will require planning, legal, and computer experts to operate in concert throughout the targeting cycle.[105]

Finally, much as CNA challenges existing notions of "attack," it will also test traditional understanding of combatant status. This results from the use of typically civilian technology and know-how to conduct military operations via computer. Failure to strictly comply with the limitations on the participation of civilians in hostilities will inevitably lead to heightened endangerment of the civilian population and weaken humanitarian law norms.

So the jury remains out. While humanitarian law in its present form generally suffices to safeguard those it seeks to protect from the effects of computer network attack, and even though it offers the promise of periodically enhancing such protection, significant prescriptive fault lines do exist. Thus, as capabilities to conduct computer network attacks increase, both in terms of sophistication and availability, continued normative monitoring is absolutely essential. We must avoid losing sight of humanitarian principles, lest the possible in warfare supplant the permissible.

Notes

* An abbreviated version of this chapter appears in the *International Review of the Red Cross* (2002) edition commemorating the 25th anniversary of the Protocols Additional.

1. The United States National Military Strategy cites information superiority as a key element of its strategy for this century. "Information superiority is the capability to collect, process, and disseminate an uninterrupted flow of precise and reliable information, while exploiting and denying an adversary's ability to do the same." Chairman of the Joint Chiefs of Staff, National Military Strategy, (1997), www.dtic.mil/jcs/nms/strategy.htm, at n.p. For an excellent collection of essays on the nature of war in the 21st century, see FUTURE WARFARE ANTHOLOGY (Robert H. Scales ed., 2000). On the specific issue of information and conflict, see STEVEN METZ, ARMED CONFLICT IN THE 21ST CENTURY: THE INFORMATION REVOLUTION AND POST-MODERN WARFARE (2000); WILLIAM A. OWENS & EDWARD OFFLEY, LIFTING THE FOG OF WAR (2000); THE INFORMATION REVOLUTION AND NATIONAL SECURITY (Thomas E. Copeland ed., 2000); DAVID S. ALBERTS, JOHN J. GARSTKA & FREDERICK P. STEIN, NETWORK CENTRIC WARFARE: DEVELOPING AND LEVERAGING INFORMATION SUPERIORITY (1999); DAN KUEHL, STRATEGIC INFORMATION WARFARE: A CONCEPT (1999); THE CHANGING ROLE OF INFORMATION WARFARE (Zalmay Khalilzad & John White eds., 1999); DOROTHY E. DENNING, INFORMATION WARFARE AND SECURITY (1998); JAMES ADAMS, THE NEXT WORLD WAR: COMPUTERS ARE THE WEAPONS AND THE FRONT LINE IS EVERYWHERE (1998).

2. Chairman of the Joint Chiefs of Staff, Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1-02, April 12, 2001, at 203 [hereinafter Joint Pub 1-02]. Operations that might constitute information operations include operations security,

psychological operations, military deception, electronic warfare, physical attack, and computer network attack. *See* Chairman of the Joint Chiefs of Staff, Joint Publication 3-13, Joint Doctrine for Information Operations, at I-9, (1998) [hereinafter Joint Pub 3-13].

3. At the strategic level, IO can be employed to "achieve national objectives by influencing or affecting all elements (political, military, economic, or informational) of an adversary's or potential adversary's national power while protecting similar friendly elements." At the operational level, the focus of IO is "on affecting adversary lines of communication (LOCs), logistics, command and control (C2), and related capabilities and activities while protecting similar friendly capabilities and activities." Finally, at the tactical level the objective is to affect adversary "information and information systems relating to C2, intelligence, and other information-based processes directly relating to the conduct of military operations. . . ." Joint Pub 3-13, *supra* note 2, at I-2–I-3.

4. Joint Pub 1-02, *supra* note 2, at 203.

5. *Id.* at 88. The USAF Intelligence Targeting Guide, AF Pamphlet 14-210, Feb, 1, 1998, para. 11.4.3, notes IW employment concepts:

> Corruption – The alteration of information content; the manipulation of data to make it either nonsensical or inaccurate. Destroying existing knowledge.
>
> Deception – A specific type of corruption; the alteration of, or adding to, information to portray a situation different from reality. Creating false knowledge to include masquerading.
>
> Delay – The reversible slowing of the flow of information through the system, and the slowing of the acquisition and dissemination of new knowledge.
>
> Denial – The reversible stopping of the flow of information for a period of time; although the information may be transmitted and used within friendly territory, the adversary is denied access to it. The prevention of the acquisition and dissemination of new knowledge.
>
> Disruption – The reduction of the capacity to provide and/or process information (reversible). This is a combination of delay and corruption. The delay of the acquisition and dissemination of new knowledge and the destruction of existing knowledge.
>
> Degradation – The permanent reduction in the capacity to provide and/or process information.
>
> Destruction – The destruction of information before it can be transmitted; the permanent elimination of the capacity to provide and/or process information.

6. Thus, electronic attack (EA) would not fall within this category. For instance, using an electromagnetic pulse to destroy a computer's electronics would be EA, whereas transmitting a code or instruction to a system's central processing unit to cause the power supply to short out would be CNA. *Id.*

7. On CNA and the *jus ad bellum*, that body of international law governing the legality of the resort to force by States, see Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUMBIA JOURNAL OF TRANSNATIONAL LAW 885 (1999); Richard Aldrich, *How Do You Know You are at War in the Information Age?*, 22 HOUSTON JOURNAL OF INTERNATIONAL LAW 223 (2000).

8. For a discussion of CNA in the context of both law and ethics that concludes a new convention is required, see William J. Bayles, *The Ethics of Computer Network Attack*, PARAMETERS, Spring 2001, at 44.

9. On this point see Emily Haslam, *Information Warfare: Technological Changes and International Law*, 5 JOURNAL OF CONFLICT AND SECURITY LAW 157 (2000), particularly her discussion of points made in Richard Aldrich, *The International Legal Implications of Information Warfare*,

AIRPOWER JOURNAL, Fall 1996, at 99, and Mark Shulman, *Discrimination in the Laws of Information Warfare*, 37 COLUMBIA JOURNAL OF TRANSNATIONAL LAW 939 (1999).

10. Hague Convention IV Respecting the Laws and Customs of War on Land, Oct. 18, 1907, pmbl., 36 Stat. 2295, 1 Bevans 634, reprinted in ADAM ROBERTS & RICHARD GUELFF, DOCUMENTS ON THE LAWS OF WAR 67 (3d ed. 2000); Protocol Additional (I) to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, art. 1(2), Dec. 12, 1977, 1125 U.N.T.S. 3, 16 INTERNATIONAL LEGAL MATERIALS 1391 (1977), *reprinted in* ROBERTS & GUELFF, *supra,* at 419 [hereinafter Protocol Additional I].

11. The Statute of the International Court of Justice defines custom as "a general practice accepted by law." Statute of the International Court of Justice, June 26, 1977, art. 38(1)(b), 59 Stat. 1031, T.S. No. 933, 3 Bevans 1153, 1976 Y.B.U.N. 1052. The Restatement notes that custom "results from a general and consistent practice of states followed by them from a sense of legal obligation." Restatement (Third), Foreign Relations Law of the United States, sec. 102(2) (1987). See also North Sea Continental Shelf Cases, 1969 I.C.J. 3, 44 ("Not only must the acts concerned amount to settled practice, but they must also be such, or be carried out in such a way, as to be evidence of a belief that this practice is rendered obligatory by the existence of a rule requiring it."); The Paquete Habana, 175 US 677, 20 S.Ct. 290, 44 L.Ed 320 (1900); The Case of the S.S. Lotus (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10(1927); Asylum Case (Col. v. Peru), 1950 I.C.J. 266; Case Concerning Right of Passage over Indian Territory (Port. v. India), 1960 I.C.J. 6. For academic comment on customary international law, see Jack L. Goldsmith & Eric A. Posner, *Understanding the Resemblance Between Modern and Traditional Customary International Law*, 40 VIRGINIA JOURNAL OF INTERNATIONAL LAW 639 (2000); Patrick Kelly, *The Twilight of Customary International Law*, 40 VIRGINIA JOURNAL OF INTERNATIONAL LAW 449 (2000); ANTHONY A. D'AMATO, THE CONCEPT OF CUSTOM IN INTERNATIONAL LAW (1971).

12. Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion), 1996 I.C.J. 226 (July 8), 35 INTERNATIONAL LEGAL MATERIALS 809, para. 85.

13. Protocol Additional I, *supra* note 10, art. 36: "In the study, development, acquisition or adoption of new weapons, means or methods of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party." For the United States, the weapon review is required by Department of Defense Instruction 5000.2, Operation of the Defense Acquisition System, Oct. 23, 2000, para. 4.7.3.1.4. It provides, in relevant part, that "DoD acquisition and procurement of weapons and weapon systems shall be consistent with all applicable domestic law and all applicable treaties, customary international law, and the law of armed conflict (also known as the laws and customs of war) . . . . Additionally, legal reviews of new, advanced or emerging technologies that may lead to development of weapons or weapon systems are encouraged."

14. For instance, see the analysis in Robert G. Hanseman, *The Realities and Legalities of Information Warfare*, 42 AIR FORCE LAW REVIEW 173, 183–184 (1997).

15. *See generally*, Schmitt, *supra* note 7.

16. *See generally*, contributions to *Symposium: The International Legal Fallout from Kosovo*, 12 EUROPEAN JOURNAL OF INTERNATIONAL LAW 391 (2001); Bruno Simma, *NATO, the UN and the Use of Force: Legal Aspects*, 10 EUROPEAN JOURNAL OF INTERNATIONAL LAW 1 (1999); Antonio Cassese, *Ex iniuria ius oritur: Are We Moving towards International Legitimation of Forcible Humanitarian Countermeasures in the World Community*, 10 EUROPEAN JOURNAL OF INTERNATIONAL LAW 23 (1999).

17. For a description of Russian actions, see Human Rights Watch, World Report 2001 (Russia), www.hrw.org/wr2k1. The abuses were condemned in UN Commission on Human

Rights Resolution 2001/24, Situation in the Republic of Chechnya of the Russian Federation, UN Doc. E/CN.4/RES/2001/24, April 20, 2001.

18. LESLIE C. GREEN, THE CONTEMPORARY LAW OF ARMED CONFLICT 70 (2d ed. 2000).

19. Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, art. 2, 6 U.S.T. 3114, 75 U.N.T.S. 31 [hereinafter GC I]; Geneva Convention for the Amelioration of the Condition of the Wounded, Sick and Shipwrecked Members of the Armed Forces at Sea, Aug. 12, 1949, art. 2, 6 U.S.T. 3217, 75 U.N.T.S. 85 [hereinafter GC II]; Geneva Convention Relative to the Treatment of Prisoners of War, Aug. 12, 1949, art. 2, 6 U.S.T. 3316, 75 U.N.T.S. 135 [hereinafter GC III]; and Geneva Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, art. 2, 6 U.S.T. 3516, 75 U.N.T.S. 287 [hereinafter GC IV] (emphasis added). The conventions are *reprinted in* ROBERTS & GUELFF, *supra* note 10, at 195, 221, 243, and 249 respectively.

20. Protocol Additional I, *supra* note 10, art. 1.

21. Protocol Additional (II) to the Geneva Conventions of August 12, 1949, and Relating to the Protection of Victims of Non-international Armed Conflicts, June 8, 1977, 1125 U.N.T.S. 609, 16 INTERNATIONAL LEGAL MATERIALS 1442 (1977), *reprinted in* ROBERTS & GUELFF, *supra* note 10, at 481.

22. Protocol Additional I deals with conflict between States, whereas Protocol Additional II is that between a State and a rebel group (or groups).

23. Non-international armed conflict can occur solely within the confines of a single State.

24. Hague Convention (III) Relative to the Opening of Hostilities, Oct. 18, 1907, art. 1, 1 Bevans 619, 2 AMERICAN JOURNAL OF INTERNATIONAL LAW (Supp.) 85 (1908), *reprinted in* DIETRICH SCHINDLER & JIRI TOMAN, THE LAWS OF ARMED CONFLICT 57 (1988). According to the commentary to the 1949 Geneva Conventions, "[t]here is no longer any need for a formal declaration or war, or for recognition of the state of war, as preliminaries to the application of the Convention. The Convention becomes applicable as from the actual opening of hostilities." COMMENTARY: GENEVA CONVENTION FOR THE AMELIORATION OF THE CONDITION OF THE WOUNDED AND SICK IN ARMED FORCES IN THE FIELD 32 (Jean Pictet ed., 1952) [hereinafter GC I COMMENTARY].

25. GC I COMMENTARY, *supra* note 24, at 32–33 (emphasis added).

26. COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, para. 62 (emphasis added) (Yves Sandoz, Christophe Swinarki & Bruno Zimmerman eds., 1987) [hereinafter PROTOCOLS ADDITIONAL COMMENTARY]. The commentary to Protocol Additional II refers back to the commentary to common Article 3 of the 1949 Conventions and to that on Protocol Additional I. *Id.*, para. 4448, fn 2.

27. PROTOCOLS ADDITIONAL COMMENTARY, *supra* note 26, para. 4341 (emphasis added).

28. *See, e.g.*, discussion in INGRID DETTER, THE LAW OF WAR 20–21 (2d ed. 2000); Christopher Greenwood, *Historical Development and Legal Basis*, *in* THE HANDBOOK OF HUMANITARIAN LAW IN ARMED CONFLICT 1, 42 (Dieter Fleck ed., 1995).

29. For instance, the Preamble to Protocol Additional I notes that "it [is] necessary . . . to reaffirm and develop the provisions protecting the victims of armed conflicts and to supplement measures intended to reinforce their application." Additional Protocol I, *supra* note 10, pmbl.

30. The designation "Geneva Law" refers to that portion of the law of armed conflict addressing protected classes of persons: civilians, prisoners of war, the sick or shipwrecked, and medical personnel. It is distinguished from "Hague Law," which governs methods and means of combat, occupation, and neutrality. For a discussion of the international instruments which fall into each category, and of those which display elements of both, see FREDERIC DEMULINEN, HANDBOOK ON THE LAW OF WAR FOR ARMED FORCES 3-4 (1987).

31. On the topic of attribution of an act to a State, see the International Law Commission's Draft Articles on State Responsibility, 1996 ILC Report, ch. III, www.un.org/law/ilc/reports/1996/chap03.htm#doc38.

32. This possibility was described in PRESIDENT'S COMMISSION ON CRITICAL INFRASTRUCTURE PROTECTION, CRITICAL FOUNDATIONS: PROTECTING AMERICA'S INFRASTRUCTURES, Oct. 1997, at A-46.

33. Although not a Party to Protocol Additional I, the United States considers many of its provisions to be declaratory of customary international law. For a non-official, but generally considered authoritative, delineation of those viewed as declaratory, see Michael J. Matheson, *Session One: The United States Position on the Relation of Customary International Law to the 1977 Protocols Additional to the 1949 Geneva Conventions*, 2 AMERICAN UNIVERSITY JOURNAL OF INTERNATIONAL LAW AND POLICY 419 (1987). *See also* INTERNATIONAL & OPERATIONAL LAW DIVISION, OFFICE OF THE JUDGE ADVOCATE GENERAL, DEPARTMENT OF THE AIR FORCE, OPERATIONS LAW DEPLOYMENT DESKBOOK, tab 12, no date, and comments by the then State Department Legal Advisor Abraham D. Soafer in *Agora: The US Decision Not to Ratify Protocol I to the Geneva Conventions on the Protection of War Victims*, 82 AMERICAN JOURNAL OF INTERNATIONAL LAW 784 (1988).

34. Protocol Additional I, *supra* note 10, art. 48. The centrality of the principle to humanitarian law is noted in the ICRC commentary thereon:

> The basic rule of protection and distinction is confirmed in this article. It is the foundation on which the codification of the laws and customs of war rests: the civilian population and civilian objects must be respected and protected in armed conflict, and for this purpose they must be distinguished from combatants and military objectives. The entire system established in The Hague in 1899 and 1907 and in Geneva from 1864 to 1977 is founded on this rule of customary law. It was already implicitly recognized in the St. Petersburg Declaration of 1868 renouncing the use of certain projectiles, which had stated that "the only legitimate object which States should endeavour to accomplish during war is to weaken the military forces of the enemy." Admittedly this was concerned with preventing superfluous injury or unnecessary suffering to combatants by prohibiting the use of all explosive projectiles under 400 grammes in weight, and was not aimed at specifically protecting the civilian population. However, in this instrument the immunity of the population was confirmed indirectly.
>
> In the Hague Conventions of 1899 and 1907, like the Geneva Conventions of 1929 and 1949, the rule of protection is deemed to be generally accepted as a rule of law, though at that time it was not considered necessary to formulate it word for word in the texts themselves. The rule is included in this Protocol to verify the distinction required and the limitation of attacks on military objectives.

PROTOCOLS ADDITIONAL COMMENTARY, *supra* note 26, paras. 1863–64.

35. Protocol Additional I, *supra* note 10, art. 51.2.

36. *Id.*, art. 52.1.

37. *Id.*, art. 51.4.

38. *Id.*, art. 52.2.

39. *Id.*, arts. 51.1 & 51.2 (emphasis added).

40. PROTOCOLS ADDITIONAL COMMENTARY, *supra* note 26, para. 1875 (emphasis added).

41. It is reasonable to include human suffering in the meaning based on the fact that the protocol prohibits causing terror, also a mental condition. Protocol Additional I, *supra* note 10, art. 51.2.

42. *Id.*, arts. 51.5(b); 57.2(a)(iii); 57.2(b).

43. *Id.*, arts. 35.3 & 55.1.

44. *Id.*, art. 56.1.

45. PROTOCOLS ADDITIONAL COMMENTARY, *supra* note 26, para. 1881.

46. *But see* Haslam, *supra* note 9, at 173.

47. Indeed, the United States has even developed doctrine for the conduct of psychological operations. Chairman of the Joint Chiefs of Staff, Joint Doctrine for Psychological Operations, Joint Publication 3-53, July 10, 1996. Actions intended to terrorize the civilian population are prohibited by Protocol Additional I, *supra* note 10, art. 51.2.

48. Protocol Additional I, *supra* note 10, art. 57.2(a)(i). The commentary to the provision further explains the obligation.

> Admittedly, those who plan or decide upon such an attack will base their decision on information given them, and they cannot be expected to have personal knowledge of the objective to be attacked and of its exact nature. However, this does not detract from their responsibility, and in case of doubt, even if there is only slight doubt, they must call for additional information and if need be give orders for further reconnaissance to those of their subordinates and those responsible for supportive weapons (particularly artillery and air force) whose business this is, and who are answerable to them. In the case of long-distance attacks, information will be obtained in particular from aerial reconnaissance and from intelligence units, which will of course attempt to gather information about enemy military objectives by various means. The evaluation of the information obtained must include a serious check of its accuracy, particularly as there is nothing to prevent the enemy from setting up fake military objectives or camouflaging the true ones. In fact it is clear that no responsible military commander would wish to attack objectives which were of no military interest. In this respect humanitarian interests and military interests coincide.

PROTOCOLS ADDITIONAL COMMENTARY, *supra* note 26, para. 2195.

49. Protocol Additional I, *supra* note 10, art. 43.1–2.

50. *Id.*, art. 52.2.

51. Indeed, the commentary states that: "The text of this paragraph certainly constitutes a valuable guide, but it will not always be easy to interpret, particularly for those who have to decide about an attack and on the means and methods to be used." PROTOCOLS ADDITIONAL COMMENTARY, *supra* note 26, para. 2016.

52. *Id.*, paras. 2020–23.

53. *Id.*, para. 2024.

54. US Navy/Marine Corps/Coast Guard, The Commander's Handbook on the Law of Naval Operations (NWP 1-14M, MCWP 5-2.1, COMDTPUB P5800.7), para 8.1.1 (1995), *reprinted in* its annotated version as Volume 73 of the US Naval War College's International Law Studies series [hereinafter Handbook]. This assertion is labeled a "statement of customary international law." The Handbook cites General Counsel, Department of Defense, Letter of Sept. 22, 1972, *reprinted in* 67 AMERICAN JOURNAL OF INTERNATIONAL LAW 123 (1973), as the basis for this characterization.

55. Bankovic & Others v. Belgium, the Czech Republic, Denmark, France, Germany, Greece, Hungary, Iceland, Italy, Luxembourg, the Netherlands, Norway, Poland, Portugal, Spain, Turkey and the United Kingdom.

56. Protocol Additional I, *supra* note 10, art. 50.1.

57. *Id.*, art. 52.1.

58. *Id.*, art. 51.2 & 52. The Statute for the International Criminal Court also prohibits the direct targeting of civilians or civilian objects. Rome Statute for the International Criminal Court, art. 8.2(b)(i) & (ii), U.N. Doc. A/Conf. 183/9, July 17, 1998, at Annex II [hereinafter Rome Statute], *reprinted in* 37 INTERNATIONAL LEGAL MATERIALS 999 (1998), and M. CHERIF BASSIOUNI,

THE STATUTE OF THE INTERNATIONAL COURT: A DOCUMENTARY HISTORY 39 (1999), and available on-line at www.un.org/law/icc/texts/romefra.htm.

59. *Id.*, arts. 50.1 (for civilians) & 52.3 (for civilian objects).

60. *Id.*, art. 51.3; PROTOCOLS ADDITIONAL COMMENTARY, *supra* note 26, para. 1944.

61. Letter from DAJA-IA to Counselor for Defense Research and Engineering (Economics), Embassy of the Federal Republic of Germany (Jan. 22, 1988), *cited in* W.H. Parks, *Air War and the Law of War*, 32 AIR FORCE LAW REVIEW 1, 34 (1992).

62. GC III, *supra* note 19, art. 4(4).

63. *Id.*

64. Protocol Additional I, *supra* note 10, art. 56.1. This prohibition extends to attacks on other military objectives in their vicinity if the attack might cause such a release. There are exceptions to the general prohibition of the article.

> 2. The special protection against attack provided by paragraph 1 shall cease:
> (a) for a dam or a dyke only if it is used for other than its normal function and in regular, significant and direct support of military operations and if such attack is the only feasible way to terminate such support;
> (b) for a nuclear electrical generating station only if it provides electric power in regular, significant and direct support of military operations and if such attack is the only feasible way to terminate such support;
> (c) for other military objectives located at or in the vicinity of these works or installations only if they are used in regular, significant and direct support of military operations and if such attack is the only feasible way to terminate such support.

Id., art. 56.2.

65. *Id.*, art. 54.2. See also Rome Statute, *supra* note 58, art. 8.2(b)(xxv).

66. PROTOCOLS ADDITIONAL COMMENTARY, *supra* note 26, para. 2110. However, the prohibition does not apply to objects used solely for the sustenance of enemy forces or "in direct support of military action." Protocol Additional I, *supra* note 10, art. 54.3. An example of the latter would be a agricultural area used for cover by military forces.

67. *Id.*, arts. 35.3 & 55. See also Rome Statute, *supra* note 58, art. 8.2(b)(iv). On the issue of environmental damage during armed conflict, see THE ENVIRONMENTAL CONSEQUENCES OF WAR: LEGAL, ECONOMIC, AND SCIENTIFIC PERSPECTIVES (Jay E. Austin & Carl E Bruch eds., 2000); Michael N. Schmitt, *Green War: An Assessment of the Environmental Law of International Armed Conflict*, 22 YALE JOURNAL OF INTERNATIONAL LAW 1-109 (1997); PROTECTION OF THE ENVIRONMENT DURING ARMED CONFLICT AND OTHER MILITARY OPERATIONS (Richard J. Grunawalt, John E. King & Ronald S. McClain eds., 1996) (Vol. 69, US Naval War College International Law Studies).

68. Protocol Additional I, *supra* note 10, art. 12. However, note that there are specific criteria for the extension of protection to civilian facilities. *Id.*, art. 12.2. See also Rome Statute, *supra* note 58, art. 8.2(b)(ix) & (xxv).

69. *Id.*, arts. 21–31. The extent of the protection varies depending on the category of transportation and its location.

70. *Id.*, art. 53.

71. *Id.*, art. 62.3.

72. *Id.*, art. 70. Special provisions as to when such operations are entitled to the protection apply. Rome Statute, *supra* note 58, art. 8.2(b)(iii).

73. GC I, *supra* note 19, art. 46; GC II, *supra* note 19, art. 47; GC III, *supra* note 19, art. 13; GC IV, *supra* note 19, art. 33; Protocol Additional I, *supra* note 10, arts. 20, 51–56.

74. An example of an attack on a combatant that would be unlawful is one that employs a forbidden weapon, such as poison.

75. Soafer, *supra* note 33, at 470. For the official US position on reprisals against civilians, see Handbook, *supra* note 54, paras. 6.2.3 & 6.2.3.1–3.

76. The reservation reads:

> The obligations of Articles 51 and 55 are accepted on the basis that any adverse party against which the United Kingdom might be engaged will itself scrupulously observe those obligations. If an adverse party makes serious and deliberate attacks, in violation of Article 51 or Article 52 against the civilian population or civilians or against civilian objects, or, in violation of Articles 53, 54 and 55, on objects or items protected by those Articles, the United Kingdom will regard itself as entitled to take measures otherwise prohibited by the Articles in question to the extent that it considers such measures necessary for the sole purpose of compelling the adverse party to cease committing violations under those Articles, but only after formal warning to the adverse party requiring cessation of the violations has been disregarded and then only after a decision taken at the highest level of government. Any measures thus taken by the United Kingdom will not be disproportionate to the violations giving rise there to and will not involve any action prohibited by the Geneva Conventions of 1949 nor will such measures be continued after the violations have ceased. The United Kingdom will notify the Protecting Powers of any such formal warning given to an adverse party, and if that warning has been disregarded, of any measures taken as a result.

Reprinted on the International Committee of the Red Cross Treaty Database website, www.icrc.org/ihl.

77. For a comprehensive review of the principle, see ESBJÖRN ROSENBLAD, INTERNATIONAL HUMANITARIAN LAW OF ARMED CONFLICT: SOME ASPECTS OF THE PRINCIPLE OF DISTINCTION AND RELATED PROBLEMS (1979).

78. This typology is adopted from Christopher Greenwood, *The Law of Weaponry at the Start of the New Millennium*, in THE LAW OF ARMED CONFLICT: INTO THE NEXT MILLENNIUM 185 (Michael N. Schmitt & Leslie C. Green eds., 1998) (Vol. 71, US Naval War College International Law Studies). By contrast, the US Air Force employs the categories of military necessity, humanity, and chivalry, with proportionality folded into necessity, whereas the US Navy uses necessity, humanity and chivalry. *Compare* DEPARTMENT OF THE AIR FORCE, INTERNATIONAL LAW—THE CONDUCT OF ARMED CONFLICT AND AIR OPERATIONS (AF Pamphlet 110-31, 1976), at 1-5–1-6 with Handbook, *supra* note 54, para. 5-1.

79. PROTOCOLS ADDITIONAL COMMENTARY, *supra* note 26, para. 1957.

80. On the attacks, see U.S. DEPARTMENT OF DEFENSE, CONDUCT OF THE PERSIAN GULF WAR (Title V Report to Congress) (1992), at 623, *reprinted in* 31 INTERNATIONAL LEGAL MATERIALS 612 (1992).

81. An expanded discussion is in Michael N. Schmitt, *Bellum Americanum: The US View of Twenty-First Century War and its Possible Implications for the Law of Armed Conflict*, 19 MICHIGAN JOURNAL OF INTERNATIONAL LAW 1051, 1080–81 (1998).

82. Protocol Additional I, *supra* note 10, arts. 51.5(a) & 57.2(a)(iii) & (b). On proportionality, see William J. Fenrick, *The Rule of Proportionality and Protocol Additional I in Conventional Warfare*, 98 MILITARY LAW REVIEW 91 (1982); Judith G. Gardam, *Proportionality and Force in International Law*, 87 AMERICAN JOURNAL OF INTERNATIONAL LAW 391 (1993).

83. PROTOCOLS ADDITIONAL COMMENTARY, *supra* note 26, para. 2209.

84. A number of understandings/declarations/reservations have been issued on this point by Parties to Protocol Additional I. For instance, the United Kingdom made the following reservation when ratifying the protocol in 1998: "In the view of the United Kingdom, the military advantage anticipated from an attack is intended to refer to the advantage anticipated from the attack

considered as a whole and not only from isolated or particular parts of the attack." ICRC website, *supra* note 76.

85. An additional problem is that the valuation process itself is complex. For instance, culture may determine the value placed on an item or the value of an item may shift over time. The issue of valuation paradigms is explored, in the context of environmental damage during armed conflict, more fully in Michael N. Schmitt, *War and the Environment: Fault Lines in the Prescriptive Landscape*, 37 ARCHIV DES VOLKERRECHTS 25 (1999).

86. PROTOCOLS ADDITIONAL COMMENTARY, *supra* note 26, para. 1978.

87. *NATO Denies Targeting Water Supplies*, BBC WORLD ONLINE NETWORK, May 24, 1999, http://news.bbc.co.uk/hi/english/world/europe/newsid_351000/351780.stm.

88. *See generally*, Protocol Additional I, *supra* note 10, art. 57.

89. The Joint Warfare Analysis Center currently is engaged in modeling foreign infrastructures and contingent outcomes.

90. *Id.*, art. 57.2(a).

91. *Id.*, art. 57.3.

92. Article 39 of Additional Protocol I prohibits the use of the enemy's military emblems, insignia or uniforms. This prohibition, which the United States disagrees with except when it occurs during the actual engagement (*see* Handbook, *supra* note 54, para 12.1.1, fn 2), does not extend to the use of codes, passwords, and the like. MICHAEL BOTHE, KARL J. PARTSCH & WALDEMAR A. SOLF, NEW RULES FOR VICTIMS OF ARMED CONFLICTS (1982). However, Article 38 prohibits the misuse of protective signals.

93. Protocol Additional I, *supra* note 10, art. 37. *See also* Rome Statute, *supra* note 58, art. 8.2(b)(vii) & (xi). Convention (IV) respecting the Laws and Customs of War on Land, Oct. 18, 1907, annexed Regulations, art. 23(b)7, 36 Stat. 2277, 205 Consolidated Treaty Series 277, *reprinted in* ROBERTS & GUELFF, *supra* note 10, at 73, prohibits treacherous killing.

94. Protocol Additional I, *supra* note 10, annex, art. 11.

95. Office of General Counsel, Department of Defense, An Assessment of Legal Issues in Information Operations (Nov. 1999). The paper is appended to this volume as the Appendix.

96. *Id.*, art. 37.1(c); US Army Judge Advocate General's School, Operational Law Handbook 5-16 (2000).

97. Protocols Additional Commentary, *supra* note 10, paras. 1492–94.

98. GC IV, *supra* note 19, art. 28; Protocol Additional I, *supra* note 10 art. 51.7. *See also* Rome Statute, *supra* note 58, art. 8.2(b)(xxiii); Hans P. Gasser, *Protection of the Civilian Population*, *in* THE HANDBOOK OF HUMANITARIAN LAW IN ARMED CONFLICT 209, 218 (Dieter Fleck ed., 1995).

99. Protocol Additional I, *supra* note 10, art. 47.2. The United States does not support Article 47.

100. *Id.*, art. 47.1. This is problematic because States Party to the International Convention against the Recruitment, Use, Financing and Training of Mercenaries, albeit limited in number and though the convention is not yet in force (it has only secured 21 of the 22 necessary ratifications as of October 2001), are obligated to amend their domestic laws to outlaw mercenarism. GA Res. 44/34 (1989), art. 5.3, ICRC website, *supra* note 76.

101. For a description of hesitancy to use CNA during Operation ALLIED FORCE, see Bradley Graham, *Military Grappling with Rules for Cyber Warfare: Questions Prevented Use on Yugoslavia*, WASHINGTON POST, Nov. 8, 1999, at A1.

102. *See* Schmitt, *Computer Network Attack*, *supra* note 7.

103. Consider the comment of Lieutenant General Michael Short, USAF, who commanded the air war during Operation ALLIED FORCE:

> I felt that on the first night, the power should have gone off, and major bridges around Belgrade should have gone into the Danube, and the water should be cut off so that the next

morning the leading citizens of Belgrade would have got up and asked, "Why are we doing this?" and asked Milosovic the same question.

Craig R. Whitney, *The Commander: Air Wars Won't Stay Risk-Free, General Says*, THE NEW YORK TIMES, June 18, 1999, at A1.

104. PROTOCOLS ADDITIONAL COMMENTARY, *supra* note 26, para. 1871, notes that "it is the duty of Parties to the conflict to have the means available to respect the rules of the Protocol. In any case, it is reprehensible for a Party possessing such means not to use them, and thus consciously prevent itself from making the required distinction."

105. A typical Information Operations cell is illustrated in Joint Pub 3-13, *supra* note 2, at figure IV-4 and accompanying text. It includes an IO officer from J-3; representatives from J-2, 4, 5, 6, 7, supporting combatant commands, and service and functional components; a judge advocate; and public affairs, counterintelligence, civil affairs, targeting, special operations, special technical operations, electronic warfare, psychological operations, military deception, and operations security experts.

XII

Proportionality, Cyberwar, and the Law of War

Ruth G. Wedgwood

The advent of the computer has enormously increased the efficiency of modern economies, lending computational prowess to the organization of industrial production, inventory, communications, the integration of power grids, the control of financial transactions, and transportation routing. The decentralized architecture of the personal computer, and its Internet platform, have linked economic actors screen-to-screen, allowing direct communications and disintermediated transactions, bypassing a costly institutional structure of wholesale and retail agencies. The real-time communication of common written texts through e-mail and document formats has strengthened coordination within and between organizations, permitting consultative processes to work in staggered time. Cybernetic life has also brought new problems in public and private law, including data privacy, jurisdiction for regulating speech and the protection of intellectual property.

Challenges for the law in a cybernetic age will extend to the battlefield. Cybernetics have transformed war. In data-sharing, military planners were the first to engineer joint access to a common pool through the "DARPANET," fabled forerunner of the civilian sector's Internet. In air operations and even for ground forces, computer and sensor technology can eventually be used to construct a real-time picture of an integrated battlespace, to be shared among friendly forces.

Computers, supporting sensors and global positioning satellites will enhance the precision of weaponry and maneuvers, supplementing human judgment with digital assessments. The accuracy of kinetic weapons will be improved by using optical matches of targets and trajectory, and reconciling the real coordinates of projectiles and aim points. (Even in the last ten years, the navigational capabilities of cruise missiles have been transformed.) Though budget constraints and procurement cycles may slow down the implementation of this virtual battlespace, the prospects are clear. A shared system of observation and control will support the adjustment of tactics, the dynamic targeting of the adversary's assets, the full integration of multiple weapons platforms, and safeguards against friendly fire. Advanced electronics and computing capabilities also hold the promise of confusing an adversary's command and control, disrupting his operating systems, and masking his view of the battlespace. The future of national missile defense also depends on the extraordinary computing capabilities that can handle massive data on launch speed, trajectory, and atmospheric perturbations.

Computer technology will also continue to support American military transportation, communications, and logistics—essential in mobilizing, deploying, and sustaining a combat force, so often the Achilles' heel of lesser military forces. The American military is a far-flung force, deployed around the globe, conducting exercises, patrols, and peace operations in numerous theatres at once. Access to common data and immediate communications can integrate a decentralized force structure.

But the luxury of a new technology also can create vulnerabilities, and enhancement can become dependency. The sophistication of American military operations may invite a new mode of asymmetric attack. Opposing forces whose own organization is far more primitive may attempt an electronic version of jiu-jitsu. The same technological doors that permit easy communication also allow unwanted foreign entry. The portals for adjustment of operations may permit deliberate disruption. Encryption of data and communications has grown in power, but code-breaking has also benefited from number-crunching bionics. Protecting sensitive information through compartmentalization is more difficult when access may be gained through trap doors and undetected keyholes. The quickly changing design of software and hardware, and the Pentagon's frequent reliance on commercially available products for "non-critical" operations, also means that information technologists may not fathom the vulnerability of the systems they employ. Rather like war-gaming, defensive understanding is often gained only after a simulated attack. The advantages of cybernetic organization for military campaigns must be weighed against the dangers of compromise and disruption.

Military law must also address the new architecture of cyberwar, including the ill fit of existing normative structures for electronic warfare. A primary challenge for military thinkers is what to do about civilian safety. Over the centuries, the operational harshness of warfare has been challenged by the ideals of proportionality and discrimination. These ideals of the profession of arms, implemented by military commanders and their legal advisors, ask for a critical distinction between civilian and military targets, and teach that military advantage always must be measured against civilian loss. Cybernetic conflict may pose new hazards to civilian safety, taxing our traditional notions of the division between the battlefield and civilian life. It is well to consider some of these problems in advance in order to construct the necessary safeguards.[1]

Discrimination among targets is a fundamental norm of military law, acknowledging that there is, ultimately, an important distinction to be made between civilian objects and military assets. The idea of discrimination is rooted in the belief that warfare should be effective, rather than punitive, and that wars can be won without deliberately harming civilians. The moral compromises of war do not extend to unnecessary cruelty. Noncombatants are considered innocent (even where, in their political lives, they may have favored a war) and enjoy a right to life protected even in warfare. Apart from the ethical claim, there is a practical reason to observe this scruple. The reciprocal practice of discrimination means that a soldier has greater assurance that his own family members will survive the conflict. A military operator also will see discrimination as the practical application of economy of force, saving one's firepower for targets that matter. The norm is further supported by a working hypothesis about war termination—armed conflicts may end earlier where defeated soldiers can reintegrate into a workable civilian society, in which there is something to return to. Renewal of the conflict may be more likely if civilian society is left destitute and a generation reared seeking revenge.

Proportionality extends the protection for civilians beyond the ban on deliberate targeting. Proportionality argues that dominant intention is not enough in choosing the objects of destruction in a war. Even with a military target directly in view, there must be some balancing between the advantage to the war effort from a target's destruction and the foreseeable "incidental" damage to civilians. The terms of trade in this moral exchange are not terribly clear, to be sure—the relative weighting of military gain and civilian harm is a complex judgment that involves both battlefield expertise and situational ethics. But at the limit, there is an admitted case in which an ephemeral military advantage could not outweigh enormous harm.

In the idealized account of the law of war, the operational code of *jus in bello* is equally binding on both sides no matter who was at fault in starting the conflict. In this view, the operational norms regulating how a war is fought do not vary according to the purpose of the war. The same tactics govern a virtuous or condemnable war. *Jus in bello* binds a combatant despite his status as invader or as a victim defending his homeland. The perceived value of this separation is that a third party or protecting power can monitor the observance of humanitarian law without venturing into the hotly disputed territory of *casus belli* and the merits of the underlying dispute. The international limits on the initiation of warfare, *jus ad bellum*, are placed in a separate normative framework. (The practical tolerance of political publics for this attempted distinction is another matter. Indeed, in the preparation for the Nuremberg trials, at least one prominent scholar argued that any use of force by the Axis, even against traditional military targets, should be considered a war crime, since each use of force aided the Nazi war of aggression.[2] The obverse conclusion, that any tactic was permissible to defeat Nazism, was not openly mooted, but may underlie some of our practical assessments.)

Protecting civilians is harder than it sounds on paper for a number of reasons. First, in modern warfare, the mobilization of national economies and war production makes industrial plants and infrastructure into a second battlefield. Economic assets are considered military targets for their support of the war effort. Critics have questioned the efficacy of particular air campaigns, but the legitimacy of weakening an adversary's industrial base and war production facilities is generally accepted. Unless an air campaign can be confined to night-time bombing, the targeting of war industries will endanger workers in the plants, even though they are technically noncombatants. Locating war industries in urban areas is also likely to endanger residential areas, unless precision bombing is used.

Second, the rural conflicts of the Cold War and decolonization also challenged the protection of civilians. The techniques of guerrilla warfare typically involve camouflaging insurgent forces among the civilian population as protection against more powerful adversaries. Distinctive military insignia or dress has been a long-standing requirement of legitimate warfare in order to distinguish civilians from combatants and the failure to identify forces traditionally deprived the disguised combatants of the protections of the law of war, including prisoner of war status. But the norm of self-identification was derided as a luxury in an era of wars against "colonial domination."[3] Undermining this rule of combatant identification poses obvious dangers to innocent civilians.[4] In civil war, terrorist tactics against civilians also have been deliberately used as a powerful advertisement that the established government cannot guarantee

protection. Governments, in turn, have used terror to persuade civilian populations to withhold support from insurgents.

The problem of target masquerade extends even to conventional warfare, since combatants are sometimes tempted to disguise military assets as civilian facilities. Secreting a weapons cache inside a school building serves to collapse the attempted distinction between civilian and military sites, and is an act of perfidy punishable as a war crime. Misuse of a civilian facility deprives the target of its protected status, but the damage remains because it makes combatants less inclined generally to respect the protection guaranteed to civilian sites.

The third source of heightened danger for civilians stemmed from nuclear confrontation in the Cold War, with its strategies of deterrence through mutually assured destructive capability, flexible response, and counterforce targeting. Even with the confinement of nuclear targeting to military objects such as missile silos, troop concentrations, and ports and airfields, the externalities of radiation, electromagnetic pulse, and a broad radius of immediate destruction meant that civilian populations would have been gravely endangered.

Since the end of the Cold War, the proliferation of ethnic conflicts has continued to pose grave hazards to civilians. In a war whose target is the civilian population itself, atrocious acts are often committed against noncombatants as one way of causing populations to flee. The war aim of creating a mono-ethnic territory is used to justify terror tactics in order to displace populations. Attacks on civilians are not incidental, but rest at the center of the conflict, serving the central war aim of purging minorities and ethnic rivals. Where advantage may be gained by the rapid consolidation of territory, the employment of terror against civilians is hard to contain.

Even with the most worthy war aims, the principled distinction between military and civilian targets may be under pressure (though it is still mandatory to avoid terror tactics). In a humanitarian intervention such as the 1999 Kosovo campaign, designed to stem the gross mistreatment of civilian populations, responsible leaders must seek to undermine the transgressing adversary's will to resist, using war as a mode of coercive diplomacy. Winning such a limited conflict is quite different from the unconditional surrender sought in the great land campaigns of the world wars. Striking mobile military vehicles, tanks, and artillery pieces in a mountainous terrain is exceedingly difficult, and (in a humanitarian intervention designed to thwart genocide) an expedited end to the conflict may be urgent. At least one high Yugoslav official has suggested that the Kosovo campaign was abandoned by Belgrade because Milosevic doubted the ultimate loyalty of the Yugoslav military. This disaffection was caused in part by the military's concern about how the steady destruction of Serbia's infrastructure would

affect the welfare of their own families. While there is widespread consensus that civilians must not be deliberately reduced to starvation or other life-threatening conditions, at least one analyst has suggested that the rule of discrimination should permit the disabling of facilities that sustain some conveniences of modern civilian life. The danger of a slippery slope is evident—the loss of water purification and sewage disposal, for example, could cause devastating disease and lies beyond the pale of easy ethical analysis. Yet the problems of stopping a war that seems remote to the controlling polity are also evident, and the limit of "mere inconvenience" does not abandon the broader norm of protecting civilian survival. The troubling question of how to persuade an adversary to desist has not been made easier as well by the last decade's record of ineffective employment of economic sanctions as an alternative instrument of coercion.

Another difficult challenge to the conceptual categories of civilian and military objects has been created, ironically, by the new precision of guided munitions. With navigation by global positioning and optical recognition, aim points and target impact may be as exact as the particular courtyard of a building in an urban area. Targeting has an exactitude, and therefore a transparency of intention, unknown to other wars. The targets sought in an air campaign are evident and public. The five-mile radius of uncertainty that surrounded the aerial delivery of munitions in the Second World War served to obscure the target aim, apart from internal knowledge of the campaign plans. But precision-guided munitions announce their destination, and pose the questions of target distinction masked in earlier wars.

Finally, there is the serious dilemma of dual-use targets. This is again a problem of distinction between military and civilian objects. It stems from the joint infrastructure of modern economies. Military and civilian facilities share a need for electricity, natural gas, and oil to sustain their basic services. Rarely is there a dedicated infrastructure exclusively serving military facilities. To disable the facilities that sustain a military adversary may unavoidably burden the local civilian populations. In the Kosovo and Iraqi air campaigns, allied forces needed to suppress anti-aircraft capability and ground radar guidance in order to allow safe allied entry into hostile airspace. Mobile facilities, camouflaged and positioned under the lee of a hill, are difficult to target even in clear weather. The only assurance of safe air space may lie in pulling the plug on anti-aircraft by disabling a power grid. The legitimacy of doing so depends on a judgment about proportionality. Vital civilian functions such as schools, old age homes, and hospitals may also depend on electrical power. The civilian harm from their temporary disability must be conscientiously weighed against the military advantage. The merger of military and civilian electrical infrastructure shows the difficulty of a

strict principle of distinction, and the quandaries of judgments on proportionality. Oil and gasoline supplies, too, present a dual-use dilemma. Loss of refining and storage facilities can severely limit an adversary's ability to field armored divisions for extended operations. Yet oil supplies may be necessary for the winter heating of civilian dwellings in urban areas. The ability of a regime to deprive its civilian population in favor of continued military capability makes the linkage even more painful. None of these real-world problems of ethics, law, and principle can be easily solved,[5] even while the law of armed conflict must maintain the ideals of discrimination and proportionality.

The legal texts that have accompanied these historical changes are worthy of note, as a preliminary matter. The Hague Rules of 1907 were modest in their scope, anticipating in the Martens Clause that a changing technology and the unsettled practice of States might make codification difficult.[6] The Hague Rules forbid pillage and attacks on undefended towns, and require sparing, "as far as possible," cultural and medical institutions. Arms "calculated to cause unnecessary suffering" were also banned. But some of the modern operational dilemmas lay beyond anticipation or consensus.

Operational targeting was incidentally addressed in the 1949 Geneva Conventions, through the establishment of protections for hospitals and neutralized zones for civilians who "perform no work of a military character," as well as the right of evacuation of children and aged persons from encircled areas.[7] But in the 1977 Geneva Protocols,[8] there was new attention both to a broader definition of proportionality and the nature of civilian targets. The effort was not altogether successful for Protocol I has been disputed in several of its features. The Protocol was signed but not ratified by the United States, and was excluded by the Security Council from the Statute of the International Criminal Tribunal for the former Yugoslavia as a direct source of law for the tribunal. Its formal definition of proportionality has been modified further in the Rome negotiations for a permanent international criminal court.

Article 51(b) of Protocol I deems an attack "indiscriminate" if it "may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated." The International Criminal Court (ICC) treaty limited the language, noting that military advantage is to be assessed in the context of an "overall" military campaign—allowing military commanders and operators to seek more distant, as well as immediate objectives.[9] A military advantage, for example, need not be "temporally or geographically related to the object of the attack."[10] In addition, the ICC treaty notes that the military commander breaches a criminal rule only where the

incidental loss of civilian life or injury to civilians is "clearly" excessive.[11] "Knowledge" is an essential element. The uncertainties of war are legendary, and the commander's assessment must be based on the information he has available at the time. Only where a commander, based on the information available to him at the time, "knew" the damage caused would be clearly excessive, is there a criminally culpable act.[12] This may include self-conscious knowledge of the breaching of a legal limit, as well as knowledge of the actual facts of the campaign. As noted by the committee of experts advising the prosecutor of the International Criminal Tribunal for the former Yugoslavia:

> It is much easier to formulate the principle of proportionality in general terms than it is to apply it to a particular set of circumstances because the comparison is often between unlike quantities and values. One cannot easily assess the value of innocent human lives as opposed to capturing a particular military objective.[13]

So, too, the text of the 1977 Protocol defining civilian objects was deemed incomplete by the Rome negotiators. Article 51(2) of Protocol I says, with apparent clarity, that the "civilian population as such, as well as individual civilians, shall not be the object of attack. Acts or threats of violence the primary purpose of which is to spread terror among the civilian population are prohibited."[14] Article 52 prescribes that "civilian objects shall not be the object of attack or of reprisals," but notes, tautologically, that "[c]ivilian objects are all objects which are not military objectives as defined in paragraph 2."[15] The search for specificity is not greatly aided by the next bundle of negotiated language. Paragraph 2 of Article 52 notes broadly that "military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage."

The difficulties of definition were implicitly recognized in the Rome negotiations for the permanent international criminal court. The implementation of Article 51 noted the centrality of intention—requiring proof that a commander "intended" that civilians as such be "the object of the attack"—arguably requiring specific intent to cause such harm and knowledge of the legal status of the protected persons.

The Rome drafters also attempted to craft a criminal rule to implement Article 52, condemning attacks where the "object of the attack" was "civilian objects, that is, objects which are not military objectives."[16] But the difficulties of distinction in regard to dual-use assets is implicitly acknowledged elsewhere in Protocol I. In Article 54, starvation of civilians as a method of warfare is

prohibited, and it is equally prohibited to attack or destroy "objects indispensable to the survival of the civilian population" where the "specific purpose" is to deny them to the civilian population. But attack is concededly permitted where the asset is used in "direct support of military action," unless this would cause starvation or forced movement.

How do these principles apply to computer attacks and computer defense, in an age of cyberwarfare?

The requirement of discrimination between civilian and military objects presents a substantial challenge in cyberwarfare—complicated as well by the question of neutrality. If, in a defensive mode, the United States were the victim of an attack on vital computer systems, the temptation to respond in kind would be considerable. Yet the ultimate source of a computer attack can be acutely difficult to determine—a problem magnified by the deliberate use of "looping" or "weaving"—using another's server to disguise the origination of the attack. An attack is likely to be sent through an unrelated server in order to mask its authorship, and a response in kind may end up damaging or disabling the "looped" server. The intermediate servers may be largely dedicated to civilian functions, and may even be in a country other than the originator of the attack. Even where the retaliatory response successfully limits its impact to the ultimate point of origin, the counterattack may end up disabling civilian functions. The attacker can use a civilian platform for convenience or in order to mask State-sponsorship, even though the latter could qualify as perfidy.

In a world of real geography, it is simpler to frame a response to the problem of unauthorized use of platforms. A sovereign State is held responsible to police the misuse of its territory. An insurgent force cannot launch cross-border attacks with impunity, and one rationale for permitting a counterattack across the border is that the harboring State abandoned or was unable to discharge the duty to police its own soil. The same duty could be imposed on the proprietors of electronic space and governing civilian authorities. But the organization of cyberspace is in private hands, and has no single authoritative source of police. Misappropriation of a server can be accomplished quickly and secretly, and even if a server's vulnerability has been detected before, not every trespass on a server is worth preventing. Unless the involvement of a nation State is evident, say by advertising an available "free zone" for cyberpirates, a retaliatory response may be disputed.

In addition, it may be far harder to confine the effects of the counterattack than in a land-based response. Cyberspace counterattack is especially troublesome because the topography is unknown. The shape of cyberspace is truly *terra incognita*, including a server's network linkages to civilian structures. In a

conventional military campaign employing land forces or air attack against an adversary, the proximity of civilian structures and other protected objects can be mapped by surveillance aircraft, drones, or ground spotters. The information may be imperfect, and there may be no realistic way to avoid all incidental harm, but there is some relative idea of the likely consequences of an attack. A prepared target list or "bombing encyclopedia" is designed to permit estimates of probable civilian casualties. The method of approach to a target may be altered in some cases in order to minimize civilian harm should munitions go wide of the mark. But in cyberspace, there is often a rapidly changing architecture of linkage and control, and the attempt to intrude in order to map its geography may itself be detected and considered a hostile act. Nonetheless, one might be inclined to propose a defeasible duty of "benign" or "humanitarian" espionage—attempting to map cyberlinks in order to contain the consequences of a defensive counterattack. The technical feasibility of this is open to question, with the added difficulty that the very act of intrusion may be detected.

For any form of cyber counterattack, one necessary scruple may be to build firewalls into the very instrument of intrusion. Where it is not feasible to conduct benign mapping in advance, it may be conceivable to have the intrusion device map or filter as it goes, for example, by characterizing the content of files before it destroys them. This might help to distinguish between military and civilian objects linked to the same server. Another palliative may be to conceive of proportionality as a dynamic matter. Greater damage to civilian objects may be tolerated in order to eliminate a security threat, so long as the damage is reversible or, indeed, aid is given in its restoration.[17]

An additional problem in applying proportionality is the twilight between criminal acts and acts of war. In the midst of a major conflict fought by conventional means, any accompanying electronic attack will be regarded as a matter of utter gravity, justifying a strong response against the actor, even with ensuing collateral damage. But in a more ambiguous setting, for example, where a State actor is gathering information that would facilitate illicit entry and hostile operations, there is no predicate that provides a classical justification for the use of overwhelming force in response. To be sure, intrusions even by non-State actors, where they cause serious interference with vital operations or loss of life, would fit the ordinary understanding of terrorism. But Washington has chosen to emphasize the tools of criminal law in responding to most forms of terrorism, attempting to arrest and indict members of international networks, rather than treating them as combatants in an undeclared private war. Force is fully warranted to capture an international terrorist or thwart a planned attack, but criminal law creates a set of expectations that are often frustrating to an effectively

fought conflict. Criminal law withholds any justification of punitive force until after proof has been mustered in court and a verdict is rendered by an independent fact finder. Its proceedings are public, and the sources of evidence are often compromised during a trial by the public disclosure of the methods of surveillance. Proof beyond a reasonable doubt is an appropriate standard for protecting domestic liberty in a civil society. The extraordinary difficulty of detaining an individual offender is a worthy price to pay in order to preserve a libertarian political culture. But criminal law's demanding standards are founded on the assumption that civil society enjoys the underlying fidelity of the relevant actors. International politics and the security decisions of nation States must sometimes proceed on more ambiguous indicators.[18]

In addition, the invocation of criminal law creates the expectation that action taken abroad will defer to local State consent. Because criminal processes are public, any related government action abroad is likely to become known. Actions taken for intelligence purposes that do not enjoy the consent of the foreign territorial State may do especially grave damage to bilateral relations if they are broadcast. Thus, when invoked, the criminal law paradigm tends to dominate Washington's response to a situation, since all other modalities must be weighed in light of the cost of their public disclosure. (Sometimes it is the mere fact of publicity that will cause a foreign government to react strenuously to an international security measure out of a perceived affront to its public dignity or *amour propre*.)

Recent negotiations for a convention on cybercrime illustrate the point. Lengthy talks were conducted through the Council of Europe, with the participation of the United States, Canada, Japan, and Australia. The draft treaty requires each participating country to criminalize various forms of computer misuse, including deliberate denial of service through distributed network attacks, and to create real-time methods of preserving and gathering relevant proof.[19] This is especially important since tracing an attacker may be possible only while the attack is underway and the actor is still on line. One of the treaty's more controversial features would require Internet service providers to preserve information at the request of a State party. Nonetheless, a successful criminal inquiry will depend on the treaty cooperation of each country through which an attacker loops his communication. It will not take much sophistication for a cyber adversary to filter his messages through countries outside the treaty regime. Any direct response to the attack, through counterattack or disabling measure, may be resented by the treaty States in the loop as "derisive" of the treaty regime and discourage their later cooperation. Deference to the enforcement jurisdiction of local authorities is a premise of the treaty architecture, and

yet may be unworkable for intelligence operations and national security measures. Private hackers in Europe offered their services to Iraq during the Persian Gulf War, and, in a similar situation, the slow and deliberate processes of criminal law may not be adequate for infrastructure protection.

Even if there is a decision to treat State-sponsored cyber attacks as acts of war rather than crimes, it will remain difficult to identify these more serious incidents in a timely way. In biological warfare, it has recently been observed, it may be hard to distinguish the spread of natural pathogens from deliberate acts of contamination. The same difficulty can arise in distinguishing a prankster or technological sociopath from an international adversary. The difference is surely important in assessing whether the attack is likely to escalate as the diversionary prelude to other more deadly methods of warfare. The ambiguity of sponsorship that one saw in the surrogate conflicts of the Cold War is likely to plague cyber defense as well.

The dilemmas of civilian protection in cyber conflict are a circumstance to be lived with. Technology may solve some of the problems it has created. And the technological superiority of the United States in all modalities of conflict may mean that we can afford to accept some risk for the sake of maintaining a moral high ground. The best answer to the Solomonic cyber quandaries will require the continuing collaboration of technologists, warfighters, ethicists, and, lest we forget, experts in the law of war.

Notes

1. Thoughtful commentaries on the law of war and its relation to cyber conflict include Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUMBIA JOURNAL OF TRANSNATIONAL LAW 885 (1999); Mark Russell Shulman, Legal Constraints on Information Warfare, Occasional Paper No. 7, Center for Strategy and Technology, Air War College, Maxwell Air Force Base (March 1999); and Office of the General Counsel, Department of Defense, An Assessment of International Legal Issues in Information Operations (Nov. 1999). The latter paper is appended to this volume as the Appendix.

2. *See* SHELDON GLUECK, THE NUREMBERG TRIAL AND AGGRESSIVE WAR 105 (1946) ("Since the initiation and conduct of such a war of aggression is at least unlawful, all acts of warfare in pursuance thereof—whether they violate the laws and customs of war or do not do so—are illegal. They also become *criminal* in considering the effect of illegality upon the defense of 'justification' in criminal law.").

3. *See* Protocol Additional (I) to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, art. 44(3), Dec. 12, 1977, 1125 U.N.T.S. 3 [hereinafter Protocol I].

4. The 1977 Protocols to the Geneva Conventions were criticized by some for the suggestion that guerrillas should only be required to distinguish themselves en route to an attack. *See* Colonel G.I.A.D. Draper, *The Status of Combatants and the Question of Guerrilla Warfare*, 1971 BRITISH

YEARBOOK OF INTERNATIONAL LAW 173, *reprinted in* REFLECTIONS ON LAW AND ARMED CONFLICTS: THE SELECTED WORKS ON THE LAWS OF WAR BY THE LATE PROFESSOR COLONEL G.I.A.D DRAPER, OBE (Michael Meyer and Hilaire McCoubrey eds., 1998).

5. It is worth recognizing that the law of war has both rules and principles—or, if you like, self-executing rules that require little interpretation, and others that are highly fact specific and context sensitive in their application. In a report of experts assessing the 1999 NATO bombing campaign in Yugoslavia, prepared for the prosecutor of the International Criminal Tribunal for the former Yugoslavia, it was noted that "[e]veryone will agree that a munitions factory is a military objective and an unoccupied church is a civilian object. When the definition is applied to dual-use objects which have some civilian uses and some actual or potential military use (communications systems, transportation systems, petrochemical complexes, manufacturing plants of some types), opinions may differ. The application of the definition [of civilian object] to particular objects may also differ depending on the scope and objectives of the conflict. Further, the scope and objectives of the conflict may change during the conflict." *See* Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia, para. 37, www.un.org/icty/pressreal/nato061300. htm.

6. The Martens Clause noted that "[u]ntil a more complete code of the laws of war has been issued, the high contracting parties deem it expedient to declare that, in cases not included in the Regulations adopted by them, the inhabitants and the belligerents remain under the protection and the rule of the principles of the law of nations, as they result from the usages established among civilized peoples, from the laws of humanity, and from the dictates of public conscience." *See* Convention respecting the Laws and Customs of War on Land and Annex: Regulations respecting the Laws and Customs of War on Land, *in* PROCEEDINGS OF THE HAGUE PEACE CONFERENCES 620-631 (1920). This reunion of law and conscience may disturb positivists, but is not so dissimilar from the working sources of customary legal norms in other social contexts.

7. Convention Relative to the Protection of Civilian Persons in Time of War (Geneva IV), Aug.12, 1949, arts. 15, 18, and 19, 6 U.S.T. 3516, 75 U.N.T.S. 287 (entered into force Oct. 21, 1950; entered into force for the United States Feb. 2, 1956).

8. Protocol I, *supra* note 3, and Protocol Additional (II) to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-international Armed Conflicts, June 8, 1977, 1125 U.N.T.S. 609 (entered into force Dec. 7, 1978).

9. Rome Statute of the International Criminal Court, art. 8(2)(b)(iv), U.N. Doc. A/CONF.183/9* (July 17, 1998) [hereinafter Rome Statute].

10. Report of the Preparatory Commission for the International Criminal Court, Finalized draft text of the Elements of Crimes, U.N. Doc. PCNICC/2000/1/Add.2 (Nov. 2, 2000), art. 8(2)(b)(iv), para. 2 and note 36.

11. Rome Statute, *supra* note 9, art. 8(2)(b)(iv).

12. Finalized draft text of the Elements of Crimes, *supra* note 10, art. 8(2)(b)(iv), para. 3 and note 37.

13. Final Report to the Prosecutor, *supra* note 5, para. 48.

14. This leaves open the question, however, whether diminishing civilian morale is a legitimate war aim.

15. Protocol I, *supra* note 3, art. 52.

16. *See* Rome Statute, *supra* note 9, art. 8(2)(b)(ii), and Elements of Crimes, *supra* note 10, art. 8(2)(b)(ii).

17. A "first strike" against an adversary's computer systems, as part of anticipatory self-defense, is another possibility that we may imagine. The disruption of a national computer network may disrupt an adversary's military communications, military mobilization, the processing of targeting information, and other vital military functions. But the attack may also present the same "dual server" problems discussed above. The same preventative measures of benign espionage and a

dynamic conception of proportionality (permitting greater damage with speedy restoration) may be called for.

18. War and peace entertain different standards for lethal force in enforcement measures. In civilian societies, the use of lethal force is generally limited to the prevention of immediate deadly harm, with a high threshold of knowledge. In a state of war, the threshold for using force is lower. The identification of combatants is made on the basis of information reasonably available in the situation. A foot soldier will rarely be expected to use the sparing rules of engagement of a civil policeman.

19. *See* Draft Convention on Cyber-Crime and Explanatory Memorandum Related Thereto, Council of Europe, European Committee on Crime Problems, Strasbourg, France, June 29, 2001, www.conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm and www.conventions.coe.int/Treaty/EN/projets/FinalCyberRapex.htm.

XIII

Neutrality and Information Warfare

George K. Walker[1]

"There is nothing new about revising neutrality; it has undergone an almost constant process of revision in detail," Philip Jessup concluded in 1936.[2] He also believed

> . . . [N]othing could be more fallacious than the attempt to test the application of rules of neutrality by the principles of logic. Since they are products of compromise and of experience, logic has found practically no place in their development and cannot properly be used in their application.[3]

Over half a century into the UN Charter era, little would change these observations, even in the information warfare (IW)[4] context. New considerations have appeared,[5] including the Charter itself; the process of analyzing the law of neutrality defies a straightforward, positivist, black-letter approach. Principles of neutrality for maritime warfare have been seen to be less rigid, from an historical perspective, than those for air or land warfare,[6] for example.

Some claim neutrality is in "chronic obsolescence."[7] A major reason, according to those who say future applications of the law of neutrality will be minimal, is an argument that the Charter has ended the rights and duties of the old law of neutrality.[8] Another argument is that since the Charter has outlawed war,[9] there can be no state of war, and therefore there is no need for a law of neutrality.[10]

(This position might be considered in light of the Pact of Paris [1928], outlawing aggressive war.[11] World War II began a decade later.)

Many others, reflecting State practice and claims in the Charter era, maintain that the law of neutrality continues to exist. The *San Remo Manual* recognizes maritime neutrality.[12] The 1992-96 International Law Association Committee on Maritime Neutrality studied neutrality, and the 1998 ILA conference accepted the Committee's final report.[13] Individual researchers assert that neutrality remains a valid legal concept, albeit modified by the impact of the Charter and other considerations.[14]

Like the reports of Mark Twain's passing, accounts of neutrality's demise in the Charter era have been greatly exaggerated, as the ensuing analysis of the application of neutrality principles to information warfare demonstrates.

Application of the Principles of the Law of Neutrality to Information Warfare

The law of warfare has little, if any, direct reference to problems of armed conflict involving IW. The Charter applies across the board to all treaties, and perhaps customary law as well.[15] Although there are a few treaties with some bearing on transmission of information, e.g., Hague V and XIII, in most cases the analysis must proceed from general custom, general principles, and analysis by analogy. General principles of law occupy an anomalous position among sources of international law. Although the Statute of the International Court of Justice lists them among primary sources that may be cited in cases before the Court,[16] and some commentators include them among primary sources for deriving rules of law,[17] others accord them secondary status, perhaps as gap-fillers.[18] Whichever view one might take, in a new and fast-moving area of the law where there are few guideposts, resort to general principles of law, and commentators that discuss them,[19] may be the only sources that are available.

What then should be the method of analysis for IW issues?

The first and primary rule should be application of mandatory Charter norms, e.g., the right of self-defense, with, e.g., its limitations of necessity and proportionality for reaction in self-defense,[20] or UN Security Council decisions.[21] The next level of analysis should employ the mixture of treaties, custom, etc. that must apply in specific neutrality situations. For example, if Hague V and XIII principles applicable to telecommunications are customary law, they should be applied, perhaps alongside general law of armed conflict (LOAC) principles such as necessity and proportionality in a given situation, except where there is a prohibitory rule, e.g., no first use of poison gas, for which there can be no proportionality or necessity qualifications.[22] In applying these principles to the

modality of transmitting Internet messages, States will indirectly affect use of and messages through the Internet. The fact that cables may be used for Internet-based messages as well as traditional telephone or telegraph messages can be necessity and proportionality factors.

Where there is no "hard law," i.e., black-letter rules governing conduct, resort must be had to general customary LOAC principles, i.e. military objective, necessity and proportionality, which may be different from similar principles to be observed in self-defense responses.[23] The content of the law for these situations might be informed by analogies from custom, treaties and principles applied in the law of land, sea, air and space law. As will be seen, the law of the sea (LOS) and the law of naval warfare may offer the most and best analogies for neutrals in IW situations.

Neutrality, Land Warfare, and Information Warfare

The implications for IW from the law of neutrality relating to neutral land territory are several. The Charter may impact decisions on the law of neutrality, and treaty suspension or termination principles may apply for international agreements other than those dealing with warfare.[24] The Security Council may make legally binding decisions under Articles 25 and 48 of the Charter, and therefore may obligate UN Members under Articles 41-42 to take action that might be inconsistent with traditional neutrality principles. The Council also may make nonbinding "call[s] upon" Members under Articles 40-41. It also may make nonbinding recommendations under Articles 39-40. If Council decisions differ from traditional neutrality principles, the latter must give way.[25] If Council or General Assembly resolutions are at variance from traditional neutrality principles, and restate customary or other binding sources of law,[26] these resolutions also will affect the traditional law of neutrality.[27]

Thus, Council decisions may compel a State to behave inconsistently with traditional neutrality practice by requiring what would otherwise be belligerent acts or by restricting rights neutrals traditionally enjoy.[28] Nevertheless, belligerent attacks must be conditioned on general warfare principles of military objective, necessity, and proportionality.[29]

A neutral has a duty to prevent use of its territory for a belligerent's operations, base, or as a sanctuary.[30] The activity, depending on personnel involved, e.g., belligerent forces operating the Internet computer, may be a violation of the neutral's territorial integrity under the Charter.[31] If a neutral knows or has reason to know of activity within its territory involving Internet use that is non-neutral in nature, the neutral must act to end that activity under the LOAC,

and may invoke the Charter if the activity involves a violation of the neutral's territorial integrity. If a neutral may be required to mobilize forces to ensure fulfillment of its responsibility to prevent belligerent forces from crossing into neutral territory, and thus act in self-defense,[32] by analogy it may be argued that a neutral may mobilize or order its forces to counter an Internet attack conducted from its territory, even if a belligerent's forces are not involved. If war materials and supplies belonging to a belligerent, either as a matter of title or use, are employed in an Internet attack while situated within a neutral's borders, the neutral can act against the materials and supplies. If belligerent forces operate the computers, etc., the case for neutral action is stronger.

If a neutral does not or cannot effectively enforce compliance, an aggrieved belligerent may take proportional action, either under the law of self-defense or the LOAC, to counter these Internet activities.[33] Of course, there is a risk that the neutral may assert a violation of its territorial integrity by the aggrieved belligerent and resort to self-defense measures.[34] In these situations, an aggrieved belligerent's prior notice to the neutral may be prudent, unless the neutral is seen to be cooperating with the offending belligerent.

If belligerents may not build radio stations on neutral territory, by analogy they cannot use Internet "stations" in neutral territory, and a neutral must shut these down.[35] If a neutral does not have the means, or the willingness to do so, an aggrieved belligerent may take proportional action.[36] It would seem, however, that if neutrals need not control their own stations, or acts of their nationals acting in a private capacity,[37] then there is no obligation to do the same for Internet information thus passed to a belligerent under the Hague law. Query whether the pattern of neutrals' controlling radio stations in two World Wars[38] gives credence to establishing a customary norm obliging neutrals to do so in future conflicts.

The land warfare rules for railway rolling stock offer an interesting parallel. Hague V provides that belligerents may not requisition railway rolling stock of companies chartered by a neutral State except if absolutely necessary.[39] However, if a private company chartered by a neutral consents to the stock's use for warlike purposes, the stock acquires enemy character and may be seized and appropriated as though it is enemy State property.[40] If a belligerent may not use neutral-owned rolling stock unless absolutely necessary but may seize stock a belligerent uses for carrying war goods, could it not be argued by analogy that a belligerent may not "seize" neutrals' Internet transmissions except in emergency, but that if the neutral allows the Internet to be used for messages harmful to the belligerent, those aspects of the Internet are fair game?

Humanitarian law allows a neutral to authorize passage of wounded and sick from belligerent forces if vehicles transporting them carry no combatants or war materials. If a neutral allows passage, the neutral assumes responsibility for providing for control and safety of these personnel.[41] If a neutral has discretion to authorize passage for belligerents' sick and wounded armed forces personnel while assuming responsibility for their control and safety, it would seem that the neutral may, but is not required to, allow Internet messages regarding belligerent sick and wounded, if the neutral can be sure that no information affecting the war is passed home.[42] Similarly, a prisoner of war staying in neutral territory[43] may not be allowed Internet access to send information home that amounts to belligerent activity, any more than the prisoner of war should be allowed to mail, telephone, televise, etc., such information.

Neutrality at Sea, Naval Warfare, and Information Warfare

The same Charter principles applicable to land warfare apply to war at sea, including any IW component.[44] Oceans users, whether neutral or belligerent, must pay due regard[45] to other oceans users' rights and freedoms besides the rules of naval warfare, which apply in armed conflict situations through the LOS conventions' other rules clauses.[46] Treaty suspension or termination principles also may apply. Although many treaties may bear on IW issues, during armed conflict they may be impossible to perform,[47] fundamental change of circumstances may intervene,[48] or there may be a material breach.[49] *Jus cogens* norms, e.g., perhaps the inherent right of self-defense,[50] may trump treaty law.[51] War, or armed conflict, may end or suspend treaty obligations.[52] General principles of necessity and proportionality in attack govern as in land warfare.[53]

Hague XIII, governing maritime neutrality, imposes virtually the same rules as Hague V, governing land warfare, in forbidding belligerent use of neutral ports and waters for erecting wireless telegraphy stations or any apparatus for communicating with belligerent forces. Belligerents cannot use neutral ports or waters as a base of operations.[54] The same considerations and applications of these principles in land warfare to IW issues should apply in maritime warfare situations.[55] Moreover, because these principles appear in two major multilateral treaties and the regional Maritime Neutrality Convention, their common principles are strengthened.[56]

There is an important difference between neutrals' duties with respect to movement of belligerent troops across neutral land territory and movement of belligerent naval forces into neutral ports and waters. The duty to repel troop movements is absolute, while the duty to detect and oust belligerent naval

forces is subject to the neutral's having the means to do so.[57] A neutral is only "entitled," not required, to intern a belligerent warship when that warship should have departed neutral waters.[58] When the Hague Conventions were signed in 1907, there were many countries that may not have had naval forces or detection capability sufficient to oust a belligerent naval force or to intern it. There must have been a presumption that any State could use its military or other forces, perhaps police, to repel a belligerent troop movement, but that might not be the case for naval incursions. The same is true today. For IW neutrality principles, it could be argued that the duty of a neutral to act to prevent belligerent IW warfare from within its territory is not absolute, but conditional on the ability of the neutral to detect IW activity and to be able to act to counter this activity. Not every country has computer and related systems as sophisticated as, e.g., the United States, and these countries should not be held to an absolute duty. Such being the case, computer-sophisticated nations like the United States must be held to the same duty, i.e., use of means at the disposal of the United States, which might be quite considerable.

Principles governing destruction of undersea cables strengthen a view that belligerents can operate to seize or destroy Internet connections in enemy territory and in areas subject to no State's sovereignty, e.g., the high seas, if a belligerent controls that area, e.g., for blockade. Belligerents can seize or destroy cables connecting enemy territory with neutral territory, but only a terminus in enemy territory. These cables may be seized or destroyed only "in cases of absolute necessity," i.e., general principles of necessity and proportionality[59] must be observed. No distinction is made between publicly and privately owned cables.[60] Neutrals' control of radio broadcasting within their territorial waters during two World Wars[61] is another example of proper control of electronic emissions by neutrals within their territories. If neutrals had this obligation for radio, the "Internet" of the day, is it not also true for today's World Wide Web of communications?

Issues related to contraband, visit and search or diversion, and the possibility of destruction of neutral merchant ships that have acquired enemy character[62] or ships or aircraft that are believed to be aiding the enemy although otherwise exempt[63] might seem to have little to do with IW. However, certain general principles might be derived and used in the IW context.

Given Internet technology's exponential growth, it would seem extraordinarily useless to go through a lengthy treaty negotiation process to draft an agreement listing prohibited Internet behaviors or actions that would be as out of date as the computers that began to produce the treaty at the start of the drafting and negotiation process. This has been the experience of trying to define

contraband. The lesson from contraband law is that in a fast-developing or ever-changing scenario, trying to go beyond general principles is rarely wise, except in the obvious, "hospital ship" or poison gas situation, where everyone agrees on the rules, at least for hospital ships if they are not used to further an enemy war effort, and for poison gas as long as there is no use.[64]

If we analogize dealing with Internet messages to neutral merchantmen on the high seas, could an electronic "visit and search," followed by appropriate proportional and necessary action, perhaps electronic diversion, be devised for belligerents to use with neutrals?[65]

If an Internet message or "hack" contributes to enemy war-fighting or war-sustaining efforts, assists an enemy's armed forces intelligence system, or acts as an auxiliary military or naval channel of communication or information, is not the attack and destruction option available, subject to necessity and proportionality principles?[66] To be sure, perhaps special principles analogous to the passenger and crew safety rule when a merchantman must be destroyed,[67] might be devised. For example, if messages relating to safety of civilians are involved, can they be electronically isolated and allowed through?

Might an electronic "firewall" analogous to blockade principles in the law of naval warfare[68] be devised to let appropriate messages get through? The Internet might be used for traditional blockades and other interdictions, besides the usual Notices to Airmen (NOTAMs) and Notices to Mariners (NOTMARs) published, e.g., by radio.

Is it useful to think in terms of specific exemptions for neutral Internet usage? Hague XI lists enemy vessels exempt from capture and possible destruction because of their nature, among them a debatable exemption for mails as distinguished from mail ships.[69] Would it be helpful to develop exempted computer systems, kinds of messages, or Internet systems exempt from "capture" and possible destruction unless used to aid an enemy? What about generally exempt ships, e.g., hospital ships unless they aid an enemy, that send Internet-based messages that might be construed by a belligerent to be encrypted messages? Would this raise a suspicion, however unfounded, such that use of Internet-based messages by neutral exempt vessels should be banned or somehow restricted? Can system segregation be done with today's technology? Is it too early for this? Could the Internet itself be used to advise of these exemptions, if a case by case basis seems appropriate?

Might military commanders consider declaring control of immediate areas of military operations on the Internet, analogous to the immediate area of naval operations?[70] To be sure, this kind of declaration may invite more trouble than it is worth, i.e., it could tell adversaries where to go. The Internet can, of course, be

used to send these notices, besides NOTAMs and NOTMARs sent by more traditional means for addressees who lack Internet capability, or to assure transmission and receipt, i.e., where there is a possibility that an Internet-based message did not go through.

Although it is not part of the law of neutrality, any country can declare temporary use of the high seas for naval maneuvers, including air operations.[71] These maneuvers can be conducted during armed conflict. Is there a correlative right of declaring temporary use of part of the Internet for "IW maneuvers"? Might notice of these IW maneuvers be posted on the Internet besides more traditional means, e.g., NOTAMs or NOTMARs? (As in the case of warning of immediate area of naval operations during war, such a notice, whether by NOTAM or NOTMAR through traditional media or the Internet, invites attention.)

Could or should an "Internet exclusion zone" be declared,[72] warning neutrals of higher risk if they "surf" in the area or otherwise use the "zone"? Like notices for immediate areas of naval operations, these warnings could be posted on the Internet, as well as by more traditional means, e.g., NOTAMs and NOTMARs. (Notice of blockade, immediate area of naval operations, or exclusion zones, must be effective;[73] while the Internet might be a valuable communication medium, it cannot replace more traditional and widely available methods until it has become as universal as more traditional means; this may be a problem for vessels flagged in countries that are not as advanced in Internet technology as, e.g., the United States.)

Could States declare temporary "defense zones" for parts of the Internet spectrum, analogous to a high seas defense zone or *cordon sanitaire* that may be announced for an area of naval and air operations, to warn other countries of a risk of self-defense responses? This is not a feature of naval warfare but an incident of self-defense.[74] And because the technology is still emerging, and any treaty now might be premature,[75] down the road when and if the problem settles down, could agreements modeled on the INCSEA agreements[76] be considered to minimize confrontation? Longstanding treaties promoting safety at sea offer another model.[77]

Might states proclaim an "Internet Identification Zone" (IIZ) for parts of the Internet spectrum, analogous to an ADIZ?[78] The IIZ would be a warning, perhaps published on the Internet and in other sources to assure notice, of a possibility of interception if Internet users approach too close to a neutral State's vital interests (analogous to its territory, the anchor for an ADIZ), including, e.g., defense and central economic communications systems. The ADIZ is not an air

warfare feature; it serves as an identification method. An IIZ might have a similar function.

I do not have technical competence to respond to these questions, or perhaps to ask others, but might they be asked? Some inquiries may be far-fetched or impractical, but given the exponential growth of technology, some of which may be shrouded for national security reasons, I ask them.

The Internet is like a merchant shipping system or the US public highway system. There is no regulation of the Internet akin to systems regulating radio and television broadcasting. It is up to the individual or government as to the nature of vehicles used (the computers) and, beyond a small access charge paid Internet access providers, the user is largely on its own as to how the Internet is employed as to content and destination. Therefore, although there may be belligerent and neutral rights, perhaps by analogy to those for naval warfare as I have posited them, there are relatively few positive duties, apart from a requirement to respect belligerents' and neutrals' rights, however those may be stated.

As a final point, the due regard principle, derived from the LOS and its law of naval warfare counterpart,[79] might be part of the analysis; i.e., belligerents must have due regard for rights of Internet users that are neutral, even as Internet users must have due regard for others on the Net in the absence of armed conflict. And even as belligerents must have due regard for the maritime environment in today's wars at sea, might they be required to have due regard for the general Internet environment?

Neutrality, Aerial Warfare, and Information Warfare

As in the cases of land and sea warfare, Charter principles may apply in given situations.[80] Treaty suspension or termination principles may apply.[81] Besides air warfare rules, belligerents must observe principles of military objective, necessity, and proportionality applying to all modes of war.[82]

Like neutrality rules for land and sea warfare, air warfare rules require respect for neutral airspace; belligerent military aircraft cannot enter it.[83] When coupled with identical treaty-based neutrality rules applicable to land and sea warfare, this principle is strengthened.[84] The Hague Air Rules principle, the same as those for land warfare but differing from the weaker requirements for neutrals for naval warfare, is that actions taken by a neutral to enforce neutral rights, cannot be construed as a hostile act.[85] Since two branches of the law of neutrality protect the neutral in its actions to enforce neutrality, particularly since Internet activity necessarily ultimately involves the land in terms of sending and reception of messages, and the flight of Internet messages through lines might be

analogized to aircraft flight, should not the rule be that actions taken by a neutral should not be deemed a hostile act, and not an unfriendly one, as the law of naval warfare has it? A neutral might enforce its rights by an unfriendly act, i.e., a retorsion,[86] a lesser action in that it does not involve proportional reprisals, i.e., an unlawful act designed to compel compliance.[87]

There is an important difference between neutrals' duties with respect to movement of belligerent troops across neutral land territory and movement of belligerent naval forces into neutral ports and waters, or movement of belligerent military aircraft into neutral airspace. The duty to repel troop movements is absolute, while the duty to detect and oust belligerent naval or air forces is subject to a neutral having the means to do so.[88] When the Hague Conventions were signed, many countries may not have had naval forces or detection capability sufficient to oust a belligerent naval force. The same assumption may underlie the 1923 Hague Air Rules regarding intruding belligerent military aircraft and their internment. There must have been a presumption that any State could use its military or other forces, perhaps police, to repel belligerent troop movements, but that might not be the case for every country for naval or military aircraft incursions. The same is true today. For IW neutrality rules, it could be argued that a neutral's duty to act to prevent belligerent IW from within its territory is not absolute, but conditional on the neutral's ability to detect IW activity and to act to counter it. Not every nation has computer and related systems as sophisticated as, e.g., the United States, and these countries should not be held to an absolute duty. Such being the case, computer-sophisticated nations like the United States must be held to the same duty, i.e., use of means at the disposal of the United States, which might be quite considerable.

A neutral's duty to prescribe a route away from belligerents' military operations for aircraft ordered by a belligerent[89] might be seen, by analogous precedent for IW, to say a neutral must prescribe Internet "routes" not to interfere with military operations. The qualifying phrase in the Hague Air Rules, that a neutral must exact guarantees, indicates a possible weakness of the prescription, however. For IW, if a neutral prescribes a "route," can the neutral enforce the prescription, given the Internet's decentralized nature? The Hague Air Rules principle that a neutral must, commensurate with the means at its disposal, prevent aerial observation of belligerent operations,[90] is in the same vein. Should neutrality law for IW say that a neutral must, commensurate with the means at its disposal, prevent IW observation, through reading Internet traffic, of belligerent military operations?

The Hague Air Rules, like naval warfare rules, allow a belligerent's force commander to prohibit neutral aircraft from passing in an immediate vicinity of

a commander's forces or to make aircraft follow a particular route, if the commander considers the aircraft is likely to prejudice success of military operations. If an aircraft, once notified, refuses to comply, a belligerent may fire on it.[91] In the IW context, might a belligerent assert a similar right to prohibit Internet activity in an immediate electronic or physical vicinity of military operations, or direct that Internet traffic follow routes? Can the belligerent "shoot down" noncomplying Internet traffic, using proportional means, coming close to military Internet operations, after notice? Might notice of these areas of operations be posted on the Internet besides more traditional means? (A correlative problem is that any radio or Internet message invites attention to the location of belligerent forces.)

Although it is not part of the law of neutrality, any country can declare temporary use of the high seas for naval maneuvers, including air operations.[92] These maneuvers can be conducted during armed conflict. Is there a correlative right of declaring temporary use of part of the Internet for "IW maneuvers"? Might notice of these "maneuvers" be posted on the Internet? (As in the case of the warning of the immediate area of naval operations during war, such a notice, whether by NOTAM or NOTMAR through traditional media or the Internet, invites attention.)

Exclusion zones for neutral aircraft as well as ships, reasonable in scope and duration and which are properly noticed, are a valid method of warfare at sea today. They are not free-fire zones but are designed to warn neutral aircraft of heightened danger if they enter a zone.[93] Might an "IW exclusion zone" with similar qualifications be declared to warn Internet users of a heightened risk of being "fired on" if they venture into certain "areas" of the Internet? Might notice of these zones by NOTAMs and NOTMARs be posted on the Internet besides more traditional means?

Could States declare temporary "defense zones" for certain parts of the Internet spectrum, analogous to a high seas defense zone or *cordon sanitaire* that may be announced for an area of air operations, to warn other countries of a risk of self-defense responses? This is not a feature of air warfare but an incident of self-defense. Here too INCSEA and safety of life at sea treaties could be models for advance agreements for these situations.[94]

Might States proclaim an "Internet Identification Zone" (IIZ) for certain parts of the Internet spectrum, analogous to the ADIZ?[95] The IIZ would be a warning, perhaps published on the Internet and in other sources to assure notice, of a possibility of interception if Internet users approach too close to a neutral State's vital interests (analogous to its territory, the anchor for an ADIZ), including, e.g., its defense and central economic communications systems. The ADIZ

is not a feature of air warfare; it serves as an identification method. The IIZ might have a similar function.

Neutrality and Information Warfare in Space

There is little new "hard law" in norms applicable to conflict in outer space,[96] other than applying Charter law,[97] the law of suspension or termination of treaties,[98] and general principles of necessity and proportionality, and perhaps due regard in some cases, applying to armed conflict anywhere.[99] There is no special neutrality law like that applying to land, sea, or air warfare. Any law of neutrality applicable to IW in space must be derived by analogy from these other sources, as was the case before agreements like the Outer Space Treaty, the Liability Convention, the Registration Convention, etc., were negotiated.[100] And it is this general methodology that may be the most useful. If law for outer space could be derived by analogy from other systems before formal treaties appeared, cannot the same be said for IW? Which legal system(s) should supply the model(s)?

Conclusions: Appraisal of Neutrality in the Charter Era in the Context of Information Warfare

As the manned space flight era became a reality, commentators recommended applying other, well-established law to space age situations by analogy. UN Charter law applies to situations in space, as it does for interactions on land, at sea, and in the air. Today treaties, and practice pursuant to them, govern many other aspects of space interactions, but not all of them. These agreements are subject to Charter law primacy and to law of treaties rules for suspension or termination. Beyond the treaties, some space law issues remain unresolved, and applying other systems of law by analogy seems to be the norm.

Internet warfare issues involving neutrals, and the law to be applied to them, seem close to the situation for warfare in space. Charter-based norms, e.g., prohibition against violating States' territorial integrity or political independence, the right of self-defense and the primacy of Security Council decisions, must be applied. There are telecommunications treaties to which Charter norms and law of treaties rules for suspension and termination are subject. Some LOAC principles, e.g., those related to telegraphy, will apply to Internet messages as well as more conventional communications, although these are also subject to Charter norms, e.g., self-defense. Beyond these relatively well-established norms, there are many principles, primarily in the law of naval warfare but also some from the

law of land and air warfare, that may be cited by analogy in IW situations involving neutrals.

Undeniably neutrality as a general concept has as much vitality today as in the pre-Charter era. The claim, that there is a customary right to assert an intermediate status of nonbelligerency between traditional neutrality and belligerency, may have been strengthened since 1945, although most States and commentators do not recognize it. The precedents in some cases are almost identical with those in the last two centuries. Even if nonbelligerency cannot be asserted as a customary norm, the overlay of principles of self-defense, retorsion, reprisals not involving use of force, and state of necessity apply to support actions at variance with a practice of strict neutrality in the traditional sense.[101]

Because of options under the Charter for non-binding resolutions by the Security Council and perforce the General Assembly, the potential for exceptions even with a binding Council decision and the opportunity for claims of neutrality—perhaps modified by a new non-belligerency concept in the Charter era—remains large. "Far from being moribund, these traditional rights [of neutrality and self-defense] apply logically in conditions of limited wars"—the type of conflicts that have beset the planet since 1945—even more rigorously than in conditions of total war.[102]

The advent of information war may call for modifying Jessup's remarks published in 1936 when the world was recovering from a world war and preparing for the next one.[103] Transoceanic communication was dependent on undersea cables for urgent messages, although radio signals could also reach across the seas. The most advanced countries had cross-border telephone and telegraph access by landlines. Most transoceanic communications went by ship, although the first international air mail deliveries were beginning for transoceanic and transcontinental communications. However, the usual means of communication then for most messages was what we call "snail mail" today. The Internet was a Cold War creation.[104] Today, Jessup might say that although the basic neutrality rules remain in place and they apply for IW, their application for IW must be by analogy.

One option is a non-law analysis[105] although that alternative is less than fashionable today, given a tendency to find some law (perhaps publicist's views if there is no customary law, treaty, or general principle available).[106] Commentators correctly assert that it is almost universally accepted that a considerable body of law applies to States' use of force in cyberspace contexts.[107] If that is true, a correlative is that the considerable body of traditional neutrality law, some of it restated in treaties of longstanding duration that are now almost universally recognized as declaring custom, and the rest in customary norms or general

principles, also exists. If we choose to operate in the context of law, under a rule of law, the law of neutrality developed for more traditional warfare modalities offers useful analysis by analogy where there are no positive standards, e.g., rules governing cables.

Today one exception to the traditional law is Charter law, e.g., the inherent right to individual and collective self-defense, which predates the Charter. Others include prohibitions against violating a State's territorial integrity, and the primacy of UN Security Council decisions.[108] Another might be human rights, although human rights treaties' derogation clauses reflect traditional rules of suspension or termination during international armed conflict.[109] The policies of peacetime telecommunications treaties, although perhaps limited in application during armed conflict because of their terms or because of general rules of treaty suspensions or termination, are another.[110] Analysis of IW issues in a context of the law of neutrality as it applies to land, sea, and air warfare reveals common denominators and differences. For example, belligerents have a duty not to cross neutral's land territory by land or air, or to use neutral land or seas (i.e., the territorial sea) for a base of operations.[111] A neutral's duty to repel these incursions varies with the modality of incursion. If it is by land, there is apparently an absolute duty, at least to try. If the incursion is by belligerent air or naval forces, the neutrals' duty is relative. It must use the means at its disposal to counter an incursion, including means at its disposal to intern an intruding aircraft and those aboard. A neutral may elect to detain a belligerent warship that has remained in port when it is not entitled to stay there. Undoubtedly the 1907 Hague drafters, and the 1923 Commission of Jurists that prepared the Hague Air Rules, believed every country had some semblance of ground forces to repel a belligerent's troop movements across neutral lands, but that not every State had the means of detecting or repelling incursions by air or sea, or of interning belligerent military vessels or aircraft.[112] The "means at a neutral's disposal" principle should be the test for a neutral's duty for belligerents' IW incursions; the neutral should be held to apply the means at its disposal to detect and repel these incursions. Such being the case, the correlative right of a belligerent aggrieved by IW incursions should be that the belligerent may take such actions as are necessary in the territory of a neutral that is unable (or perhaps unwilling) to counter enemy IW force activities, making unlawful use of that territory, a principle from the law of naval warfare.[113]

Beyond these general rules applying to neutrality in a context of all warfare modes, the rules begin to diverge among the different kinds of armed conflict, the closest kinship being seen between the law of naval warfare and aerial warfare, particularly naval warfare. From a geographic perspective, these mediums

for combat offer more persuasive reasons for analogy to IW. Both are concerned with "fluid" mediums, like the Internet's electronic pathways.[114] The law of naval warfare is concerned with warfare on the high seas, a part of the globe that is no nation's property. It also is concerned with ocean areas over which coastal States may exercise sovereignty, i.e., the territorial sea; or jurisdiction, i.e., the exclusive economic zone (EEZ). There is also a relatively well-developed set of rules or general principles in the LOS and the law of naval warfare upon which analogies for IW may be drawn.[115] Closer examination of the LOS and the law of naval warfare in connection with and its interfaces with Charter law, the LOS and treaty termination or suspension principles may produce analogies suitable for developing IW principles.

The LOAC is replete with notice requirements.[116] The new technology might be employed to give notice, adequate under the circumstances, in traditional warfare situations in addition to the usual means of doing so. Given IW technology's fluidity and exponential growth, the relative lack (thus far) of practice in IW situations, and the relatively minimal number (again thus far) of claims and counterclaims[117] in the worldwide electronic arena, any international agreement(s) on IW would likely be obsolete in terms of hardware and practice before their ink would be dry.[118] Haphazard as the prospect may be, rules for IW should be left to developing customary norms and general principles, perhaps with help from commentators,[119] before serious consideration of a treaty begins.

Notes

1. Parts of this chapter have been adapted from GEORGE K. WALKER, THE TANKER WAR 1980–88: LAW AND POLICY (Vol. 74, US Naval War College International Law Studies) chs. 3, 5 (2000); George K. Walker, *Maritime Neutrality in the Charter Era*, 17 CENTER FOR OCEANS LAW AND POLICY PROCEEDINGS 124 (1993) [hereinafter Walker, *Maritime Neutrality*].

2. PHILIP C. JESSUP, NEUTRALITY: TODAY AND TOMORROW 156 (1936).

3. *Id.* at 16, quoting PHILIP C. JESSUP & FRANCIS DEAK, NEUTRALITY: THE ORIGINS xiii-xiv (1935). Oliver Wendell Holmes wrote in similar vein that a page of history is worth a volume of logic and that the life of the law has not been logic but experience. *New York Trust Co. v. Eisner*, 256 U.S. 345, 349 (1921) (Holmes, J.); OLIVER WENDELL HOLMES, THE COMMON LAW 5, 244 (Mark DeWolfe Howe ed. 1963).

4. Information warfare (IW) is information operations (IO), i.e., actions taken to affect adversary information and information systems while defending one's own information and information systems, conducted during crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries. Joint Chiefs of Staff, Joint Pub 1-02, Dictionary of Military and Associated Terms 422 (2001). *See also* WALTER G. SHARP, SR., CYBERSPACE AND THE USE OF FORCE 23–24 (1999) [hereinafter SHARP].

5. *E.g.*, MYRES S. MCDOUGAL & FLORENTINO FELICIANO, LAW AND MINIMUM WORLD PUBLIC ORDER ch. 5 (1961); NILS ORVIK, THE DECLINE OF NEUTRALITY 1914–1941 ch. 6 (2d ed. 1971); Walter L. Williams, Jr., *Neutrality in Modern Armed Conflict: A*

Survey of the Developing Law, 90 MILITARY LAW REVIEW 9 (1980) consider a multi-factor approach to neutrality law and its place in the law of war (LOW), i.e., the law of armed conflict (LOAC). (The ensuing analysis cites the LOW and the LOAC interchangeably and also refers to "war" and "armed conflict" interchangeably. More conventional analyses include, *e.g.*, ANNOTATED SUPPLEMENT TO THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS ch. 7 (A. Ralph Thomas and James C. Duncan eds., 1999) (Vol. 73, US Naval War College International Law Studies) (Annotated Supplement); D.W. BOWETT, SELF-DEFENCE IN INTERNATIONAL LAW ch. 8 (1958); IAN BROWNLIE, INTERNATIONAL LAW AND THE USE OF FORCE BY STATES (1963); ERIK CASTREN, THE PRESENT LAW OF WAR AND NEUTRALITY ch. 3 (1954); C. JOHN COLOMBOS, THE INTERNATIONAL LAW OF THE SEA chs. 16–21 (6th rev. ed. 1967); YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENCE chs.1.D, 6.D (3d ed. 2001); JURG MARTIN GABRIEL, THE AMERICAN CONCEPTION OF NEUTRALITY AFTER 1941 (1988); MORRIS GREENSPAN, THE MODERN LAW OF LAND WARFARE chs. 13–14 (1959); 7 GREEN H. HACKWORTH, DIGEST OF INTERNATIONAL LAW ch. 24 (1943); 3 CHARLES CHENEY HYDE, INTERNATIONAL LAW CHIEFLY AS INTERPRETED AND APPLIED BY THE UNITED STATES Tit. K (2d ed. 1945); HANS KELSEN, COLLECTIVE SECURITY UNDER INTERNATIONAL LAW 154–71 (Vol. 49, US Naval War College International Law Studies) (1954); HANS KELSEN, PRINCIPLES OF INTERNATIONAL LAW 154–73 (Robert W. Tucker ed. 2d ed. 1967); 2 D.P. O'CONNELL, LAW OF THE SEA ch. 30 (1984); 2 LASSA OPPENHEIM, INTERNATIONAL LAW, Part III (Hersch Lauterpacht ed., 7th ed. 1952); JOHN F.L. ROSS, NEUTRALITY AND INTERNATIONAL SANCTIONS: SWEDEN, SWITZERLAND AND COLLECTIVE SECURITY (1989); JULIUS STONE, LEGAL CONTROLS OF INTERNATIONAL CONFLICT chs. 13–19, 21 (1959); ROBERT W. TUCKER, THE LAW OF WAR AND NEUTRALITY AT SEA chs. 6–12 (Vol. 50, US Naval War College International Law Studies) (1955); 11 MARJORIE M. WHITEMAN, DIGEST OF INTERNATIONAL LAW ch. 33 (1968); Michael Bothe, *Neutrality at Sea,* ch. 6 *in* IGE F. DEKKER & HARRY H.G. POST, THE GULF WAR OF 1980-88 (1992); Michael Bothe, *Neutrality in Naval Warfare: What Is Left of Traditional Law?, in* HUMANITARIAN LAW OF ARMED CONFLICT: CHALLENGES AHEAD 387 (Astrid J.M. Delissen & Gerard J. Tanja eds. 1971); Francis Deak, *Neutrality Revisited, in* TRANSNATIONAL LAW IN A CHANGING SOCIETY: ESSAYS IN HONOR OF PHILIP C. JESSUP 137 (Wolfgang Friedman et al. eds. 1972); Andrea Gioia, *Neutrality and Non-Belligerency, in* INTERNATIONAL ECONOMIC LAW AND ARMED CONFLICT 51 (Harry H.G. Post ed. 1994); Andrea Gioia & Natalino Ronzitti, *The Law of Neutrality: Third States' Commercial Rights and Duties,* ch. 7 *in* DEKKER & POST, *supra*; Mark W. Janis, *Neutrality,* ch. 6, *in* THE LAW OF NAVAL OPERATIONS (Horace B. Robertson, Jr. ed., 1991) (Vol. 64, US Naval War College International Law Studies); Titus Komarnicki, *The Place of Neutrality in the Modern System of International Law,* 80 RECUEIL DES COURS DE L'ACADEMIE DE DROIT INTERNATIONAL 395 (1952); J.F. Lalive, *International Organizations and Neutrality,* 24 BRITISH YEARBOOK OF INTERNATIONAL LAW 72 (1972); John H. McNeill, *Neutral Rights and Maritime Sanctions: The Effects of Two Wars,* 31 VIRGINIA JOURNAL OF INTERNATIONAL LAW 631 (1991); Patrick M. Norton, *Between the Ideology and the Reality: The Shadow of the Law of Neutrality,* 17 HARVARD INTERNATIONAL LAW JOURNAL 249 (1976); Dietrich Schindler, *Transformations in the Law of Neutrality Since 1945, in* HUMANITARIAN LAW, *supra,* at 367; Frank L. Wiswall, Jr., *Neutrality, the Rights of Shipping and the Use of Force in the Persian Gulf,* 31 VIRGINIA JOURNAL OF INTERNATIONAL LAW 619 (1991).

6. CASTREN, *supra* note 5, at 427.

7. Janis, *supra* note 5, at 148, citing NEILL H. ALFORD, JR., MODERN ECONOMIC WARFARE) 326 (1963 (Vol. 56, US Naval War College International Law Studies); *see also* Norton, *supra* note 5, at 249, citing Richard R. Baxter, *Humanitarian Law or Humanitarian Politics? The 1974 Conference on Humanitarian Law,* 16 HARVARD INTERNATIONAL LAW JOURNAL 1, 2 (1975) (Neutrality has had a "juridical half-life" since World War II).

8. Janis, *supra* note 5, at 148, citing C.G. Fenwick, *Is Neutrality Still a Term of Present Law?*, 63 AMERICAN JOURNAL OF INTERNATIONAL LAW 102 (1969).

9. *Cf.* UN Charter, preamble, arts. 2(3)–2(4); *see also* LELAND M. GOODRICH *ET AL.*, CHARTER OF THE UNITED NATIONS 19–25, 41–55 (3d ed. 1969); BRUNO SIMMA, THE CHARTER OF THE UNITED NATIONS 45–48, 97–128 (1994).

10. GABRIEL, *supra* note 5, at 69; *see also* ORVIK, *supra* note 5, at 251–56.

11. Treaty Providing for Renunciation of War As an Instrument of National Policy, Aug. 27, 1928, arts. 1–2, 46 Stat. 2343, 2345–46, 94 L.N.T.S. 57, 63 (Pact of Paris); *see also infra* note 15 and accompanying text.

12. *See* SAN REMO MANUAL ON INTERNATIONAL LAW APPLICABLE TO ARMED CONFLICTS AT SEA 68, ¶¶ 13(d), 14–26, 29–32, 34–36, 67–71, 74–75, 86–88, 92–94, 99, 106, 109, 111, 113–16, 118–20, 122–24, 126–27, 130, 132–34, 146–58 (Louise Doswald-Beck ed. 1995) [hereinafter SAN REMO MANUAL].

13. *See* International Law Association, International Committee on Maritime Neutrality, *Neutrality and Naval Warfare* (Michael Bothe, rptr.), *in* International Law Association, Report of the Sixty-Fifth Conference: Cairo, Egypt 163 (1993); International Law Association, International Committee on Maritime Neutrality, *Neutrality and Naval Warfare* (Michael Bothe, rptr.) *in* International Law Association, Report of the Sixty-Sixth Conference: Buenos Aires, Argentina 570 (1994); International Law Association, International Committee on Maritime Neutrality, *Neutrality and Naval Warfare* (Michael Bothe, rptr.; Wolff Heintschel von Heinegg, alt. rptr.), *in* International Law Association, Report of the Sixty-Seventh Conference: Helsinki, Finland 367 (1996); International Law Association, Committee on Maritime Neutrality, *Final Report: Helsinki Principles on the Law of Maritime Neutrality* (Dietrich Schindler, chair; von Heinegg, rptr.), *in* International Law Association, Report of the Sixty-Eighth Conference Held at Taipei, Taiwan, Republic of China 496 (1998) (Helsinki Principles). For a critique of the Cairo report, *see* Walker, *Maritime Neutrality, supra* note 1.

14. *E.g.*, COLOMBOS, *supra* note 5, § 759; MCDOUGAL & FELICIANO, *supra* note 5, at 197–436; 2 O'CONNELL, *supra* note 5, at 1141–42; Bothe, *Neutrality at Sea, supra* note 5, at 205; Thomas A. Clingan, Jr., *Submarine Mines in International Law, in* Robertson, *supra* note 5, at 351, 352 (argument that neutrality no longer exists is specious); Gioia & Ronzitti, *supra* note 5, at 223; Vaughan Lowe, *The Commander's Handbook of the Law of Naval Operations, in* Robertson, *supra* note 5, at 109, 134–38; McNeill, *supra* note 5, at 642–43; Natalino Ronzitti, *The Crisis of the Traditional Law Regulating International Armed Conflicts at Sea and the Need for Its Revision, in* THE LAW OF NAVAL WARFARE; A COLLECTION OF AGREEMENTS AND DOCUMENTS 1, 6–12 (Ronzitti ed. 1988); Williams, *supra* note 5, at 47–48; Wiswall, *supra* note 5, at 619. Even commentators arguing that the force of the law of neutrality has been greatly diminished do not say it has disappeared in the Charter era. *See, e.g.*, ALFORD, *supra* note 7, at 326; Janis, *supra* note 5, at 153; Norton, *supra* note 5, at 311.

15. UN Charter, art. 103. In 1928 the Pact of Paris was concluded, *supra* note 11. Subject to later agreements such as the Charter, the Pact remains in force today. *See* Pact of Paris, *supra* note 11, arts. 1–2, 46 Stat. 2343, 2345–46, 94 L.N.T.S. 57, 63; UN Charter, art. 103; United States Department of State, Treaties in Force 447 (1999) (TIF); GOODRICH *ET AL.*, *supra* note 9, at 614–17; SIMMA, *supra* note 9, at 1116–25.

16. I.C.J. Statute, art. 38(1).

17. *E.g.*, IAN BROWNLIE, PRINCIPLES OF PUBLIC INTERNATIONAL LAW 1–25 (5th ed. 1998), citing *The Scotia*, 81 US (5 Wall.) 170, 181–82 (1872); 1 OPPENHEIM'S INTERNATIONAL LAW §§ 9–14 , at 28 (Robert Jennings & Arthur Watts eds., 9th ed. 1992) (1 OPPENHEIM).

18. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 102(3), 102(4) & cmt. f (1987) (RESTATEMENT [THIRD]); GERHARD VON GLAHN, LAW AMONG NATIONS: AN INTRODUCTION TO PUBLIC INTERNATIONAL LAW 20–21 (6th ed.

1992); OSCAR SCHACHTER, INTERNATIONAL LAW IN THEORY AND PRACTICE 50–55 (1991); *cf.* ANNOTATED SUPPLEMENT, *supra* note 5, at xxxvii-xxxviii, ¶¶ 5.4–5.4.2 (recognition of custom, treaties).

19. Nearly all agree that qualified scholars are only a secondary source, or are evidence of rules of law. I.C.J. Statute, art. 38(1)(d); BROWNLIE, *supra* note 17, at 24; 1 OPPENHEIM, *supra* note 17, § 14; RESTATEMENT (THIRD), *supra* note 18, § 103(2)(c); VON GLAHN, *supra* note 18, at 21; *but see* Annotated Supplement, *supra* note 5, at xxxvii-xxxviii, ¶¶ 5.4-5.4.2 (only custom, treaties recognized).

20. UN Charter, arts. 51, 103. This is particularly true if the right to self-defense is a *jus cogens* norm. To the extent the Charter and action pursuant to it is customary law or perhaps *jus cogens*, later custom or *jus cogens* might trump inconsistent earlier customary obligations or an older treaty. I.C.J. Statute, art. 38(1); Vienna Convention on the Law of Treaties, May 23, 1969, preamble, arts. 53, 64, 1155, 1159, U.N.T.S. 331, 333, 341 (Vienna Convention). *Compare, e.g., Military & Paramilitary Activities in & Against Nicaragua* (*Nicaragua v. United States*), 1986 I.C.J. 14, 347 (Schwebel, J., dissenting) (*Nicaragua* Case); STANIMAR A. ALEXANDROV, SELF-DEFENSE AGAINST THE USE OF FORCE IN INTERNATIONAL LAW 296 (1996); BOWETT, *supra* note 5, 187–93; 1 OPPENHEIM, *supra* note 17, 127; KELSEN, COLLECTIVE SECURITY, *supra* note 5, at 27; TIMOTHY L.H. MCCORMACK, SELF-DEFENSE IN INTERNATIONAL LAW: THE ISRAELI RAID ON THE IRAQI NUCLEAR REACTOR 122–24, 238–39, 253–84, 302 (1996); MCDOUGAL & FELICIANO, *supra* note 5, at 232–41; OSCAR SCHACHTER, INTERNATIONAL LAW IN THEORY AND PRACTICE 152–55 (1991); SHARP, *supra* note 4, at 33–48 (real debate is the scope of the anticipatory self-defense right; responses must be proportional); JULIUS STONE, OF LAW AND NATIONS: BETWEEN POWER POLITICS AND HUMAN HOPES 3 (1974); ANN VAN WYNEN THOMAS & A.J. THOMAS, THE CONCEPT OF AGGRESSION IN INTERNATIONAL LAW 127 (1972); George Bunn, *International Law and the Use of Force in Peacetime: Do U.S. Ships Have to Take the First Hit?*, 39 NAVAL WAR COLLEGE REVIEW 69–70 (May–June 1986); Christopher Greenwood, *Remarks, Major Maritime Events in the Persian Gulf War, in* Panel, *Neutrality, The Rights of Shipping and the Use of Force in the Persian Gulf War (Part I)*, 1988 AMERICAN SOCIETY OF INTERNATIONAL LAW PROCEEDINGS 158, 160–61; David K. Linnan, *Self-Defense, Necessity and U.N. Collective Security: United States and Other Views*, 1991 DUKE JOURNAL OF COMPARATIVE AND INTERNATIONAL LAW 57, 65–84, 122; Lowe, *supra* note 14, at 127–30; James McHugh, *Forcible Self-Help in International Law*, 25 NAVAL WAR COLLEGE REVIEW 61 (No. 2, 1972); Rein Mullerson & David J. Scheffer, *Legal Regulation of the Use of Force, in* BEYOND CONFRONTATION: INTERNATIONAL LAW FOR THE POST-COLD WAR ERA 93, 109–14 (Lori Fisler Damrosch *et al.* eds. 1995); John F. Murphy, *Commentary on Intervention to Combat Terrorism and Drug Trafficking, in* LAW AND FORCE IN THE NEW INTERNATIONAL ORDER 241 (Lori Fisler Damrosch & David J. Scheffer, eds., 1991); W. Michael Reisman, *Allocating Competences to Use Coercion in the Post-Cold War World: Practices, Conditions, and Prospects, in id.* 25, 45; Horace B. Robertson, Jr., *Contemporary International Law: Relevant to Today's World?*, 45 NAVAL WAR COLLEGE REVIEW 89, 101 (1992); Robert F. Turner, *State Sovereignty, International Law, and the Use of Force in Countering Low-Intensity Aggression in the Modern World, in* LEGAL AND MORAL CONSTRAINTS ON LOW-INTENSITY CONFLICT 43, 62–80 (Alberto R. Coll *et al.* eds., 1995) (Vol. 67, US Naval War College International Law Studies); Claude Humphrey Meredith Waldock, *The Regulation of Force by Individual States in International Law*, 81 RECUEIL DES COURS DE L'ACADÉMIE DE DROIT INTERNATIONAL 451, 496–99 (1952) (anticipatory self-defense permissible, as long as principles of necessity, proportionality observed) *with, e.g.*, BROWNLIE, *supra* note 5, at 257–61, 275–78, 366–67; DINSTEIN, *supra* note 5, at 182–87, 190; LOUIS HENKIN, INTERNATIONAL LAW: POLITICS AND VALUES 121–22 (1995); PHILIP C. JESSUP, A MODERN LAW OF NATIONS 166–67 (1948); D.P. O'CONNELL, THE INFLUENCE OF LAW ON SEA POWER 83, 171 (1979); 2 OPPENHEIM, *supra* note 5, § 52aa, at 156;

AHMED M. RIFAAT, INTERNATIONAL AGGRESSION 126 (1974); SIMMA, *supra* note 9, at 675–76; Tom Farer, *Law and War, in* 3 CYRIL E. BLACK & RICHARD A. FALK, THE FUTURE OF THE INTERNATIONAL LEGAL ORDER 30, 36–37 (1971); Yuri M. Kolosov, *Limiting the Use of Force: Self-Defense, Terrorism, and Drug Trafficking, in* LAW AND FORCE; Josef L. Kunz, *Individual and Collective Self-Defense in Article 51 of the Charter of the United Nations,* 41 AMERICAN JOURNAL OF INTERNATIONAL LAW 872, 878 (1947); Rainer Lagoni, *Remarks, in* Panel, *supra*; Robert W. Tucker, *The Interpretation of War Under Present International Law,* 4 INTERNATIONAL LAW QUARTERLY 11, 29–30 (1951); *see also* Robert W. Tucker, *Reprisals and Self-Defense,* 66 AMERICAN JOURNAL OF INTERNATIONAL LAW 586 (1972) (States may respond only after being attacked. US policy is that States may respond in anticipatory self-defense, subject to necessity and proportionality principles, and admitting of no other alternative. ANNOTATED SUPPLEMENT, *supra* note 5, ¶¶ 4.3.2–4.3.2.1. George K. Walker, *Anticipatory Collective Self-Defense in the Charter Era: What the Treaties Have Said,* 365, 379, 381–86, 351–59, *in* THE LAW OF MILITARY OPERATIONS: LIBER AMICORUM PROFESSOR JACK GRUNAWALT (Michael N. Schmitt ed., 1998) (Vol. 72, US Naval War College International Law Studies) discusses drafting of Article 51, UN Charter. The right of self-defense also inheres to belligerents' warships while in neutral waters, or neutral warships in belligerents' waters as well as on the high seas, Helsinki Principle 5.1.1 & cmt., *supra* note 13, at 506. Some defense treaties are not published, RESTATEMENT (THIRD), *supra* note 18, § 312 r.n.5; *see also* 1 US Code. § 112a(b) (1994). UN Charter, art. 102 requires treaties to be published in *United Nations Treaty Series* if parties wish to invoke them before a UN organ; Covenant of the League of Nations, art. 18, required members to register all treaties with the League; they were not binding until registered. Article 18 was among US President Woodrow Wilson's Fourteen Points. GOODRICH *ET AL.*, *supra* note 9, at 610–14; SIMMA, *supra* note 9, at 1103–16. National legislation may require publication of agreements or notifying the national legislature of all international agreements, *e.g.,* 1 US Code § 112b (1994). Some commentators believe *jus cogens*, e.g., perhaps the right of self-defense, may trump treaty law: *See* Carin Kahghan, *Jus Cogens and the Inherent Right to Self-Defense,* 3 INTERNATIONAL LAW STUDENTS ASSOCIATION JOURNAL OF INTERNATIONAL AND COMPARATIVE LAW 767, 827 (1997).

21. UN Charter, arts. 25, 48, 103 (Council decisions). *See also* Lalive, *supra* note 5, at 78-81; SYDNEY D. BAILEY & SAM DAWS, THE PROCEDURE OF THE UN SECURITY COUNCIL ch. 1.5 (3d ed. 1998); JORGE CASTENEDA, LEGAL EFFECTS OF UNITED NATIONS RESOLUTIONS ch. 3 (Alba Amoia trans. 1969); GOODRICH ET AL., *supra* note 9, at 126, 144, 290–314; SIMMA, *supra* note 9, at 284, 407–18, 605–36, 652; CASTREN, *supra* note 5, at 434. Nonbinding Assembly or Council resolutions can add strength to a preexisting norm to evidence its existence and vitality or can contribute to development of a new norm. BROWNLIE, *supra* note 17, at 14–15, 694; 1 OPPENHEIM, *supra* note 17, § 16, at 47–49; RESTATEMENT (THIRD), *supra* note 18, § 103(2)(d), cmt. c, r.n.2.

22. Helsinki Principles 1.4, 3.1, 4, *supra* note 13, at 500, 503, 505; ANNOTATED SUPPLEMENT, *supra* note 5, ¶¶ 8.1–8.1.3; San Remo Manual, *supra* note 12, ¶¶ 34–42, 44, 46. Protocol for Prohibition of Use in War of Asphyxiating, Poisonous or Other Gases, & of Bacteriological Methods of Warfare, with US no-first-use reservation, June 17, 1925 & Apr. 10, 1975, 26 U.S.T. 571, 94 L.N.T.S. 65 (gas, bacteriological warfare).

23. *See supra* note 20 and accompanying text.

24. One example of Charter law modifications is the UN Charter, art. 103, treaty trumping provision.

25. Helsinki Principle 1.2 & cmt., *supra* note 13, at 499; Dietrich Schindler, *Commentary, in* LAW OF NAVAL WARFARE, *supra* note 14, at 211.

26. RESTATEMENT (THIRD), *supra* note 18, § 103.

27. *Cf.* Helsinki Principle 1.2 & cmt., *supra* note 13, at 499.

28. UN Charter, art. 2(5); Quincy Wright, *The Outlawry of War and the Law of War,* 47 AMERICAN JOURNAL OF INTERNATIONAL LAW 365, 371–72 (1953). Permanently neutral countries have supported UN action. *See, e.g.,* GABRIEL, *supra* note 5, at 132–33 (Swedish, Swiss economic aid and/or support during Korean War); ROSS, *supra* note 5, chs. 7–9 (Swedish, Swiss actions against Rhodesia).

29. Helsinki Principles 1.4, 3.1, 4, *supra* note 13, at 500, 503, 505; ANNOTATED SUPPLEMENT, *supra* note 5, ¶¶ 8.1-8.1.3; SAN REMO MANUAL, *supra* note 12, ¶¶ 34–42, 44, 46.

30. International law prohibits belligerents' hostile acts in neutral territory, including a neutral's land and internal waters, territorial sea, and airspace, or using neutral territory as a sanctuary. Convention Respecting Rights & Duties of Neutral Powers & Persons in Case of War on Land, Oct. 18, 1907, art. 1, 36 Stat. 2310, 2322 (Hague V); Convention Concerning Rights & Duties of Neutral Powers in Naval War, Oct. 18, 1907, art. 2, 36 Stat. 2415, 2427 (Hague XIII); Convention on Maritime Neutrality, Feb. 28, 1928, art. 3, 47 Stat. 1989, 1991, 135 L.N.T.S. 187, 196 (Maritime Neutrality Convention). The United States is party to it and to the Convention Regarding Rights of Neutrals at Sea, July 22, 1854, 10 *id.* 1105, in force among Nicaragua, the former USSR and the United States. TIF, *supra* note 15, at 445-46, 470-71. *See also* General Declaration of Neutrality of the American Republics, Oct. 3, 1939, ¶ 3(a), 3 BEVANS 604, 605 (General Declaration), among 21 Western Hemisphere countries including the United States; Declaration for the Purpose of Establishing Similar Rules of Neutrality, May 27, 1938, arts. 8-10, 11, 188 L.N.T.S. 294, 301, 308-09, 315, 321, 329 (Nordic Neutrality Rules), among Denmark, Finland, Iceland, Norway and Sweden. Commission of Jurists, Hague Rules of Air Warfare, Dec. 1922 - Feb. 1923 (Hague Air Rules) art. 40, *reprinted in* DIETRICH SCHINDLER & JIRI TOMAN, THE LAWS OF ARMED CONFLICT 207, 214 (3d ed. 1988). *See also* Helsinki Principle 1.4, *supra* note 13, at 500; 3 HYDE, *supra* note 5, § 887; 2 HOWARD S. LEVIE, THE CODE OF INTERNATIONAL ARMED CONFLICT 785 (1985); ANNOTATED SUPPLEMENT, *supra* note 5, ¶ 7.3; SAN REMO MANUAL, *supra* note 12, ¶¶ 17–18; US Department of the Air Force, International Law—The Conduct of Armed Conflict and Air Operations ¶ 2–6c (1976) (AFP 110-31). Hague V, *supra,* reflects custom as to its rules on neutral territory; ANNOTATED SUPPLEMENT, *supra* note 5, ¶¶ 7.3 n.22, 7.3.2 n.32. Where the Maritime Neutrality Convention, *supra,* parallels their terms, it too can be assumed to restate custom. Hague Air Rules, *supra,* are generally regarded as declaring customary law.

31. UN Charter, arts. 2(4), 103; *see also* note 9, Pact of Paris, *supra* note 11; United States Department of State, Treaties in Force 439 (1998) (TIF); GOODRICH *ET AL.*, *supra* note 9, at 614–17; SIMMA, *supra* note 9, at 1116–25. Commentators and countries continue debating whether anticipatory self-defense, i.e., a response with force that is necessary, proportional and admitting of no other alternative, is permitted in the UN Charter era. *Compare, e.g., Nicaragua* Case, *supra* note 20, at 14, 347 (Schwebel, J., dissenting); STANIMAR A. ALEXANDROV, SELF-DEFENSE AGAINST THE USE OF FORCE IN INTERNATIONAL LAW 296 (1996); BOWETT, *supra* note 5, at 187–93; 1 OPPENHEIM, *supra* note 20, § 127; KELSEN, COLLECTIVE SECURITY, *supra* note 5, at 27; MCCORMACK, *supra* note 20, at 122–24, 238–39, 253–84, 302; MCDOUGAL & FELICIANO, *supra* note 5, at 232–41; SCHACHTER, *supra* note 18, at 152–55; SHARP, *supra* note 4, at 33–48 (real debate is the scope of the anticipatory self-defense right; responses must be proportional); STONE, *supra* note 20, at 3; THOMAS & THOMAS, *supra* note 20, at 127; Bunn, *supra* note 20, at 69–70; Greenwood, *Remarks, in* Panel, *supra* note 20, at 158, 160–61; Linnan, *supra* note 20, at 57, 65–84, 122; Lowe, *supra* note 14, at 127–30; McHugh, *supra* note 20, at 61; Mullerson & Scheffer, *supra* note 20, at 93, 109–14; Murphy, *supra* note 20, at 241; Reisman, *supra* note 20, at 25, 45; Robertson, *supra* note 20, at 89, 101; Turner, *supra* note 20, at 43, 62–80; Waldock, *supra* note 20, at 451, 496–99 (anticipatory self-defense permissible, as long as principles of necessity, proportionality observed) *with, e.g.,* BROWNLIE, *supra* note 5, at 257–61, 275–78, 366–67; DINSTEIN, *supra* note 5, at 182–87, 190; HENKIN, *supra* note 20, at 121–22; JESSUP, *supra*

note 20, at 166–67; O'CONNELL, *supra* note 20, at 83, 171; 2 OPPENHEIM, *supra* note 5, 52aa, at 156; RIFAAT, *supra* note 20, at 126; SIMMA, *supra* note 9, at 675–76; Farer, *supra* note 20, at 30, 36–37; Kolosov, *supra* note 20, at 232, 234; Kunz, *supra* note 20, at 872, 878; Lagoni, *supra* note 20, at 161, 162; Tucker, *The Interpretation of War Under Present International Law, supra* note 20, at 11, 29–30; *see also* Tucker, *Reprisals and Self-Defense, supra* note 20, at 586 (States may respond only after being attacked). The former USSR generally subscribed to the restrictive view. Kolosov, *supra* note 20, at 234; Mullerson & Scheffer, *supra* note 20, at 107. US policy is that States may respond in anticipatory self-defense, subject to necessity and proportionality principles, and admitting of no other alternative. ANNOTATED SUPPLEMENT, *supra* note 5, ¶¶ 4.3.2-4.3.2.1. *Nicaragua* Case, *supra* note 20, at 103, declined to address the issue.

32. UN Charter, arts. 51, 103; *see also supra* notes 20, 31. A neutral member of a collective self-defense alliance, permitted by UN Charter, art. 51, may assist an alliance member that is a target of aggression by joining the self-defense response. If that occurs, whatever neutrality the assisting State might have claimed is lost, and it becomes a cobelligerent against the aggressor. On the other hand, it is possible for the neutral member to declare neutrality and confine its responses to retorsions and nonforce reprisals. If so, this may be a violation of the alliance treaty, but that is a matter between the neutral and the target of aggression. If a belligerent attacks enemy forces taking refuge on neutral territory, or these forces are there for other purposes, 2 OPPENHEIM, *supra* note 5, § 320, at 685, says this is not hostilities against a neutral, "but are mere violations of neutrality; and they must be repulsed, or reparation must be made for them, . . . ," citing *id.* § 362. Besides a violation of neutrality law, it is submitted that an attacking belligerent, unless attacking under a theory of necessity, has committed a violation of UN Charter, art. 2(4), rendering it susceptible to self-defense or other responses by the invaded neutral; *cf.* 1 OPPENHEIM, *supra* note 20, § 326.

33. In naval warfare, for example, if a neutral cannot or will not enforce its duty to require belligerent forces to cease and desist from the conduct of hostilities while in that neutral's waters, an aggrieved belligerent may act against those belligerent forces present in neutral waters. Helsinki Principle 2.1, *supra* note 13, at 501; ANNOTATED SUPPLEMENT, *supra* note 5, ¶ 7.3; 2 O'CONNELL, *supra* note 5, at 1118–19 (*Dresden, Altmark* incidents); 2 OPPENHEIM, *supra* note 5, §§ 325–25a (same).

34. UN Charter, arts. 51, 103; *see also supra* notes 20, 31, 32 and accompanying text.

35. Under Hague V, Art. 3, and Hague XIII, Art. 5, the latter applying to naval warfare, belligerents may not "(a) Erect on the territory of a neutral Power a wireless telegraphy station or other apparatus for . . . communicating with belligerent forces on land or sea; [or] (b) Use any installation of this kind established by them before the war on the territory of a neutral Power for purely military purposes, and which has not been opened for the service of public messages." Hague V, *supra* note 30; Hague XIII, *supra* note 30. Under Hague V, Arts. 8–9, "A neutral Power is not called upon to forbid or restrict the use on behalf of belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies of private individuals. . . . Every measure of restriction or prohibition . . . must be impartially applied . . . to both belligerents. A neutral Power must see to the same obligation being observed by companies or . . . individuals owning telegraph or telephone cables or wireless telegraphy apparatus." The 1923 Hague Radio Rules echo these principles, adding that belligerent mobile radio stations must abstain from using their apparatus. Commission of Jurists to Consider & Report Upon Revision of Rules of Warfare, Rules for the Control of Radio in Time of War, Feb. 19, 1923, arts. 2–4 (Hague Radio Rules), *reprinted in* LAW OF NAVAL WARFARE, *supra* note 14, at 367, 368.

36. *See supra* note 33 and accompanying text.

37. A neutral cannot, however, allow belligerents to establish intelligence offices on its territory. 2 OPPENHEIM, *supra* note 5, § 356, at 748–51; *see also* 11 WHITEMAN, *supra* note 5, at 220.

38. *See supra* note 35.

39. Hague V, *supra* note 30, art. 19, 36 Stat. at 2326; *compare* Convention with Respect to Laws & Customs of War on Land, July 29, 1899, Regulations, art. 54, 32 *id.* 1803, 1823; *see also* 2 LEVIE, *supra* note 30, at 832.

40. 2 OPPENHEIM, *supra* note 5, § 355, at 747.

41. Hague V, *supra* note 30, arts. 13-14, 36 Stat. at 2324–25; ANNOTATED SUPPLEMENT, *supra* note 5, ¶ 7.3.1.

42. This is by analogy from the rule that vehicles transporting sick and wounded carry no combatants or war materials and rules for belligerent radio stations on neutral territory. *See supra* notes 35–36 and 39–41 and accompanying text.

43. *See supra* note 41 and accompanying text.

44. *See* UN Charter, art. 103. United Nations Convention on the Law of the Sea, Dec. 10, 1982, art. 221, 1833 U.N.T.S. 3, 489 (LOS Convention); Convention Relating to Intervention on the High Seas in Cases of Oil Pollution Casualties, Nov. 29, 1969, art. 1(1), 26 U.S.T. 765, 767, 970 U.N.T.S. 211, 212 (Intervention Convention); *see also* 4 UNITED NATIONS CONVENTION ON THE LAW OF THE SEA: A COMMENTARY ¶¶ 221.1–221.9(h) (Myron H. Nordquist et al. eds., 1991); 2 O'CONNELL, *supra* note 5, at 1006–8. The 1958 Law of the Sea Conventions and the LOS Convention "other rules" clauses, repeated in the navigational articles, have almost universally been said to mean the LOS is subject to the LOAC in appropriate situations. *Compare, e.g.,* LOS Convention preamble (matters not regulated by Convention to be governed by rules, principles of international law), arts. 2(3) (territorial sea), 19(1), 21(1), 31 (innocent passage), 34(2) (straits transit passage), 58(1), 58(3) (EEZs), 78(2) (continental shelf; coastal State cannot infringe or interfere with "navigation and other rights and freedoms of other States as provided in this Convention"), 87(1) (high seas), 138 (the Area), 303(4) (archaeological, historical objects found at sea; "other international agreements and rules of international law regarding the protection of objects of an archaeological and historical nature"), 1833 U.N.T.S. at 398, 400, 404–05, 408, 410, 419, 431–32, 446, 517, *with, e.g.,* Convention on the High Seas, Apr. 29, 1958, preamble, art. 2, 13 U.S.T. 2312, 2314, 450 U.N.T.S. 11, 82 (High Seas Convention), (treaty restates customary law); Convention on the Territorial Sea & Contiguous Zone, Apr. 29, 1958, arts. 1(2), 14(4), 17, 22(2), 15 *id.* 1606, 1608, 1610, 1611, 1612, 516 U.N.T.S. 205, 206–08, 214, 216, 220 (Territorial Sea Convention). Although the other 1958 law of the sea conventions do not have other rules clauses, they say they do not affect the status of waters above that are part of the high seas, for the continental shelf; or other high seas rights, for high seas fisheries. Convention on the Continental Shelf, Apr. 29, 1958, arts. 1, 3, *id.* 471, 473, 499 U.N.T.S. 311, 312, 314 (Continental Shelf Convention); Convention on Fishing & Conservation of Living Resources of the High Seas, Apr. 29, 1958, arts. 1–8, 13, 17 *id.* 138, 140–43, 559 U.N.T.S. 285, 286–92, 296 (Fishery Convention); Territorial Sea Convention, *supra,* art. 24(1), 15 *id.* at 1612, 516 U.N.T.S. at 220 (contiguous zone). Thus the High Seas Convention regime, including its Article 2 other rules provision, is incorporated by reference into these Conventions, which modify some High Seas Convention principles but not the Article 2 other rules clause. The LOS Convention, *supra,* art. 33, 1833 U.N.T.S. at 409, governing the contiguous zone, refers to an ocean belt contiguous to the territorial sea, which is part of the high seas except declared EEZ, fishing or continental shelf areas, otherwise subject to the high seas regime. *See also* JESSUP, *supra* note 2; JESSUP & DEAK, *supra* note 3; W. ALISON PHILLIPS & ARTHUR H. REEDE, NEUTRALITY: THE NAPOLEONIC PERIOD (1936); EDGAR TURLINGTON, NEUTRALITY: ITS HISTORY, ECONOMICS AND LAW (1936).

45. The LOS conventions also promote a due regard principle for shared ocean uses; one user must observe due regard for other users' rights, e.g., a right to lay cables that might carry Internet messages. *Compare* LOS Convention, *supra* note 44, arts. 87, 112–15, 1833 U.N.T.S. at 433, 440 *with* High Seas Convention, *supra* note 44, arts. 2, 26–29, 13 U.S.T. at 2314, 2319–20, 450 U.N.T.S. at 82, 96–98; Convention for Protection of Submarine Cables, Mar. 14, 1884, 24 Stat. 989; Declaration Respecting Interpretation of Articles II & IV, Dec. 1, 1886, 25 *id.* 1424; *see also*

COLOMBOS, *supra* note 5, §§ 399–400; 3 UNITED NATIONS CONVENTION ON THE LAW OF THE SEA 1982: A COMMENTARY ¶ 87.9(k) (Myron H. Nordquist et al. eds., 1995); ANNOTATED SUPPLEMENT, *supra* note 5, ¶ 2.4.3; 2 O'CONNELL, *supra* note 5, at 796–99, 819–24; 1 OPPENHEIM, *supra* note 17, §§ 285, at 789; 310–11; RESTATEMENT (THIRD), *supra* note 18, § 521(3); Bernard H. Oxman, *The Regime of Warships Under the United Nations Convention on the Law of the Sea*, 24 VIRGINIA JOURNAL OF INTERNATIONAL LAW 837–88 (1984); Horace B. Robertson, Jr., *The "New" Law of the Sea and the Law of Armed Conflict at Sea,* 273–74, *in* READINGS ON INTERNATIONAL LAW FROM THE NAVAL WAR COLLEGE REVIEW 1978–1994 (John N. Moore & Robert F. Turner eds., 1994) (Vol. 68, US Naval War College International Law Studies). Due regard clauses apply to other sea areas. *See, e.g.*, LOS Convention, *supra* note 44, arts. 27(4) (territorial sea), 39(3)(a) (straits transit passage), 56(2), 58(3), 60(3) (EEZ), 79(5) (cables, pipelines), 142(1), 148 (the Area), 234 (ice-covered areas), 1833 U.N.T.S. at 407-08, 411–12, 418–20, 430, 448, 450, 493; Continental Shelf Convention, *supra* note 44, arts. 1, 3–5(1), 15 U.S.T. at 473, 499 U.N.T.S. at 312, 314 ("reasonable measures for exploration . . . [and] exploitation" of continental shelf balanced against right to lay, maintain submarine cables, pipelines; continental shelf exploration, exploitation must not result in "unjustifiable interference with" navigation, high seas fishing, oceanographic research); Territorial Sea Convention, *supra* note 44, art. 19(4), 15 U.S.T. at 1611, 516 U.N.T.S. at 216–18 (due regard for navigation interests); *see also* RESTATEMENT (THIRD), *supra* note 18, §§ 511(b)–511(d), 514–15. LOS Convention, *supra* note 44, art. 311(1), 1833 U.N.T.S. at 519, declares it supersedes the Continental Shelf, High Seas and Territorial Sea Conventions, *supra* note 44, among parties to the LOS Convention. Recent commentaries advocate a due regard standard for belligerents during war; e.g., they must pay due regard to neutrals' high seas, continental shelf and EEZ rights and duties besides observing other LOAC rules. Helsinki Principles 3.1, 4 & cmts., *supra* note 13, at 503, 505; San Remo Manual, *supra* note 12, ¶¶ 34–36; Robertson, *supra* at 303. Helsinki Principle 1.4, cmt., *supra* note 13 at 500-01, recites a due regard standard in a context of requiring proportional attacks under the LOAC where neutral territory, waters or airspace might be involved.

46. *See supra* note 44 and accompanying text.

47. A country creating the state of impossibility of performance cannot invoke the principle. Vienna Convention, *supra* note 20, art. 61, 1155 U.N.T.S., at 346; BROWNLIE, *supra* note 17, at 623; T.O. ELIAS, THE MODERN LAW OF TREATIES 177–87 (1974); RESTATEMENT (THIRD), *supra* note 18, §§ 102–03, 128–30; Helsinki Principle 1.3 & cmt., *supra* note 13, at 499; International Law Commission, Report on the Work of Its Eighteenth Session, *Report of the Commission to the General Assembly,* UN Doc. A/6309/Rev. 1, *reprinted in* 2 (1974) YEARBOOK OF THE INTERNATIONAL LAW COMMISSION 225–26 (ILC Report); 1 OPPENHEIM, *supra* note 17, § 650; RESTATEMENT (THIRD), *supra* note 18, § 336 cmt. c & r.n.3; George K. Walker, *Integration and Disintegration in Europe: Reordering the Treaty Map of the Continent,* 6 TRANSNATIONAL LAW 1, 65–66 (1993); *but see* LORD MCNAIR, THE LAW OF TREATIES 685 (2d ed. 1961) (no separate impossibility doctrine).

48. Fundamental change of circumstances may not be invoked to suspend or terminate humanitarian law treaty obligations, particularly their reprisal provisions, or by a party causing the problem. Vienna Convention, *supra* note 20, art. 62, 1155 U.N.T.S. at 347; *see also Gabcikovo-Nagymaros Project* (Hung. v. Slovakia), 1997 I.C.J. 7, 39 (art. 62 a customary norm); *Fisheries Jurisdiction* (U.K. v. Ice.), 1973 I.C.J. 3, 18 (same); BROWNLIE, *supra* note 17, at 623–26; Harvard Draft Convention on the Law of Treaties, art. 28, 29 AMERICAN JOURNAL OF INTERNATIONAL LAW SUPPLEMENT 657, 662–63 (1935); Helsinki Principle 1.3 & cmt., *supra* note 13, at 499; MCNAIR, *supra* note 47, at 685–91; 1 OPPENHEIM, *supra* note 17, § 651; RESTATEMENT (THIRD), *supra* note 18, §§ 336, 339; IAN SINCLAIR, THE VIENNA CONVENTION ON THE LAW OF TREATIES 20 (2d ed. 1984); David Bederman, *The 1871 London*

Declaration, Rebus Sic Stantibus and a Primitivist View of the Law of Nations, 82 AMERICAN JOURNAL OF INTERNATIONAL LAW 1 (1988); Gyorgy Harsatzti, *Treaties and the Fundamental Change of Circumstances,* 146 RECUEIL DES COURS DE L'ACADÉMIE De DROIT INTERNATIONAL 1, 21 (1975); Walker, *supra* note 47, at 66–68; *compare* ARIE E. DAVID, THE STRATEGY OF TREATY TERMINATION ch. 1 (1975); Oliver J. Lissitzyn, *Treaties and Changed Circumstances,* 61 AMERICAN JOURNAL OF INTERNATIONAL LAW 895 (1967) (criticizing Vienna Convention approach) *with* ELIAS, *supra* note 47, at 119–28 (traditional *rebus sic stantibus* approach no longer admissible today).

49. Vienna Convention, *supra* note 20, art. 60, 1155 U.N.T.S. at 346; *see also Gabcikovo-Nagymaros Project, supra* note 48, at 39 (Article 60 a customary norm); *Namibia,* 1971 I.C.J. 4, 47; BROWNLIE, *supra* note 17, at 622–23; ILC Report, *supra* note 47, at 253–255; MCNAIR, *supra* note 47, ch. 36; 1 OPPENHEIM, *supra* note 17, § 649; SINCLAIR, *supra* note 48, at 20, 166, 188–90.

50. Kahghan, *supra* note 20, at 767, 827. Belligerents can respond by non-force reprisals or retorsions. TUCKER, *supra* note 5, at 199 n.5. Reprisal has been characterized as a kind of self-help or sanction. Most commentators say reprisals involving force against a State not engaged in armed conflict with the acting State are not lawful in the Charter era. However, other coercion that is unlawful, e.g., deliberate breach of a trade treaty to compel a State engaging in unlawful conduct to comply with international norms, is admissible. Anticipatory reprisal using force is forbidden. A State considering reprisal must first call upon an offending State to mend its ways. *Compare* Declaration on Principles of International Law Concerning Friendly Relations & Co-Operation Among States in Accordance with the Charter of the United Nations, G.A. Res. 2625, ¶¶ 1, 3, UN GAOR, 25th Sess., Supp. No. 28, U.N. Doc. A/8028 (1970), *reprinted in* 9 I.L.M. 1292, 1294, 1297 (1970); *Gabcikovo-Nagymaros Project, supra* note 48, at 54; *Nicaragua* Case, *supra* note 20, at 14, 127; *Air Service Agreement of 27 March 1946* (U.S. v. Fr.), 18 R.I.A.A. 417, 443; BOWETT, *supra* note 5, at 13; J.B. BRIERLY, THE LAW OF NATIONS 401–02 (Humphrey Waldock ed., 6th ed. 1963); BROWNLIE, *supra* note 5, at 281; GOODRICH *ET AL.*, *supra* note 9, at 340–47; ROSALYN HIGGINS, THE DEVELOPMENT OF INTERNATIONAL LAW THROUGH THE POLITICAL ORGANS OF THE UNITED NATIONS 217 (1963); ANNOTATED SUPPLEMENT, *supra* note 5, ¶ 6.2.3.1; 2 OPPENHEIM, *supra* note 5, §§ 43, 52a, at 152-53; SIMMA, *supra* note 9, at 105; STONE, *supra* note 5, at 286–87; Roberto Ago, *Addendum to Eighth Report on State Responsibility,* U.N. Doc. A/CN.4/318 & Add. 104, (1979), 2(1) YEARBOOK OF THE INTERNATIONAL LAW COMMISSION 13, 39, 42 (1981); Roberto Barsotti, *Armed Reprisals, in* ANTHONY CASSESSE, THE CURRENT LEGAL REGULATION OF THE USE OF FORCE 79 (1986); D.W. Bowett, *Reprisals Involving Recourse to Armed Force,* 66 AMERICAN JOURNAL OF INTERNATIONAL LAW 20 (1972); Rosalyn Higgins, *The Attitude of Western States Toward Legal Aspects of the Use of Force, in* CASSESSE, *supra,* at 435, 444; Tucker, *Reprisals and Self-Defense, supra* note 20, at 586–87; *with* DINSTEIN, *supra* note 5, at 215–16 (reprisals using force admissible in Charter era); LAWRENCE T. GREENBERG *ET AL.*, INFORMATION WARFARE AND INTERNATIONAL LAW 26–27 (1998). Retorsion, or retortion, is a target State's lawful but unfriendly response to another State's unfriendly practice or act whether illegal or not, to coerce the latter to discontinue that practice or act. Retorsionary responses must be proportional. BRIERLY, *supra,* at 399; WILLIAM EDWARD HALL, A TREATISE ON INTERNATIONAL LAW § 120 (A. Pearce Higgins ed., 8th ed. 1924); 2 HYDE, *supra* note 5, § 588; FRITS KALSHOVEN, BELLIGERENT REPRISALS 27 (1971); 7 MOORE, DIGEST § 1090; 2 OPPENHEIM, *supra* note 5, § 135; RESTATEMENT (THIRD), *supra* note 18, § 905 & r.n.8; SIMMA, *supra* note 9, at 104; STONE, *supra* note 5, at 288–89; Waldock, *supra* note 20, at 451, 458.

51. Vienna Convention, *supra* note 20, arts. 53, 64, 1155 U.N.T.S. at 344, 347.

52. Vienna Convention, *supra* note 20, does not provide for the operation of war, or armed conflict, on international agreements. However, other authorities agree that war may suspend or

terminate treaties, depending on the nature of the treaty and the circumstances of the conflict. *See, e.g.,* ILC Report, *supra* note 47, at 267; Institut de Droit International, *The Effects of Armed Conflict on Treaties,* Aug. 28, 1985, arts. 2, 3, 5, 11, 61(2) Annuaire 278, 280-82 (1986); *Regulations Regarding the Effect of War on Treaties,* 1912, arts. 1, 4, 7–10, *reprinted in* 7 AMERICAN JOURNAL OF INTERNATIONAL LAW 153–55 (1913); *Clark v. Allen,* 331 U.S. 503, 513 (1947); *Karnuth v. United States,* 79 U.S. 231, 240-42 (1929); *Techt v. Hughes,* 128 N.E. 185, 191 (N.Y.), *cert. denied,* 254 U.S. 643 (1920); 2 OPPENHEIM, *supra* note 5, §§ 99(4)–99(5); George B. Davis, *The Effects of War Upon International Conventions and Private Contracts,* 1927 PROCEEDINGS OF THE AMERICAN SOCIETY OF INTERNATIONAL LAW 124–29; G.G. Fitzmaurice, *The Judicial Clauses of the Peace Treaties,* 73 RECUEIL DES COURS DE L'ACADÉMIE DE DROIT INTERNATIONAL 255, 307–17 (1948); Harvard Draft Convention on the Law of Treaties, art. 28, 29 AMERICAN JOURNAL OF INTERNATIONAL LAW SUPPLEMENT 657, 662–64 (1935); Cecil J.B. Hurst, *The Effect of War on Treaties,* 2 BRITISH YEARBOOK OF INTERNATIONAL LAW 37, 40 (1921); James J. Lenoir, *The Effect of War on Bilateral Treaties, with Special Reference to Reciprocal Inheritance Treaty Provisions,* 34 GEOREGETOWN LAW JOURNAL 129, 173–77 (1946); Walker, *supra* note 47, at 68–71. Impossibility or fundamental change of circumstances claims may overlap war suspension or termination claims. Impossibility, fundamental change, etc., are the only bases for termination or suspension for treaty relations between belligerents and neutrals. Herbert W. Briggs, *The Attorney General Invokes Rebus Sic Stantibus,* 36 AMERICAN JOURNAL OF INTERNATIONAL LAW 89 (1942); Oliver J. Lissitzyn, *Treaties and Changed Circumstances,* 61 AMERICAN JOURNAL OF INTERNATIONAL LAW 911 (1967); Walker, *supra* note 47, at 68–69.

53. *See supra* note 33 and accompanying text.

54. *See supra* note 30 and accompanying text.

55. *See supra* notes 30–33 and accompanying text.

56. Hague V, Hague XIII, Maritime Neutrality Convention, *supra* note 30; Vienna Convention, *supra* note 20, preamble, art. 38, 1155 U.N.T.S. at 333, 341; BROWNLIE, *supra* note 17, at 5; 1 OPPENHEIM, *supra* note 17, §§ 10 , at 28, 11, at 32–36; RESTATEMENT (THIRD), *supra* note 18, § 102(3) & cmt. f.

57. Hague V, *supra* note 30, art. 5, 36 Stat. at 2323; Hague XIII, *supra* note 30, art. 25, *id.* at 2432; Maritime Neutrality Convention, *supra* note 30, arts. 4(a), 26, 47 *id.* at 1991, 1994, 135 L.N.T.S. at 196, 208; General Declaration, *supra* note 30, 3(c), at 605; Hague Air Rules, *supra* note 30, arts. 42, 47, at 214–15; AFP 110-31, *supra* note 30, ¶ 2-6c (air operations principle; Hague Air Rules, *supra,* not cited); 3 HYDE, *supra* note 5, §§ 855, 856A, 888; 2 LEVIE, *supra* note 30, at 788; ANNOTATED SUPPLEMENT, *supra* note 5, ¶ 7.3; 2 OPPENHEIM, *supra* note 5, §§ 316, 323, 325; TUCKER, *supra* note 5, at 260–61; *but see* Helsinki Principle 2.2, *supra* note 13, at 502 (neutral "must" take measures to enforce warship transit, sojourn rules).

58. This includes interning crew. If an enemy prize is brought to a neutral port under distress or similar conditions and does not leave when directed, its crew must be interned. Hague XIII, *supra* note 30, arts. 21, 22, 24, 36 Stat. at 2431-32; *see also* Maritime Neutrality Convention, *supra* note 30, art. 17, 47 Stat. at 1993, 135 L.N.T.S. at 204; Nordic Neutrality Rules, *supra* note 30, art. 4(1), 188 L.N.T.S. at 299, 305, 311, 319, 325. Hague XIII, *supra* note 30, art. 23 provides for an exception to this rule, entry of prizes under other than distress conditions, but several nations, including the United States, reserved to art. 23. *See* 36 Stat. at 2432, 2438. Hague XIII, arts. 21-22 are customary law; art. 23 is not because of US and UK reservations, now applying to more States through treaty succession principles. *The S.S. Appam,* 243 U.S. 124, 150–51 (1917); 3 HYDE, *supra* note 5, §§ 862, 864; 2 OPPENHEIM, *supra* note 5, §§ 328a; 333, at 706; 345; Symposium, *State Succession in the Former Soviet Union and in Eastern Europe,* 33 VIRGINIA JOURNAL OF INTERNATIONAL LAW 253 (1993); Walker, *supra* note 47. Neutrals must allow belligerent warship entry for asylum, distress or other purposes if they comply with innocent passage rules. LOS Convention, *supra* note 44, arts. 18–19, 1833 U.N.T.S. at 404 (innocent passage in distress,

but subject to other rules of international law, *i.e.*, LOAC); Territorial Sea Convention, *supra* note 44, arts. 1(2), 14, 15 U.S.T. 1608, 1610, 516 U.N.T.S. 206, 214; Helsinki Principle 2.2, *supra* note 13, at 502; ANNOTATED SUPPLEMENT, *supra* note 5, ¶ 3.2.2.1; 2 OPPENHEIM, *supra* note 5, §§ 343–46; SAN REMO MANUAL, *supra* note 12, ¶ 21.

59. Convention Respecting Laws & Customs of War on Land, Oct. 18, 1907, Regulations, Art. 54, 36 Stat. 2227, 2308. This is limited to land warfare when a belligerent occupies enemy territory and seizes or destroys landing ends of cables connecting that territory with a neutral State. COLOMBOS, *supra* note 5, § 569.

60. COLOMBOS, *supra* note 5, § 576; United States Department of the Navy, Law of Naval Warfare: NWIP 10-2 ¶ 520b (1955 through Change 6, 1974) (NWIP 10-2); *compare* Institute of International Law, The Laws of Naval War Governing the Relations Between Belligerents, art. 54 (1913), *reprinted in* SCHINDLER & TOMAN, *supra* note 30, at 857, 867 (Oxford Naval Manual). Modern manuals do not analyze the issue thoroughly, probably because of disuse of cables. *See* SAN REMO MANUAL, *supra* note 12, ¶ 37. ANNOTATED SUPPLEMENT, *supra* note 5, ¶ 1.6, at 24 discusses cables in an LOS context; *see also supra* note 45 and accompanying text.

61. *See supra* note 38 and accompanying text.

62. Neutral merchant ships acquire enemy character and may be treated as enemy merchant vessels if they operate directly under enemy control, orders, charter, employment or direction. ANNOTATED SUPPLEMENT, *supra* note 5, ¶ 7.5.2; SAN REMO MANUAL, *supra* note 12, ¶¶ 112–17. *See also* Helsinki Principle 5.1.2(4), *supra* note 13, at 507; ANNOTATED SUPPLEMENT, *supra* note 5, ¶ 8.2.2.2; SAN REMO MANUAL, *supra* note 12, ¶ 67.

63. E.g., hospital ships, medical aircraft; *see generally* Helsinki Principles 5.1.2(5)-5.1.2(6), *supra* note 13, at 507; ANNOTATED SUPPLEMENT, *supra* note 5, ¶ 8.2.3; SAN REMO MANUAL, *supra* note 12, ¶¶ 47–52, 136–40, 146, 151–52, citing treaties, custom (hospital ships; small coastal rescue craft; vessels granted safe conduct; vessels carrying cultural property; liners carrying only passengers; ships on religious, non-military scientific or philanthropic missions; small coastal fishing boats, coastal traders; vessels that have surrendered; life rafts, life boats). Neutral aircraft carrying passengers, or serving as medical or cartel aircraft, are also protected. *See* ANNOTATED SUPPLEMENT, *supra* note 5, ¶ 8.2.3; SAN REMO MANUAL, *supra* note 12, ¶¶ 140-45, 153–58.

64. *Cf.* Horace B. Robertson, Jr., *Modern Technology and the Law of Armed Conflict at Sea, in* Robertson, *supra* note 5, 362, 370; *New Technologies and Armed Conflicts at Sea,* 14 SYRACUSE JOURNAL OF INTERNATIONAL LAW AND COMMERCE 678, 704 (1988). This may mean that trying to define IW methods or means that are per se unlawful will fail, particularly when technology is developing exponentially.

65. For a discussion of high seas visit and search, *see generally* Helsinki Principles 5.2.1, 5.2.7, *supra* note 13, at 509, 511; ANNOTATED SUPPLEMENT, *supra* note 5, ¶¶ 7.6–7.6.2; SAN REMO MANUAL, *supra* note 12, ¶¶ 116, 118–24.

66. *See supra* note 62 and accompanying text.

67. E.g., requirements for placing passengers and crew in safety before destroying an enemy merchantman. Proces-Verbal Relating to Rules of Submarine Warfare Set Forth in Part IV of the Treaty of London of 22 April 1930, Nov. 6, 1936, 3 298, 173 L.N.T.S. 353; Treaty for Limitation & Reduction of Naval Armaments, Apr. 22, 1930, art. 22(2), 46 Stat. 2858, 2881, 112 L.N.T.S. 65, 88. *See also* ANNOTATED SUPPLEMENT, *supra* Bevans note 5, ¶¶ 8.2.2.2, 8.3, 8.4; SAN REMO MANUAL, *supra* note 12, ¶ 151.

68. Neutral merchantmen must observe blockades that are duly established and notified and are effective and impartial. Helsinki Principles 5.2.10, 5.3, *supra* note 13, at 513; ANNOTATED SUPPLEMENT, *supra* note 5, ¶¶ 7.7.1-7.7.5; SAN REMO MANUAL, *supra* note 12, ¶¶ 93-104.

69. Hague Convention (XI) Relative to Certain Restrictions with Regard to Exercise of the Right of Capture in Naval War, Oct. 18, 1907, arts. 1-2, 36 Stat. 2396, 2408 (Hague XI). *See also supra* note 63 and accompanying text.

70. Helsinki Principle 3.3, cmt., *supra* note 13, at 505; ANNOTATED SUPPLEMENT, *supra* note 5, ¶¶ 7.8–7.8.1; SAN REMO MANUAL, *supra* note 12, ¶ 108 & cmt. 108.1. Helsinki Principle 3.2, *supra* at 504, declares:

> Neutral ships should be aware of the risk and peril of operating in areas where active naval hostilities take place. Belligerents engaged in naval hostilities must, however, take reasonable precautions including appropriate warnings, if circumstances permit, to avoid damage to neutral ships.

This does not authorize converting a naval operations area into a free-fire zone and does not obliterate the customary rule that belligerents must warn away neutral shipping from operational areas. The Helsinki rule might come into play if there is a chance encounter of belligerent forces.

71. MYRES S. MCDOUGAL & WILLIAM T. BURKE, THE PUBLIC ORDER OF THE OCEANS 753–63 (1962); ANNOTATED SUPPLEMENT, *supra* note 5, ¶ 2.4.3.1; RESTATEMENT (THIRD), *supra* note 18, § 521, cmt. b; John H. Pender, *Jurisdictional Approaches to Maritime Environments: A Space Age Perspective,* 15 JAG JOURNAL 155–58 (1960); US Delegation Paper, UN Conference on the Law of the Sea, *Legality of Using the High Seas in Connection with Nuclear Weapons Tests in the Pacific Ocean,* Doc. No. US/CLS/Pos/48 (2)-(3), Annex II (Feb. 20, 1958), *reprinted in* 4 MARJORIE M. WHITEMAN, DIGEST OF INTERNATIONAL LAW 546, 549 (1968).

72. Helsinki Principle 3.3 & cmt., *supra* note 13, at 504; ANNOTATED SUPPLEMENT, *supra* note 5, ¶ 7.9; SAN REMO MANUAL, *supra* note 12, ¶¶ 105–08; WALKER, *supra* note 1, 403–10; Vaughan Lowe, *The Impact of the Law of the Sea on Naval Warfare,* 14 SYRACUSE JOURNAL OF INTERNATIONAL LAW AND COMMERCE 657, 673 (1988); W.J. Fenrick, *The Exclusion Zone in the Law of Naval Warfare,* 1986 CANADIAN YEARBOOK OF INTERNATIONAL LAW 91, 124–25 (1986). Helsinki Principle 3.2, *supra* note 13, at 504, might come into play if there is a chance encounter of belligerent forces and has no effect on exclusion zone declarations. *See also supra* note 70.

73. *See supra* notes 68, 70, and 72 and accompanying text.

74. Nyon Arrangement, Sept. 14, 1937, ¶¶ 1–4, 181 L.N.T.S. 135, 137-38, amended by Agreement Supplementary to Nyon Arrangement, Sept. 17, 1937, ¶¶ 1-3, *id.* 149, 151 appears to be the first instance of announced high seas defense zones. The belligerents declared them in the 1982 Falklands/Malvinas War; the United States announced them in the 1980–88 Tanker War. *See* O'CONNELL, *supra* note 20, at 80, 168, 172 (1979); WALKER, *supra* note 1, 398–400; L.F.E. Goldie, *Commentary, in* LAW OF NAVAL WARFARE, *supra* note 14, at 489, 493–95; Goldie, *Maritime War Zones and Exclusion Zones, in* Robertson, *supra* note 5, at 156, 192; O'Connell, *International Law and Contemporary Naval Operations,* 44 BRITISH YEARBOOK OF INTERNATIONAL LAW 54–56 (1970).

75. *See supra* note 64 and accompanying text.

76. E.g., Agreement on Prevention of Incidents on & Over the High Seas, May 27, 1972, USSR-US, 23 U.S.T. 1168, 852 U.N.T.S. 151 (INCSEA); Protocol, May 22, 1973, 24 *id.* 1063; *see also* Agreement on Prevention of Dangerous Military Activities, June 12, 1989, USSR-US, T.I.A.S. No. 1485, *reprinted in* 28 I.L.M. 879 (1989). Other countries had INCSEA treaties with the former USSR. Annotated Supplement, *supra* note 5, ¶ 2.8 n.110. These may be subject to treaty succession principles. Symposium, *supra* note 58; Walker, *supra* note 47.

77. E.g., Convention on International Regulations for Preventing Collisions at Sea, Oct. 20, 1972, 28 U.S.T. 3459; International Convention for Safety of Life at Sea, Nov. 1, 1974, 32 *id.* 47, in force for most States with many amendments. *See generally* United States Department of State, Treaties in Force 406–09 (1998) (TIF).

78. The legal basis for an ADIZ is a nation's right to establish reasonable conditions for entry into its territory. AFP 110-31, *supra* note 30, ¶ 2-1g; MYRES MCDOUGAL ET AL., LAW AND PUBLIC ORDER IN SPACE 307–09 (1963); ANNOTATED SUPPLEMENT, *supra* note 5, ¶ 2.5.2.3;

RESTATEMENT (THIRD), *supra* note 18, § 521, r.n.2; NWIP 10-2, *supra* note 60, ¶ 422b; Note, *Air Defense Identification Zones: Creeping Jurisdiction in the Airspace,* 18 VIRGINIA JOURNAL OF INTERNATIONAL LAW 485 (1978). US ADIZs are published in 14 C.F.R. part 99 (1999). *Cf.* Convention on International Civil Aviation (Chicago Convention), Dec. 7, 1944, arts. 3, 8, 11, 61 Stat. 1181–83, 15 U.N.T.S. 298, 300, 304, requiring non-military aircraft to submit to rules for entering another State's territory unless there has been a prior agreement.

79. *See supra* note 45 and accompanying text.

80. UN Charter, art. 103; *see also supra* note 15 and accompanying text.

81. Vienna Convention, *supra* note 20, does not provide for the operation of war, or armed conflict, on international agreements. However, other authorities agree that war may suspend or terminate treaties, depending on the nature of the treaty and the circumstances of the conflict. *See, e.g.,* ILC Report, *supra* note 49, at 267; Institut de Droit International, *The Effects of Armed Conflict on Treaties,* Aug. 28, 1985, arts. 2, 3, 5, 11, 61(2) Annuaire 278, 280–82 (1986); *id., Regulations Regarding the Effect of War on Treaties,* 1912, arts. 1, 4, 7–10, *reprinted in* 7 AMERICAN JOURNAL OF INTERNATIONAL LAW 153–55 (1913); *Clark v. Allen,* 331 U.S. 503, 513 (1947); *Kamuth v. United States,* 79 U.S. 231, 240–42 (1929); *Techt v. Hughes,* 128 N.E. 185, 191 (N.Y.), *cert. denied,* 254 U.S. 643 (1920); 2 OPPENHEIM, *supra* note 5, §§ 99(4)–99(5); Davis, *supra* note 52, at 124–29; Fitzmaurice, *supra* note 52, at 255, 307–17; Harvard Draft Convention on the Law of Treaties, *supra* note 52, art. 35(b), at 662–64; Hurst, *supra* note 52, at 37, 40; Lenoir, *supra* note 52, at 129, 173–77; Walker, *supra* note 47, at 68–71. Impossibility or fundamental change of circumstances claims may overlap war suspension or termination claims. Impossibility, fundamental change, etc. are the only bases for termination or suspension for treaty relations between belligerents and neutrals. Briggs, *supra* note 52, at 89; Lissitzyn, *supra* note 52, at 911; Walker, *supra* note 47, at 68–69.

82. Helsinki Principles 1.4, 3.1, 4, *supra* note 13, at 500, 503, 505; ANNOTATED SUPPLEMENT, *supra* note 5, ¶¶ 8.1-8.1.3; SAN REMO MANUAL, *supra* note 12, ¶¶ 34–42, 44, 46; *see also supra* note 45 and accompanying text.

83. LOS Convention, *supra* note 44, arts. 18–19, 1833 U.N.T.S. at 404; Territorial Sea Convention, *supra* note 58, art. 14, 15 U.S.T. at 1610, 516 U.N.T.S. at 214; Convention on International Civil Aviation (Chicago Convention), Dec. 7, 1944, arts. 1, 3, 61 Stat. 1180, 1181, 15 U.N.T.S. 295, 298; ANNOTATED SUPPLEMENT, *supra* note 5, ¶ 2.3.2.1, at 2–9; 1 O'CONNELL, *supra* note 5, at 118. Maritime Neutrality Convention, *supra* note 30, art. 14, 47 Stat. at 1993; General Declaration, *supra* note 30, ¶¶ 3(a), 3(f), at 605; Hague Air Rules, *supra* note 30, art. 40, at 214; AFP 110–31, *supra* note 30, ¶ 2-6c; Nordic Neutrality Rules, *supra* note 30, art. 8, 188 L.N.T.S. at 301, 309, 315, 321, 329 (air ambulances excepted); ANNOTATED SUPPLEMENT, *supra* note 5, ¶ 7.3.7; 2 OPPENHEIM, *supra* note 5, § 341a; SAN REMO MANUAL, *supra* note 12, ¶ 18. During World War II neutrals prohibited belligerent military aircraft entry. 11 WHITEMAN, *supra* note 5, at 357–58.

84. I.C.J. Statute, art. 38(1); RESTATEMENT (THIRD), *supra* note 18, §§ 102–03.

85. *Compare* Hague Air Rules, *supra* note 30, art. 48, at 215, *with* Hague V, *supra* note 30, art. 10, 36 Stat. at 2324 *and* Hague XIII, *supra* note 30, art. 26, *id.* at 2433 ("unfriendly act").

86. *See supra* note 50 and accompanying text.

87. Today, most commentators say a State cannot invoke a reprisal involving use of force, except when a State is a belligerent and wishes to respond, after request for the offender to comply with the law, with a proportional reprisal against an enemy. *See supra* note 50 and accompanying text.

88. *See supra* note 57 and accompanying text.

89. If a belligerent orders an aircraft from a company or person in neutral territory, the neutral must prescribe a route for the aircraft away from the neighborhood of military operations of the belligerent's opponent and "must exact whatever guarantees may be required to ensure that the

aircraft follows the route prescribed." General Declaration, *supra* note 30, ¶ 3(f), at 605; Hague Air Rules, *supra* note 30, art. 46, at 214.

90. Hague Air Rules, *supra* note 30, art. 47, at 215; *see also* Nordic Neutrality Rules, *supra* note 30, art. 13, 188 L.N.T.S. at 303, 309, 315, 323, 329; Harvard Draft Convention on Rights & Duties of Neutral States in Naval and Aerial War, art. 6, 33 AMERICAN JOURNAL OF INTERNATIONAL LAW 175, 245 (Supp. 1939) (Harvard Draft Neutrality Convention); 2 LEVIE, *supra* note 30, at 827.

91. *Compare* Hague Air Rules, *supra* note 30, art. 30, at 212 *with* AFP 110-31, *supra* note 30, ¶ 2-6b (aircraft entering area of immediate air operations subject to "damages" from hostilities; belligerents cannot deny neutral aircraft access to international airspace even if bound for enemy territory); Annotated Supplement, *supra* note 5, ¶¶ 7.8–7.8.1; San Remo Manual, *supra* note 12, ¶ 108 & cmt. 108.1; *see also supra* note 70 and accompanying text. Helsinki Principle 3.2, *supra* at 504, might come into play if there is a chance encounter of belligerent forces.

92. ANNOTATED SUPPLEMENT, *supra* note 5, ¶ 2.4.3.1; *see also supra* note 71 and accompanying text.

93. ANNOTATED SUPPLEMENT, *supra* note 5, ¶ 7.9; SAN REMO MANUAL, *supra* note 12, ¶¶ 105–08; *see also supra* note 72 and accompanying text.

94. *See supra* note 74 and accompanying text.

95. *See supra* note 78 and accompanying text.

96. *See supra* notes 83, 89 and accompanying text.

97. UN Charter, art. 103; *see also supra* notes 9, 15, 25 and accompanying text.

98. *See supra* note 81 and accompanying text.

99. *See supra* notes 45, 82 and accompanying text.

100. Convention on Registration of Objects Launched into Outer Space, Jan. 14, 1975, 28 *id.* 695, 1023 U.N.T.S. 15 (Registration Convention); Convention on International Liability for Damages Caused by Space Objects, Mar. 29, 1972, 24 *id.* 2389, 961 U.N.T.S. 187 (Liability Convention); Liability Convention; Treaty on Principles Governing Activities in Exploration & Use of Outer Space, Including the Moon & Other Celestial Bodies, Jan. 27, 1967, art. 6-8, 18 U.S.T. 2410, 2415-16, 610 U.N.T.S. 209 (Outer Space Treaty); Agreement on Rescue of Astronauts, Return of Astronauts, & Return of Objects Launched into Outer Space, Apr. 22, 1968, 19 U.S.T. 7570, 672 U.N.T.S. 119 (Rescue & Return Agreement).

101. See *supra* notes 2-53 and accompanying text.

102. 2 O'CONNELL, *supra note* 5, at 1142. Some limited, or localized, wars may have been total war from the belligerents' perspectives, but on a world scale basis, they might be considered local or limited in nature. One recent example is the 1980–88 Iran-Iraq conflict, the maritime aspects of which are examined in WALKER, *supra note* 1, ch. 2.

103. JESSUP, *supra* note 2 at 156 ("There is nothing new about revising neutrality; it has undergone an almost constant process of revision in detail.") *See also supra* notes 2–5 and accompanying text.

104. *See generally ACLU v. Reno*, 929 F. Supp 824, 830–38 (E.D.Pa. 1996)., *aff'd*, 521 U.S. 844, 849–53 (1997); G. BURGESS ALISON, THE LAWYER'S GUIDE TO THE INTERNET (1995); PHILIP BACZEWSKI *ET AL.*, THE INTERNET UNLEASHED (1994); KATIE HAFNER & MATTHEW LYON, WHERE WIZARDS STAY UP LATE: THE ORIGINS OF THE INTERNET (1996); George Johnson, *From Two Small Nodes, a Mighty Web Has Grown,* NEW YORK TIMES, Oct. 12, 1999, at D1; for historical analyses of the development of computers and the Internet. As World War ll ended, Vannevar Bush suggested the basic idea of a personal computer; he traced the history of calculators, discussed speech-controlled typewriters, and advocated document storage on super fine grain microfilm shuffled by mechanical fingers. Bush believed that new logic and new symbolism would be necessary. Although he missed the idea of electronic communication, much of what Bush wrote in this perspective, futuristic article has become reality, albeit in different

modalities. Vannevar Bush, *As We May Think*, 176 ATLANTIC MONTHLY 101 (July 1945); Johnson, *supra*. Mechanical computers were used aboard warships before World War II to supply fire control solutions to naval guns through electrical circuits. Although most firing corrections on these computers were made aboard ship by telephone communications among gunners and fire control personnel who operated visual or radar-assisted gun directors and ship's combat information centers (i.e., a room aboard ship where radar repeaters portrayed shell splashes), shore bombardment effects and recommendations for corrections sometimes came by radio communications between ships and shore spotters, e.g., Army or Marine Corps forward artillery observers on the ground or in aircraft. The ship's computer "stored" prior information that had been inserted and retained this information until it was changed by operators. Information might be relayed through internal ship communications, perhaps to other computers aboard ship, but there was no data transfer among external computers, i.e., those on other vessels. Antisubmarine warfare systems, shipboard torpedo attack systems, and submarine fire control systems for torpedo attack employed similar fire control solutions, using electronics-based systems (e.g., sonar, radar) and mechanical devices operated in similar fashion, but there was little, if any, information exchange between an attacking ship and other stations. These systems operate in similar fashion today, although electronics-based computers have replaced mechanical systems, and missiles have replaced gun projectiles in many cases.

105. "When the legal community first considered the . . . . regime that governed state activities and military operations in Cyber Space, some U.S. government attorneys stated rather boldly that (applying) modern information systems technology to military purposes was so new that *no* law applied." SHARP, *supra* note 5, at 5. A policy behind this approach is national sovereignty. See UN Charter, art 2(1); *S.S. Lotus* (Fr. V. Turk), 1927 PC. I.J., Ser. A, No. 10, at 4,18.

106. *Cf.* I.C.J. Statute, Art 38(1); RESTATEMENT (THIRD) *supra* note 18, at 102–03.

107. *E.g.* Office of General Counsel, Department of Defense, An Assessment of International Legal Issues in Information Operations (Nov. 1999). The paper is appended to this volume as the Appendix. *See also* GREENBERG, *supra* note 50, at 17; SHARP, *supra* note 5, at 5.

108. UN Charter, arts. 2(4), 25, 48, 51, 103; see *also supra* notes 2–44 and accompanying test.

109. *See, e.g.,* International Convention on Civil & Political Right, Dec. 16, 1966, arts. 4, 19(3)(b) (derogation clauses), 17 (forbidding interference with correspondence), 19 (freedom of expression), 999 U.N.T.S. 171, 174, 177, 178; European Convention for Protection of Human Rights & Fundamental Freedoms, Nov. 4, 1950, arts. 6(1), 8(2), 10(2) (derogation clauses), 8(1) (correspondence), 10 (right of free expression regardless of frontiers), 213 *id.* 221, 228, 230; American Convention on Human Rights, Nov. 22, 1969, art. 13(2)(b), 27 (derogation clauses), 13 (freedom of expression regardless of frontiers), 14 (right of reply), 9 I.L.M. 673, 679–80, 683 (1970). Banjul (African) Charter on Human & Peoples' Rights, June 27, 1981, art. 9 (rights to receive information, disseminate opinions within the law), 21 *id.* 58, 60 (1982) has no derogation clause; it would be subject, however, to the usual law of treaties principles on impossibility of performance, etc. *See also* SUBATRA ROY CHOWDHURY, RULE OF LAW IN A STATE OF EMERGENCY 12–13, 22–29, 59, 121–25, 210–11(1989) (analyzing International Law Association Minimum Standards of Human Rights Norms in a State of Emergency (1984)); MYRES S. MCDOUGAL ET AL., HUMAN RIGHTS AND WORLD PUBLIC ORDER 813–15 (1980); Joan Fitzpatrick, *Protection against Abuse of the "Concept of Emergency," in* HUMAN RIGHTS: AN AGENDA FOR THE NEXT CENTURY 203 (AMERICAN SOCIETY OF INTERNATIONAL LAW STUDIES IN TRANSNATIONAL POLICY., LOUIS HENKIN & JOHN LAWRENCE HARGROVE EDS. 1994); HENKIN, *International Human Rights as "Rights"* 1 CARDOZO LAW REVIEW 446–47 (1979); Universal Declaration of Human Rights, Dec. 10, 1948, arts. 12, 19, 27 U.N.G.A. Res. 217 (1948), *reprinted in* DIETRICH RAUSCHNING ET AL., KEY RESOLUTIONS OF THE UNITED NATIONS GENERAL ASSEMBLY 1946–1996, at 321–22 (1997). *Nuclear Weapons,* 1996 I.C.J. 226, at 239–40, observed that "the protection of the (Civil & Political Rights Covenant) does not cease

in times of war, except by operation of Article 4 of the Covenant whereby certain provisions may be derogated from in a time of national emergency. Respect for the right to life is not such a provision. . . .[T]he right not arbitrarily to be deprived of one's life applies also during hostilities. . . .[W]hat is an arbitrary deprivation of life . . . then falls to be determined by the applicable *lex specialis* . . . the [LOAC] . . . designed to regulate the conduct of hostilities. Thus whether a particular loss of life, through use of a certain weapon in warfare, is to be considered an arbitrary deprivation of life contrary to . . . the Covenant, can only be decided by . . . the [LOAC] and not . . . . from the terms of the Covenant." To the extent that human rights treaty norms represent custom, law of treaties analysis does not apply. However, derogations from custom like the persistent objector rule do, and will apply to Declaration norms having status as custom. "The United States has long denied that any obligation rests upon it when a neutral to attempt to control expressions of opinion by private persons within its territory and adverse to the cause of any belligerent," although the US Government has appealed to its citizenry to refrain from partisanship during war. 3 HYDE, *supra* note 5, § 874.

110. These might be applied through the analogy of the due regard principle, taken from the LOS and applied during armed conflict by analogy. *See supra* note 79 and accompanying text.

111. *See supra* note 30 and accompanying text.

112. *See supra* notes 57, 58 and accompanying text.

113. *See supra* note 33 and accompanying text.

114. Outer space also has this characteristic, but beyond the Charter and general principles applicable to any situation, there is little law from which analogies for neutrality law in the IW context might be drawn. *See supra* notes 96–100 and accompanying text.

115. *See supra* notes 44–79 and accompanying text.

116. *See, e.g., supra* notes 68, 70–72, 78, 89, 91–93 and accompanying text.

117. Myres S. McDougal, *The Hydrogen Bomb Tests and the International Law of the Sea*, 49 AMERICAN JOURNAL OF INTERNATIONAL LAW 356–58 (1955).

118. *See supra* note 64 and accompanying text. The law for dropping projectiles from balloons comes to mind. *See* Declaration Prohibiting Discharge of Projectiles & Explosives from Balloons, Oct. 17, 1907, 36 Stat. 2439, still in force for 28 countries including the United States, and perhaps more if treaty succession principles are taken into account. *See* TIF, *supra* note 15, at 450; Symposium, *supra* note 58; Walker, *supra* note 47.

119. I.C.J. Statute, art. 38(1); RESTATEMENT (THIRD), *supra* note 20 §§ 102–03; *see also supra* notes 18–19 and accompanying text.

XIV

Information Operations in the Space Law Arena: Science Fiction Becomes Reality

Douglas S. Anderson and Christopher R. Dooley*

The most likely way for the world to be destroyed, most experts agree, is by accident. That's where we come in; we're computer professionals. We cause accidents.[1]

War fighting has come a long way from the days of swords and shields. No longer must armed forces rely completely on "arms," or even "forces," to gain victory on the battlefield. Today, computers are becoming the weapon of choice for the military warrior. Forget the old standbys of the M-16, Abrams tank, Nimitz-class carrier, or F-16. As forces become more computer and technologically dependent, militaries of the future will have a completely different look.[2] In some respects, this should not surprise us. Technological change has always transformed the means and methods of warfare, but the *pace* of transformation has increased dramatically in the past few decades. While laptops and cyber chips may never completely displace guns and bullets in the warfighter's arsenal, they certainly will become an increasingly critical part.

Nowhere is this technological transformation more evident than in the areas of military space resources and information operations. Lasers, electronic pulses, pinpoint sensing equipment, and a vast array of other sophisticated space systems

are becoming an ordinary part of our day-to-day military experience. As the latest microchip and computer network capabilities become an integral part of attacking and defending those space systems, the future will be fraught with dramatic new possibilities. Yesterday's science fiction is becoming today's reality.

Background

This new reality is already a significant threat to the US national security infrastructure. Consider the evidence. According to former Deputy Defense Secretary John Hamre, one particular Department of Defense (DoD) computer network is penetrated as often as 10-15 times a day by computer hackers.[3] With more than 2.1 million computers and 10,000 local area networks, DoD was the target of more than 250,000 *detected* intrusions in 1998.[4] That figure is even more astounding when you consider that the Defense Information Systems Agency (DISA) estimates that only one intrusion out of every 150 is even detected.[5] In February 1998, while the US was preparing to deploy forces to the Persian Gulf, a computer attack known as "Solar Sunrise" was initiated against computer systems throughout the Department of Defense.[6] The potential implications of the attack were sobering:

> Someone, or some group of people . . . gained root access, systems administrator status, on over 20 important logistical computers throughout the Air Force and, subsequently, we learned throughout the Navy and Army. They could have therefore crashed the systems. They downloaded thousands of passwords and they installed sniffers and trap doors. And for days, critical days, as we were trying to get forces to the Gulf, we didn't know who was doing it. We assumed therefore it was Iraq. We found out it was two 14-year-olds from San Francisco. Was that good news or bad? If two 14-year-olds could do that, think about what a determined foe could do.[7]

"Eligible Receiver" was a cyber attack exercise in June 1997, which was launched by the Department of Defense against itself to see how well our systems detected and responded to the attack. For days, the attack went undetected. This exercise demonstrated the ability of a potential enemy to disrupt computer operations of major military commands, create large-scale blackouts, and interrupt emergency phone service in Washington, DC.[8] These types of cyberspace intrusions are not limited to the domain of criminals or terrorist hackers. States have been, and will continue to be, engaged in the use of information

operations. They recognize, as does the US, its value in protecting national security interests.[9] There have been reports that during the NATO-led Operation ALLIED FORCE campaign against Serbia, Serbs hacked into the NATO World Wide Web pages and flooded e-mail accounts in the US with pro-Serb messages.[10] The reported Serbian actions, and others like them, demonstrate that the threat of cyber attack is real. Both the White House and DoD are certainly convinced. In response to the threat against DoD communications systems and other government computer data, the Clinton Administration issued a White Paper in May 1998 setting forth policy and goals on critical infrastructure protection.[11] In addition, the DoD created the Joint Task Force - Computer Network Defense[12] (JTF-CND), which maintains a 24-hour operations center to provide warnings of cyber attacks on DoD systems.[13]

Couple the dangers of cyber attacks with our heavy reliance on space systems and the threat becomes all the more sobering. It is more than just an axiom that outer space is the proverbial high ground.[14] Access to, and control of, outer space are fundamental to our nation's economic and military security.[15] Moreover, we can no longer take that access and control for granted. While the US dominates outer space activity today, it is estimated that within the next 10 to 20 years more space-based systems will be available to friendly and unfriendly nations alike.[16] These systems will provide communications, weather, surveillance, and a host of other critical services that will have both a military and civilian use. Friends and foes will be able to use the same space systems.[17] Therein lies one of the dangers.

Modern military forces rely heavily on dual-use telecommunications media, including telephones, faxes, and e-mail that travel over civilian owned or operated networks. In fact, 95 percent of all DoD telecommunications traffic flows over public networks.[18] Telecommunications are a particularly acute vulnerability because of this high degree of dependence by modern militaries.[19] This reliance permeates every facet of society, thus allowing exploitation throughout the conflict spectrum at the tactical, operational, and strategic levels.[20] Because of their data transfer capacity and mobility, telecommunications are increasingly important as the critical media by which our national instruments of power are directed.[21]

The threats are real, the vulnerabilities potentially grave, and new computer technology is largely responsible. Information operations and outer space operations are uniquely intertwined through their mutual reliance on, and vulnerability to, computer technology. Moreover, that technology is changing rapidly. From a military operation or infrastructure protection perspective, it is difficult to keep pace with such rapid developments. Equally daunting is the effort to

apply existing legal regimes to these new technologies. Both information operations and space operations apply military force in a way that challenges traditional international legal norms. Admittedly, such a topic raises far more issues than can be adequately addressed here. Therefore, this chapter is intended only as a basic primer to introduce the reader to the international law applicable to information operations that affect military space systems.

Scope and Definition of the Information Operations Concept

It is readily apparent how wide-ranging the computer attack threat to our national security infrastructure can be. It can include activities such as offensive and defensive electronic jamming, information denial, manipulation of data, morphing of video transmissions, destruction of hardware, or a myriad of other techniques to render military weapons and systems ineffective, inoperable, or unavailable at a critical time. In the legal context, information operations—including threats by individuals, organizations, or nations; actions motivated by goals ranging from monetary greed to terrorist revenge; and operations with military objectives—touch both international and domestic law.

For our purposes, discussion of information operations is limited to actions by, or on behalf of, nation States. Moreover, domestic laws and regulations are not our focus, although there are certainly many regulations that apply.[22] Instead, we examine those aspects of public international law relating to outer space that may have an impact on information operations.

As a starting point, it is necessary to define terms, since "information operations" is not a term of art with a universally agreed upon meaning. Indeed, the US military services, and the DoD itself, do not use consistent terminology. For example, in the glossary of Doctrine Document 2-5, the Air Force adopts the DoD definition of "information operations" found in DoD Directive 3600.1: "actions taken to affect adversary information and information systems while defending one's own information and information systems."[23] Yet the Air Force takes the unusual step of qualifying that definition with what it calls "a more useful working definition," namely, "[t]hose actions taken to gain, exploit, defend or attack information and information systems and include both *information-in-warfare* and *information warfare* (emphasis added)."[24] Even though the Air Force and DoD definitions emphasize different aspects of information operations, their concepts, as well as that of the other military services, include both offensive and defensive operations. While we use the term "information operations" in a very broad sense that includes attacking or

defending information and information systems, for the purpose of this chapter we place particular emphasis on computers as the primary means of doing so.

The Importance of IO to Military Operations

The electron may well be the ultimate precision guided weapon,[25] for information is becoming a strategic resource that could prove as valuable and influential in the post-industrial era as capital and labor were in the industrial age.[26] Use of the term "information operations" signifies a new way of thinking that recognizes the central importance of modern information systems as force enhancers, as vitally important targets, as a means of defense, and as cyberweapons that may be used to attack certain targets.[27]

> While both netwar and cyberwar[28] revolve around information communications matters, at a deeper level they are forms of war about "knowledge"—about who knows what, when, where, and why, and about how secure a society or a military is regarding its knowledge of itself and its adversaries.
>
> Netwar refers to information-related conflict at a grand [strategic] level between nations or societies. It means trying to disrupt, damage or modify what a target population "knows" or thinks it knows about itself and the world around it. It may involve public diplomacy measures, propaganda and psychological campaigns, political and cultural subversion, deception of or interference with local media, and efforts to promote a dissident or opposition movement across computer networks.[29]

Daniel Kuehl, Professor of Military Strategy at the National Defense University's School of Information Warfare and Strategy, notes that information warfare is intended to "influence the enemy's will and ability to fight so that they stop fighting and you win."[30]

> Information is aimed at affecting the enemy's cognitive and technical abilities to use information while protecting our own—to control and exploit the information environment. In some ways it is technologically independent in that operations can be conducted in any of the media of war, not just cyberspace, to attain that key objective of weakening the enemy's will, but in other ways the new medium of cyberspace offers a particularly rich environment through which we can reach those elusive targets, the enemy's will and capability, via the various

> entry ways and connecting points in the information environment, whether they be hardware, software, or wetware [the human mind].[31]

The objective of offensive warfare has always been to deny, destroy, disrupt, or deceive the enemy—either in its employment of forces or in retaining the support of its people.[32] Mao Tse-Tung believed that "to win victory we must try our best to seal the eyes and ears of the enemy, making him blind and deaf, and to create confusion in the minds of the enemy commanders."[33] Information operations are particularly well suited to sealing the eyes and ears of the enemy. By disrupting or denying the flow of information between the enemy's military forces and its command and control elements, information operations can essentially render sightless any enemy commander.[34]

The Importance of Space Systems to Military Operations

Space denial is an important tenet of our national defense strategy.[35] Inherent in that tenet is the recognition that control of outer space is essential for victory on today's battlefield. Certainly, space power has evolved over the last ten years from merely being a useful force multiplier to being no less than an "indispensable adjunct."[36] According to one author, "the contemporary reality is that the US armed forces could not prevail, even against a modestly competent foe, without the support of space systems."[37] Air Force Chief of Staff General Michael E. Ryan gives an excellent example of the practical use of space assets in a deployed environment.

> When a U-2 reconnaissance aircraft goes on a mission, the planes can send raw surveillance data via satellite to intelligence specialists in the United States, who can analyze it and send it to Operation Allied Force's Combined Air Operations Center at Vicenza, Italy. The data can then be sent to a pilot flying a strike mission. All this can be done within minutes and reduces the number of airmen who have to deploy.[38]

During Operation ALLIED FORCE in the Balkans, a variety of space assets were used to support the NATO effort. According to Brigadier General Mike Drennan, Commander of the 21st Space Wing at Peterson Air Force Base, Colorado, navigation, strike indicators, search and rescue, communications, and weather images represented just some of the space systems support provided to commanders in the theater.[39] Additionally, both conventional air-launched cruise missiles and Tomahawk land-attack missiles launched from ships, as well as certain other precision guided weapons, owed their success to the Global

Positioning System (GPS).[40] While GPS was designed by the Department of Defense as a dual-use system, its primary purpose has been to enhance the effectiveness of US and coalition military forces.

Our national space policy expressly recognizes that US national security is dependent upon an ability to maintain access to, and use of, space.[41] At times, our national security interests may require denial of space to our adversaries. Information operations can play a key role in space control and denial. For instance, intrusions into an adversary's computer network and manipulation of key data can prevent a space launch, move an opponent's communications or remote sensing satellites out of orbit, or preclude satellite data from reaching command and control centers.

World Wide Availability of Space Data Information

One of the realities of space denial and space control objectives within our national space policies and military doctrine is that the US does not, and will not, have exclusive access to space. A growing number of nations and organizations are obtaining space assets and systems of their own.[42] China has a rapidly developing space program, as does Japan, India, Brazil, and, of course, Russia.[43] France, India, and Israel have capabilities in high-resolution satellite surveillance technology, and this type of data is now commercially available for purchase by any nation.[44] The US Landsat and the French SPOT [*Systeme Pour l'Observation de la Terre*] imaging systems have been around for years, but their technology continues to improve and become more widely available.[45] For instance, the French are currently marketing ten-meter resolution images, while some commercial satellites are now capable of one-meter resolutions.[46] More recently, the European Space Agency has developed Earth Resources Satellites (ERS) 1 and 2, and marketed their synthetic aperture radar (SAR) images. Canadian Radarsat and the Helios reconnaissance satellite owned by France, Spain, and Italy may also have future commercial availability.[47] A further example of the public commercial availability of space system technology is the US' hugely successful GPS, which, until recently, enjoyed a near monopoly in space-based navigation technology. Besides the availability of GPS, Europe is planning to launch its own satellite navigation system called Galileo, projected to be operational in 2008.

As non-US satellite navigation systems are developed and launched, additional legal issues and national security concerns arise. When a virtual US monopoly on particular space systems exists, such as there used to be with GPS, space denial or control is merely a matter of interrupting or encoding the information from our own systems so that other nations are unable to use it.[48]

However, when other nations have similar space systems, or can purchase the information they produce, space denial or control may require more aggressive means of information operations. The commercial availability of potentially sensitive data creates obvious risks to national security. According to one analyst, "Islamic Jihad could get its hands on a one-meter resolution picture of a US Air Force General's headquarters in Turkey, convert the shot to a precise three-dimensional image, combine it with data from a GPS device, and transmit it to Baghdad, where a primitive cruise missile, purchased secretly from China could await its targeting coordinates."[49]

Information operations, used to assure US space control by denying its use by others, will certainly raise eyebrows and stir heated debate in the international community. Since any decision to employ a military option, especially one affecting outer space or space systems, must weigh political concerns and sensitivities, a consideration of world opinion on the subject is useful.

International Opinion on the Weaponization of Space

Since the Soviet launch of Sputnik in 1957, many nations in the world community have been ardently concerned about preventing the placement of weapons in outer space, particularly with respect to new weapons technology. As a result, any potential use of offensive information operations in, or affecting, outer space will likely aggravate international concerns.

The debate has been polarizing, frequently pitting practical national security objectives against the desire to maintain at least one environmental realm free from military conflict. Early UN General Assembly resolutions generally sought to provide that outer space would be used exclusively for "peaceful purposes," but the term was never defined.[50] While nearly all voices claimed to be in favor of peaceful purposes, they were not so harmonious on the degree of military activity that concept included. The reality, of course, is that outer space has been a domain of the military since 1957 and has been of significant importance to the military to the present day. Today, some advocates of the non-weaponization of space seek to impede further military development of space with the ultimate hope of curtailing an arms race in outer space. While opponents of this view are not against "peaceful purposes" per se, they stress the need to be prepared for war as the best way to protect national interests.[51] In general, the two views are irreconcilable, although there is room for agreement on specific issues.

The United Nations, which includes members on both sides of the debate, has taken an active role in international space law from the very inception of the

space age. It has done so primarily through the work of the Committee on the Peaceful Uses of Outer Space (COPUOS).

Committee on the Peaceful Uses of Outer Space

In 1959, the United Nations established COPUOS[52] to enhance international cooperation in the peaceful uses of outer space. Since its creation, it has been the primary forum for the development of international space law. In fact, COPUOS was the architect for each of the existing five space law treaties. Of those, four have been ratified by most space-faring nations; together, they comprise the core body of international space law.[53]

From its inception, COPUOS has promoted the use and maintenance of outer space for peaceful purposes. Early work resulted in the adoption of General Assembly Resolution 1721 on December 20, 1961, which stated that "the common interest of mankind is furthered by the peaceful uses of outer space."[54] General Assembly Resolutions 1884 and 1962, adopted two years later, continued that theme.[55] Today, the Committee continues to encourage research and distribution of information on outer space matters, sponsor various programs and conferences, and study the legal issues arising out of space exploration and activity.[56]

As its name implies and its work confirms, COPUOS starts from the premise that outer space should be maintained for "peaceful uses." While this is a term that everyone has adopted, as noted earlier, there is strong disagreement about its meaning. Past practice has demonstrated that most COPUOS members believe military activity in outer space, as potentially contrary to the goals of international peace and security, must be closely scrutinized. In fact, at its fifty-first session, the UN General Assembly passed Resolution 51/44, "Prevention of an arms race in outer space." Included in that resolution was the statement that the General Assembly recognizes "that prevention of an arms race in outer space would avert a grave danger for international peace and security."[57] Other General Assembly resolutions contain similar language.[58]

The large number of early space treaties and General Assembly resolutions would ordinarily reflect a committee that works well together. However, that has not been the case with COPUOS. Its early success in obtaining the first four treaties was due largely to the fact that compromises on space issues were easier to obtain before the full potential of space exploration had been fully understood.[59] However, fundamental rifts soon developed within COPUOS, and have continued, between space and non-space powers.[60] More recently, the United States has found itself on the minority side of several General Assembly resolutions intended to de-militarize outer space.

From the perspective of the UN Charter, these resolutions are merely non-binding recommendations.[61] However, some commentators have asserted that the "peaceful use" of outer space concept reflects customary international law,[62] and, to the extent it is referenced, therefore believe the General Assembly resolutions contain legally binding principles.[63] This argument is not particularly helpful since it does not address the meaning of the peaceful use concept. A more practical concern about these resolutions is whether the underlying viewpoint will ultimately lead to the development of another space law treaty which significantly limits military activity, including information operations, in or transiting outer space.

Conference on Disarmament

Closely related to COPUOS is the Conference on Disarmament (CD). Also a creation of the United Nations, it was established in 1979 as the single multilateral disarmament negotiating forum of the UN. The CD has grown from its original membership of 40 nations to 66, including the United States.[64] As with COPUOS, disagreements between CD members exist. These differences were clearly evident in 1985 when an Ad Hoc Committee, formed to find a means to curtail the arms race in space, held 20 meetings over a three-month period without reaching agreement on any of their objectives.[65] The primary catalyst in forming the Ad Hoc Committee was the US "Strategic Defense Initiative" program.[66] In debating a proposal for an arms control treaty for space, the United States argued that there was no need for such a treaty since existing treaties were sufficient. In contrast, the former socialist block nations indicated a willingness to conclude an agreement that would not only prohibit space attack weapons then under development, but would also require the destruction of existing weapons. While the Soviet Union accused the United States of "disrupting" and "hampering" the ratification of several important arms control agreements, China's tone was at least as emphatic. China made it clear that "the 'Star Wars' plan must not be carried out" and that "China is firmly opposed to an arms race in outer space . . . and proposes to achieve first 'the de-weaponization of outer space' at the present stage."[67] The nonaligned and neutral States consistently supported the idea that space weapons must be prevented in outer space at all costs.[68]

A more recent example of this split of opinion is found in General Assembly Resolution A/52/37, passed in 1997. That resolution called on the CD to re-examine the idea of establishing another Ad Hoc Committee to address the issue of militarization of space. This issue had re-captured the interest of the CD

in light of recent developments in lasers and perceptions that the US was seeking to weaken the Anti-Ballistic Missile (ABM) Treaty.[69] Despite the efforts and objections of the US, the resolution was supported by 128 nations, including China, Russia, Canada, Japan, Australia, and New Zealand. The US, Great Britain, and France were among the 39 abstentions.[70] Even more recently, another General Assembly resolution called for the CD to reestablish the prior Ad Hoc Committee on the Prevention of an Arms Race in Outer Space. Adopted on December 4, 1998, by an overwhelming vote of 165 to 0, the US was one of four abstentions.[71]

China has been particularly active in the CD in its efforts to keep outer space weapon-free. In addition to co-sponsoring several UN General Assembly resolutions, it has also sought to obtain a legally binding international agreement to ensure outer space remains free of all weapons. In fact, China published a White Paper in July 1998 to outline its views on the weaponization of outer space.[72] According to this paper, "China stands for the complete prohibition and thorough destruction of weapons deployed in outer space."[73] Additionally, it seeks a "ban on the use of force or conduct of hostilities in, from, or to outer space." China also wants to preclude all countries from experimenting with any space weapons systems that would provide strategic advantages on the ground.[74] While its latest White Paper does not refer to information operations, the principles outlined therein seem to imply that China would oppose the use of information operations that could be seen as a "use of force," the "conduct of hostilities," or as "a weapon of any kind" in outer space. Despite this strong language, it is not surprising to read China's most recent statements, which express an intention not only to use information operations for military purposes, but to extend their use into space.[75]

During its 1998 session, the CD included in its agenda the frequently revisited topic of the "prevention of an arms race in outer space."[76] During that session, Canada proposed that the CD create an Ad Hoc Committee, referred to earlier, with the mandate to negotiate a convention for the non-weaponization of outer space.[77] The Canadian proposal makes two important admissions. First, it recognizes that currently there is no multilateral international agreement that prohibits the deployment of weapons in outer space other than weapons of mass destruction. This recognition is consistent with the longstanding US position. Even more important, however, is the statement that "[w]e acknowledge that there is currently no arms race in outer space. We accept the current military uses of outer space for surveillance, intelligence-gathering and communications."[78] Despite these two major concessions, it is nonetheless clear that much of the world disagrees with current US national and DoD space policy to the extent that it does not expressly denounce the weaponization of outer space.

US and DoD Space Policies

The Clinton Administration announced the latest version of the National Space Policy on September 19, 1996.[79] The National Security Space Guidelines include the principle that the US will conduct its space activities in a way that assures hostile forces cannot deny our use of space and preserves our ability to conduct both military and intelligence space-related activities. This makes some in the international community uneasy.[80] The National Space Policy also makes clear what has been obvious for quite some time—that access to and use of space "is central for preserving peace and protecting US national security."[81]

In terms of information operations, nothing in our current policy prohibits or even limits use of such technology to support our space security guidelines. In fact, it obligates the DoD to "protect critical space-related technologies and mission aspects,"[82] and maintain the capabilities to execute traditional mission areas of space support, force enhancement, space control, and force application.[83] The use of information operations to protect our communication systems and data links, while being able to interfere with the communications and data of adversaries, is wholly consistent with National Space Policy guidelines.

Assurance of space access by the US is also included in the Department of Defense's new space policy set forth in DoD Directive 3100.10.[84] Announced on July 9, 1999, this policy not only echoes the guidance of the National Space Policy, it also specifically refers to the need to maintain "information superiority."[85] Moreover, the wide variety of information operations that could be used to defend against attacks upon our space systems and to assure space control is consistent with it.

Recalling the position of many nations involved in COPUOS and the CD, many of the US national and Department of Defense space policy statements may run counter to the concept of de-militarizing space.[86] Perhaps most significantly, the first sentence of the DoD policy unequivocally announces that "space is a medium like the land, sea, and air within which military activities shall be conducted."[87] Many nations represented in COPUOS and the CD do not view outer space as analogous to "the land, sea or air," but rather more like Antarctica, where they have expended much effort to exclude nearly all military activities.

When the statements of scholars and politicians from other nations are compared generally to those in the US, a clear difference of opinion regarding the proper role of the military in space, including the use of information operations, emerges. While information operations may or may not be consistent with international opinion, they are consistent with both the national and

DoD space policies. Having considered world opinion on the issue, we turn to the applicable international law as it relates to information operations in or transiting space.

Overview of Space Law Applicable to Information Operations

There currently exist no "thou shalt nots" in space law which specifically refer to the term or concept of "information operations." In fact, there are very few *specific* military activities of any kind that are restricted or prohibited.[88] For instance, one will not find among the current space law treaties any specific reference to space lasers, anti-satellite weapons, kinetic energy guns, or information operations. For the most part, when examining space law provisions, a legal practitioner needs to work with general principles that must be applied on a fact-specific basis. Therefore, we will focus on those laws having a general application to the concept of information operations and then apply them to specific scenarios.

One means of using information operations to protect our national security interests in space is by controlling our adversaries' access to information through techniques that will interrupt, interfere with, or deny critical satellite data. At times, this can be particularly sensitive since denying data to an adversary that does not own its own space system may require disrupting a third party's space system. This, in turn, may disrupt access to data for other users who may not be involved in the conflict with the US. Using information operations for such a purpose requires careful consideration of the law as well as national policy and security interests.

US Policy on GPS Data Interference

One such national policy relates to the use of US GPS data. GPS data can be accessed in two ways. The first is through the normal operation mode of the standard positioning service (SPS). This method allows access by all users, but it also enables the US to downgrade the data provided to certain users through use of various degradation technologies and cryptography. The second means of access is the GPS Precision Positioning Service (PPS), which is granted only to DoD users and enables them to receive a clear signal with properly encrypted GPS receivers. Thus, the US military could seek to intentionally impair the navigational signals released by its global navigation system in the SPS mode to protect national security interests.[89] Such interference would only temporarily prevent commercial users and others from obtaining the same quality of

information the US needs for its military operations. It would also be preceded by a public notice warning other users of the intentionally impaired signals. Since this particular GPS belongs exclusively to the US, the United States can set appropriate limits on its use by third parties.

However, on March 29, 1996, the Clinton Administration announced a new national policy that would eventually remove prior military restrictions on the management and use of the US-owned GPS. As part of that new policy, the US committed itself to "discontinue the use of GPS Selective Availability (SA) within a decade in a manner that allows adequate time and resources for our military forces to prepare fully for operations without SA."[90] The policy also stated that GPS would be provided free of charge to the rest of the world for peaceful uses on a continuous basis.

This current policy should not unduly limit DoD information operations activities designed to impair or interrupt US GPS signals when necessary. By its terms, the policy allows the US to continue selective availability measures until alternative measures allow military forces to operate without them, even if the data is used for peaceful civil, commercial, and scientific purposes. Secondly, the policy directs the DoD to develop measures to prevent the hostile use of GPS,[91] including defensive information operation measures. Finally, in the case of actual armed conflict, this internally imposed policy decision would not preclude military use of information operations to affect an adversary's ability to use the GPS system, if deemed necessary for national security purposes.

United Nations Treaties and Pronouncements

1. Outer Space Treaty

Although it was not the first international agreement to refer specifically to outer space,[92] the Outer Space Treaty which entered into force on October 10, 1967, [93] has become the cornerstone multilateral agreement dealing with the use of space. Frequently described as the "Magna Carta" of outer space,[94] its significance cannot be over emphasized. It provides the basic framework of international space law, incorporated many of the principles set forth earlier in the non-binding 1963 Declaration of Principles,[95] has been the basis of subsequent space law treaties, and contains several provisions that have general application to information operations.

Article I(1) obligates parties to use outer space "for the benefit and in the interest of all countries" and provides that it is "the province of all mankind." Some scholars have asserted that this language means that States cannot encroach upon, or interfere with, the lawful activities of other States.[96] This language does not, however, impose any legal constraints on military operations properly authorized

under international law. For example, military action pursuant to a Chapter VII Security Council resolution is, of course, an authorized activity for the benefit and in the interest of all countries, given the UN's authority to use force to protect international peace and security.

Article I(2) expands on the use limitations of the first paragraph, stating that outer space shall be "free for exploration and use by all States without discrimination of any kind." This language affirms the principle of free access to space and prohibits interference with that access.[97] The language of paragraph two also contains an important condition that the use of outer space be "in accordance with international law." Thus, if the military action is otherwise lawful, the fact it is conducted in outer space or through information operations does not violate this provision.

Closely related to the freedom of access principle is the non-appropriation principle contained in Article II, which provides that outer space "is not subject to national appropriation by claim of sovereignty." While this language might suggest that information operations used to interfere with satellite signals or data are an act of unlawful appropriation of another State's space system, that view goes too far. Interference with a sovereign object is not the same as asserting a sovereign interest over outer space should that object be located there. Only the latter would violate the non-appropriation principle of Article II. The Law of the Sea Convention has similar language regarding claims over the high seas,[98] but it clearly has allowed use of the high seas by military warships (sovereign objects) without recognizing that interference with them constituted a claim of national appropriation over the high seas. Absent a claim of sovereignty over the high seas, interference with warships on the high seas has not been deemed equivalent to an unlawful appropriation. In both cases, what is prohibited is the assertion of territorial claims.[99]

Another potential limitation on information operations is contained in Article IV. This article contains the key provisions relating to military activity in space. Paragraph 1 prohibits nations from orbiting, installing on celestial bodies, or stationing in outer space any nuclear weapons or "any other weapons of mass destruction." The meaning of the term "weapons of mass destruction" (WMD) has "typically been defined as weapons that are intended to have indiscriminate effect upon large populations and large geographical areas."[100] It is generally accepted to include nuclear, chemical, and biological weapons.[101] Even though WMD could also include other weapons, notwithstanding the Russian position statement to the contrary,[102] the use of an information weapon is not likely to be viewed by the US as a weapon of mass destruction.[103] Ordinarily, its effects can be controlled so as not to destroy large numbers of people. For example, the

selective disabling by information operations of a particular computer system does not come within the meaning of WMD in Article IV.

For the most part, Article IV, paragraph 2, deals with the moon and other celestial bodies. Among other restrictions, it states that, "[t]he moon and other celestial bodies shall be used by all States Parties to the Treaty *exclusively for peaceful purposes.*" It also states that "[t]he use of military personnel for scientific research or *for any other peaceful purposes* shall not be prohibited." Despite the fact that the "peaceful purposes" language does not expressly refer to the domain of outer space, historically the US and other nations have generally agreed that activities in outer space should also be confined to peaceful purposes.[104] Nonetheless, it has been the US view that the peaceful purpose language does not preclude lawful military activity.[105] While this conclusion seems clear, determining which military activities in outer space are considered "peaceful"[106] has been a topic of contentious debate. Indeed, from the moment the Outer Space Treaty was drafted, the international community has been divided on this issue.[107]

Advocates for the position that the "peaceful purposes" language excludes all military activity other than scientific research often cite to similar language in the Antarctic Treaty of 1959[108] and the conforming practice of nations in Antarctica. However, such a comparison is both misleading and inappropriate. Article 1, paragraph 1 of that treaty states that "Antarctica shall be used for peaceful purposes only." While this portion of the treaty is similar to the "exclusively for peaceful purposes" language of the Outer Space Treaty, the analysis is inapt. What many of these advocates fail to mention is *additional language* that is not found in the Outer Space Treaty. Immediately following the reference to "peaceful purposes," the text of the Antarctic Treaty states that "[t]here shall be prohibited, *inter alia,* any measures of a military nature . . . ." It is the additional language contained in the Antarctic Treaty, and not found in the Outer Space Treaty, that distinguishes the interpretation of the "peaceful purposes" language. Furthermore, State practice in Antarctica in 1959, when the treaty was drafted, was exclusively non-military while State practice in space in 1967, when the Outer Space Treaty was signed, was overwhelmingly military in nature.

The US view that Article IV does not preclude lawful military activity is also supported by the historical context in which the Outer Space Treaty came into existence. When the Outer Space Treaty was signed, its two primary drafters, the US and the Soviet Union, were already using outer space for military purposes. It is unlikely that the Outer Space Treaty was intended to proscribe existing practice by its two primary drafters.[109] The idea that "peaceful purposes" meant at least some military use was also consistent with the US space policy at the time. For instance, President Eisenhower declared to Congress, when the

National Aeronautical and Space Administration (NASA) was established, that the US was committed to the principle that "outer space be devoted to peaceful and scientific purposes."[110] Similarly, the Aeronautics and Space Act of 1958 contained language that "it is the policy of the United States that activities in space shall be devoted to peaceful purposes for the benefit of all mankind."[111] Despite use of such language, that same act provided for military departments to conduct space activities, including the development of weapons systems, military operations, and the defense of the US. Thus, the US has never interpreted "peaceful purposes" to mean only non-military activity. Rather, the US position has consistently been that the concept of "peaceful purposes" only prohibits aggressive military activity contrary to international law.[112] In 1962, Senator Albert Gore, Sr. stressed this distinction before the UN General Assembly. He urged that the "test of any space activities must not be whether it is military or non-military, but whether or not it is consistent with the UN Charter and other obligations of law."[113] While this view is not held by all,[114] it now appears to represent the international consensus[115] and is consistent with Article III of the treaty, discussed later. Therefore, any information operations undertaken in self-defense pursuant to a Security Council resolution, or in accordance with any recognized lawful purpose, would not be prohibited by either Article IV or other portions of the Outer Space Treaty. Moreover, during any period of international armed conflict, it is unlikely that these provisions would even apply between the belligerents who were parties to the treaty. While there are several views as to the test for when a treaty is abrogated or suspended by war between belligerent parties, the fundamental principle is the compatibility between the particular treaty provisions at issue and a state of war or armed conflict. Since the issue depends on the "intrinsic character" of the treaty provisions in question,[116] to the extent the Outer Space Treaty provisions being discussed here are incompatible with the object and purpose of armed conflict, they would most likely be suspended.

Finally, Article IX has the most direct application to the issue of information operations that interfere with the use of outer space by other nations. Indeed, the language of this article echoes principles enunciated earlier in the 1963 Declaration. In addition to requiring all States to conduct their activities in outer space "with due regard" for the interests of other States, it goes on to declare the following:

> If a State Party to the Treaty has reason to believe that an activity or experiment planned by it or its nationals in outer space, . . . would cause *potentially harmful interference* with activities of other States Parties in the peaceful exploration and use

> of outer space, . . . it shall undertake appropriate international consultations before proceeding with such activity. . . . (emphasis added)

Through this provision, the Outer Space Treaty made legally binding the 1963 Declaration's principle of prior consultation based on the potential for harmful interference in the space activities of another State.

Although the provisions cited above are likely to be interpreted in the international community to mean that "harmful interference" is prohibited, there are two important limitations to this prohibition as applied to information operations. The first is that the interference must be directed toward the "peaceful" use of space by other States. It is clear that a State may lawfully interfere with the space activities of other States when such activities are pursuant to a lawful use of military force. The second limitation is that the interference to the space system of another must be "harmful." Information operations that intrude upon, tap into, or monitor other space systems communications or other data for a military purpose can arguably be conducted without "harming" the space system of the other State, and to the extent they do no harm, they do not violate Article IX of the Outer Space Treaty.[117] Of course, regardless of such an argument, the State whose system was intruded upon would probably beg to differ. In fact, even if the intrusion were deemed not to violate Article IX, the political fallout could be extremely problematic.

Article III is perhaps the most important and illuminating of all the Outer Space Treaty provisions, the one which puts all the others into proper context. Article III states that the Parties "shall carry on activities in the exploration and use of outer space . . . *in accordance with international law, including the Charter of the United Nations,* in the interest of maintaining international peace and security . . . ." (emphasis added) It is this standard, far more than the oft-cited concept of peaceful purposes, that is central to whether or not activities in outer space comply with the Outer Space Treaty. While academic discussions will invariably center around the peaceful purposes language, military commanders, planners, and operators who are considering activities in outer space should focus instead on whether the military activity is lawful under the traditional law of armed conflict. If a nation's military activities are conducted "in accordance with international law" and the Charter of the UN, then the Outer Space Treaty recognizes that such activities can be in the interest of international peace and security. Consequently, it is Article III, not Article IV, that should be the primary focus of attention. Since the UN Charter is one of the standards cited in Article III, it is appropriate that we turn to that instrument.

2. UN Charter

Article 1 of the UN Charter expressly states that the purpose of the UN is to "maintain international peace and security." Accordingly, military activities aimed at restoring peace and conducted pursuant to a UN mandate or otherwise consistent with the Charter would be for a peaceful purpose. Article 39 of the Charter authorizes the Security Council to determine if a threat to peace, a breach of peace, or an act of aggression exists such that measures to restore international peace and security are required. Included among the lawful measures that the Security Council is authorized to direct in restoring peace and security are those set forth in Article 41, which include "the complete or partial interruption of. . . rail, sea, air, postal, telegraphic, radio, *and other means of communication*" (emphasis added). Clearly, information operations which have the effect of interrupting communications, and which are conducted pursuant to Article 41, would not only be lawful but an act undertaken to maintain or restore international peace and security. Therefore, such information operations would also be consistent with the Outer Space Treaty.

The UN Charter goes even further in allowing for military action to maintain or restore international peace and security. Article 42 authorizes "such action . . . as may be necessary to maintain or restore international peace and security" when Article 41 measures would be, or have proven to be, inadequate. By it, the Security Council has the authority to direct its members to "use all necessary means" to carry out Chapter VII peace enforcement measures, and, indeed, past resolutions such as Security Council Resolution 678 (DESERT STORM) in 1990[118] and Security Council Resolution 1264 (East Timor) in 1999[119] have contained this language. Coupled with the "all necessary means" language of a Security Council resolution, Article 42 allows information operations of far greater scope than merely interrupting communications, as authorized by Article 41. In determining the lawfulness of a particular information operation, it is necessary to evaluate the factual context, not just the type of information operation conducted.

Information operations can also be undertaken for purposes of individual or collective self-defense, an inherent right of all nations clearly recognized by Article 51 of the Charter. The mere fact that information operations affect space systems, or are conducted from outer space, does not make those operations illegal.

International Consortia and Other International Agreements

1. International Telecommunications Convention (ITC)

The ITC is the basic charter for the International Telecommunications Union (ITU), one of the oldest existing international organizations. [120] The ITU

directly oversees the communications satellite industry, arguably the most important sector of outer space activity.[121] A specialized agency of the United Nations since 1945,[122] it has been used by the UN to promote international cooperation in space[123] through the regulation of telecommunication services and allocation of radio frequencies.

Article 45(1) of the most recent ITU Convention, which was adopted in Geneva in 1992 and amended by the Plenipotentiary Conference at Kyoto in 1994, requires that all telecommunication stations operate so as not to cause "harmful interference" to the radio service or communications of other Members.[124] The convention defines "harmful interference" as "[i]nterference which endangers the functioning of a radionavigation service or of other safety services or seriously degrades, obstructs or repeatedly interrupts a radio-communication service operating in accordance with the Radio Regulations."[125] According to at least one scholar, the term is intended to be broadly interpreted and covers "any kind of damaging or destructive activity."[126] While this interpretation may have some academic value, it is not widely held, is not consistent with the express language of the ITC, and certainly does not represent the position of the United States.[127]

Information operations, such as implanting a trap door into the communications network of a potential adversary or setting up another type of then benign, but potentially destructive, cyber agent in the telecommunications system of another State, might be seen by some as "harmful interference." Arguably, because the purpose of its presence is to enable harmful interference or provide destructive capability when needed, the fact that an information operation mechanism is currently benign does not mean it is non-harmful. It would be difficult to show that this type of interference endangered the functioning of a service, seriously degraded it, or served to repeatedly interrupt it. However, even if there were found to be "harmful interference" from the activity, if the implanting of latent viruses or other cyber instruments were taken against a military network of another State, there would be no ITC violation. The ITC restrictions provide a recognized exception for "military radio installations" through Article 48(1). A more difficult situation arises when the activity affects a dual-use civilian telecommunication system, one used for both civilian and military purposes.

Finally, the ITC does not provide for its continued application between Party belligerents during armed conflict. Since its provisions are not compatible with the object and purpose of such hostilities, they will likely be considered suspended between the belligerents throughout the duration of any international armed conflict.[128] Thus, the only time the provisions in the ITC would apply

and possibly restrict some types of information operations would be when they do not rise to such a conflict level.

2. INTELSAT Agreement of 1973

Through the International Telecommunications Satellite Consortium (INTELSAT), the US initiated the first worldwide commercial telecommunications satellite system.[129] Created to encourage global nation-to-nation public satellite service,[130] INTELSAT reflects the US view of space law and policy. For example, within its basic structure, the consortium allows nations to invest and own shares in the organization, instead of it being organized along the old one-nation, one-vote concept. This voting and profit sharing formula reflects the US positions that space is to be used for the "benefit of mankind," and that the "province of mankind" does not require an equal apportioning of space wealth.[131] Despite these "American" views of space law, the Soviet Union joined INTELSAT in 1991;[132] there are currently 143 member countries. INTELSAT operates the world's most extensive global communications satellite system in existence, and DoD has been a user of the system from its advent.[133]

Articles III (d) and (e) of the INTELSAT Agreement describe military use of INTELSAT services. These provisions set forth a clear proscription on using "specialized telecommunications services" for military purposes. However, that proscription does not preclude INTELSAT from providing standard "public telecommunications services" to a military force for a military purpose.[134] In fact, according to a COMSAT legal opinion, aside from the limitation on using "specialized" services, "there is nothing in the INTELSAT Agreement that prohibits or discourages the use of INTELSAT for either US national security or intelligence purposes."[135]

The more difficult issue is the interruption, denial, or even destruction, of the data or data links from an INTELSAT system. There is nothing in the INTELSAT Agreement[136] that specifically prohibits interference with communication systems, although it certainly is implied throughout the agreement.[137] For example, Article XIV(d) of the agreement requires a party or signatory to consult with the Assembly of Parties and furnish all relevant information prior to using an INTELSAT space segment in a way that might prejudice the establishment of direct telecommunication links of other members.

INTELSAT's requirements of prior consultation and disclosure in advance of an operation would be completely unfeasible in the context of a military information operation. Absent some agreement with the members to the contrary, a Security Council resolution authorizing "all necessary means" under a

Chapter VII action, or some other lawful justification, this INTELSAT provision could serve to require disclosure and thus limit peacetime military information operations activities that interrupt, deny, or destroy another's data from an INTELSAT service. However, as with the other international agreements, during a period of international armed conflict, these limiting INTELSAT requirements will likely be viewed as suspended between the parties to the conflict, thus allowing jamming, destruction of ground stations belonging to an adversary, or other information operations.[138]

3. INMARSAT Convention

The International Maritime Satellite Organization (INMARSAT) was formed in 1976[139] to extend the INTELSAT framework to include maritime communications and certain maritime nations excluded from INTELSAT.[140] While its purpose was to provide space connections necessary to improve maritime and aeronautical communications, it has expanded into other systems, such as mobile communications.[141]

Article 3(3) of the INMARSAT Convention[142] provides that "the Organization shall act exclusively for peaceful purposes." Initially, INMARSAT took the view that military uses per se were not compatible with peaceful purposes unless they were for distress and safety or purposes recognized by international humanitarian law.[143] Much like the Outer Space Treaty, the INMARSAT Convention, in Article 12(1)(b), obligates the INMARSAT Assembly of Parties to ensure its activities are consistent with the UN Charter. INMARSAT's "peaceful purposes" language must therefore be read in the context of the UN Charter. When that is done, it becomes clear the INMARSAT Convention does not prohibit military action conducted under the auspices of the UN Security Council, legitimate individual or collective self-defense, or military action that is otherwise consistent with international law.

A recent privatization development, however, may have rendered the entire discussion over the meaning of "peaceful purposes" in the convention moot. On April 15, 1999, the assets and liabilities of the INMARSAT intergovernmental organization were transferred to a private company called, for lack of a better term, "new INMARSAT."[144] The new company's legal obligations arise out of its Memorandum of Association (MOA) and the Public Services Agreement (PSA) between it and the residual INMARSAT organization. The MOA requires new INMARSAT to "have due regard" for certain principles, including the "peaceful purposes" principle, but COMSAT's lawyers have taken the position that this language only requires the company to take those principles into consideration.[145]

Similarly, while clause 2.3 of the PSA provides that "[t]he Company shall act exclusively for peaceful purposes," the INMARSAT Assembly believed this language was political in nature and without an enforcement mechanism for alleged violations.[146] Therefore, according to the April 15, 1999, COMSAT General Counsel Opinion, "COMSAT envisions no circumstances in which the 'peaceful purposes' principle would be invoked as a reason to deny service to the US Department of Defense or units thereof."[147] That opinion, however, does not address whether "harmful interference" with a member's INMARSAT space segment or communication link would constitute a violation of its "peaceful purposes" language. Since the new organization is still based on the INMARSAT Agreement, it is not clear to what extent a member might seek to claim a violation of the provisions of that agreement. On the other hand, since new INMARSAT is now privatized, perhaps the only remedy to the private company shareholders would be contractual in nature. Regardless, potential disputes with offended nation shareholders will likely be avoided if the proposed military action is taken pursuant to the UN Charter or other international law.

4. Arms Reduction Treaties

Arms reduction treaties also contain provisions affecting the use of information operations. For instance, the ABM Treaty, in Article XII(2), was the first to preclude any activity which interfered with the "national technical means of verification" of treaty compliance by the other Party. Most other arms reduction treaties, such as SALT II and the START Treaty, have similar language.[148] While these formerly bilateral treaties are limited in the number of Parties involved, and there are concerns about what constitutes an unlawful interference with the national technical means of verification, the interference issue is certainly problematic. Although this matter merits further elaboration beyond the confines of this chapter, suffice it to say that information operations must be conducted so as to avoid interfering with national verification means during times other than international armed conflict.

5. Principles of the Law of Armed Conflict

Readily apparent in this overview of space law applicable to information operations is that despite all the sophisticated technology involved and the potential application of additional treaties and consortia agreements, by and large, the legal principles are the same as those applicable to other places and means of warfare. Just because military operations are planned for a unique domain—space—using a unique method—information operations—does not

change the fundamental legal constraints with which militaries must abide. It is imperative, as with all military actions, that a particular information operation in space or affecting a space object be conducted pursuant to a lawful purpose and in a lawful way. It is this second aspect of lawfulness that raises the issue of law of armed conflict (LOAC) principles. Notwithstanding the claims of some information operations supporters that this method of warfare transcends the scope of existing law, LOAC applies readily to information warfare techniques.[149]

Any offensive use of electronic means during military operations would implicate the traditional law of armed conflict principles. These include the counterbalancing principles of military necessity and the avoidance of superfluous injury, as well as the corollary principles of distinction of combatants from noncombatants, proportionality, and chivalry.[150]

The principle of military necessity is used to distinguish between what is and what is not a proper subject of attack.[151] It recognizes that enemy forces, along with their equipment, are always a proper subject of attack absent some other overriding LOAC principle. Similarly, civilians and civilian property that make a direct contribution to the war effort may be attacked, as long as their damage or destruction would produce a significant military advantage[152] or accomplish a legitimate military objective.[153] The presence of a dual-use system, commonly found in the arena of space systems, makes targeting analysis more difficult, but it does not change the fundamental analysis. Dual-use systems complicate the delineation of purely military targets from purely civilian non-targets. Therefore, targeteers must resist the temptation to attack a civilian computer system, such as a banking system, university, stock exchange, or similar target, merely because their attacks may have some vague effect on the enemy.

> In a long and protracted conflict, damage to the enemy's economy and research and development capabilities may well undermine its war effort, but in a short and limited conflict it may be hard to articulate any expected military advantage from attacking economic targets.[154]

Accordingly, proposals to target civilian information systems must be examined closely to determine whether there is a military necessity for the attack. Other potential targets requiring close operational and legal analysis could include dual-use systems, such as navigation satellites or public communications systems, in which the data is provided through an international consortium such as INTELSAT, EUROSAT, or ARABSAT. Attacking data systems of international consortium organizations will likely affect many users of the data who are either not parties to the armed conflict or who are declared neutrals. Basically,

the target analysis will be the same when using information operations directed against space systems as it is using other means against other targets; it will just be more complex.

A complementary principle to military necessity is the avoidance of superfluous injury.[155] International law "forbids the infliction of suffering, injury or destruction not actually necessary for the accomplishment of legitimate military purposes. This principle of humanity results in a specific prohibition against unnecessary suffering [and] a requirement of proportionality."[156] It is the principle of superfluous injury that has led nations to agree to ban certain weapons.[157] In the context of information operations, it is difficult to imagine any specific use that has the potential of causing superfluous injury, but new technologies and uses require commanders to consider this principle.

Another important LOAC principle, distinction, demands that combatants be distinguished from noncombatants, and that military objectives be distinguished from protected property or places.[158] Only combatants and military objectives are to be attacked.[159] Additionally, indiscriminate attacks and methods and means of combat are also prohibited. A further aspect of this principle is that, with very limited exceptions, only members of a nation's regular armed forces are entitled to use force against the enemy.[160] To distinguish between combatants and noncombatants, the rule developed that combatants must wear a distinctive uniform.[161] In the case of an information operation initiated from a distant computer terminal, there is no practical need for the operator to be in uniform. However, this does not mean that the distinction between combatants and noncombatants during an information operation should not be retained.

> If a computer network attack is launched from a location far from its target, it may be of no practical significance whether the "combatant" is wearing a uniform. Nevertheless, the law of war requires that lawful combatants be trained in the law of war, that they serve under effective discipline, and that they be under the command of officers responsible for their conduct. This consideration argues for retaining the requirement that combatant information operations during international armed conflicts be conducted only by members of the armed forces.[162]

The principle of proportionality requires that any civilian injury resulting from a legitimate use of military force not be disproportionate to the military advantages anticipated.[163] International law recognizes that attacks on lawful military targets can result in unavoidable collateral injury and damage to noncombatants and civilian property.[164] While the commander ordering the

attack is responsible for making this proportionality judgment, the defender has a responsibility to properly separate military targets from noncombatants and civilian property.[165] Information systems may be legitimate military targets, but an estimate of collateral damage and the damage from attacking them must take into account whether, and to what extent, they provide essential services to noncombatants.[166] This will require thorough intelligence information on an adversary's computer systems and networks to aid a decision that must be made on a case-by-case basis.

The final principle, chivalry, prohibits treachery or perfidy during armed conflict.[167] It demands a certain amount of fairness in offense and defense, as well as a certain mutual respect, honor, and trust between opposing forces.[168] When stratagems of war are developed, belligerents must be cautious not to subvert humanitarian safeguards to effect purely military goals.[169] For example, using a computer "morphing" technique to create an image of an enemy leader informing his military that an armistice or cease-fire agreement has been signed, when in fact no such agreement exists, would be an illegal perfidious act.[170]

Due to the complexity of applying LOAC principles to information operations against space systems, specific targeting proposals should be reviewed and approved in accordance with the rules of engagement in place and the procedures established by the National Command Authorities (NCA) or the Joint Force Commander, usually through a Joint Targeting Coordination Board.[171] Overall, information operations must be conducted consistent with the Standing Rules of Engagement (SROE) and may be used in individual or unit self-defense (as defined in the SROE) or with NCA approval.[172]

Application of General Law to Specific Scenarios

Having set forth the general legal framework applicable to information operations conducted in outer space or upon space systems, we now want to apply that framework to a series of escalating factual scenarios. While we hope these scenarios are somewhat realistic, they are not intended to imply that the United States or any other nation engages in such operations or even has the capability to do so.

Scenario 1: Implanting Sniffers and Trap Doors

Nation A has a security organization that obtains information from the Internet and attempts to gain information from other nations' computers. Nation A is especially concerned with the activities of Nation B, which has been

hostile in the past. Consequently, Nation A's security organization has directed covert activities toward Nation B. Both nations are industrialized and have well-developed infrastructures. Additionally, both nations have a space program that includes surveillance and telecommunications satellites with ground-based downlinks which provide data to the computers.

A security agent of Nation A reports to his supervisors that he has gained access, through the Internet, to the computer system that serves one of Nation B's unclassified military communications networks. This network uses space assets to ensure connectivity. He proposes implanting a trap door and "sniffer" that will, once in-place, remain inert and harmless, but which can be used to monitor data coming into this network.

Discussion

Obviously, gathering unclassified information readily available to the public is legal. However, implanting a trap door and "sniffer" which can be used to monitor space communication systems of another nation is more questionable. Most likely, such intrusions would violate the domestic laws of the offended State, but there is very little authority that, during peacetime, it would violate international law.[173] This type of information operation is likely to be viewed much as peacetime espionage is viewed, namely, of no significant concern unless serious practical consequences are shown.[174] As such, except for having to weather the diplomatic costs of protest and political rhetoric by Nation B, assuming they are able to ascribe the intrusion to Nation A, international law neither provides a remedy nor imposes any sanctions.

Specific space law provisions similarly provide no legal restraint on this intrusion. The Outer Space Treaty only applies to activities in outer space, the moon, and other celestial bodies and is, therefore, not applicable to an intrusion into a ground system. Assuming Nation B is an ITU member and the system intruded is a system regulated by the ITU, then some might suggest that the ITC applies. They would be in error. As noted above, Article 45(1) of the ITC prohibits "harmful interference"—that which "endangers the functioning" of a radionavigation service or "degrades, obstructs or repeatedly interrupts" a radio communication service. Trap doors and "sniffers" do not degrade, obstruct, or interrupt communications. Moreover, such a cyber intrusion arguably does not "endanger the functioning" of the communication service.

Likewise, such an act would not violate the UN Charter. Implanting a monitoring device that establishes a passageway for future intrusions is all that this information operation entails. Such implanting is akin to a covert intrusion into the command and control center of another country and placing a monitoring

device on the phones. This action would neither endanger international peace and security under Article 2(3) of the UN Charter, nor would it constitute a threat to the political independence of any State under Article 2(4). While this type of computer penetration might constitute a threat to the territorial integrity of a UN member State, it will likely be treated much like espionage, which State practice has clearly accepted, at least tacitly. As such, it can be accomplished with little risk of prosecution under international law or UN sanction. The fact this particular intelligence gathering activity is conducted using information operations that impacts data from a space system, rather than more traditional means of espionage, does not change the basic equation.

In sum, this first scenario does not present any legal obstacles or limitations under either space law or international law. Nonetheless, it could be highly volatile in the political arena and would present a delicate policy decision that must be made by the NCA.

Scenario 2: Interruption of Command and Control Networks

Tensions between A and B increase, but have not risen to the level of armed conflict. At this point, another security agent from Nation A gains access to one of B's unclassified military communications networks through the trap door previously implanted. He temporarily jams the network so that contact with B's orbiting satellites will be interrupted for a period of approximately 30 minutes. After about twenty minutes, Nation B's space technicians regain control of their satellite network and restore normal communications. There is no damage to the satellite or permanent disruption of its functions.

Discussion

Since this has not occurred during an armed conflict, some might argue that interfering with the satellite network of Nation B would constitute a violation of Article 45(1) of the ITC if the 20-minute interruption of communications is deemed to be "harmful interference." The ITC definition requires that the interference endanger the functioning of a radionavigation service or other safety service, or seriously degrade, obstruct, or repeatedly interrupt a radio- communication service. Whether or not a 20-minute interruption of satellite communication constitutes a serious degradation or obstruction might depend on the precise nature of the communications that were interrupted. For instance, if critical search and rescue systems were interrupted thereby resulting in the loss of life of Nation B citizens, then perhaps the interruption would be seen as harmful, even though the space system itself may not have been damaged or harmed.

Under the UN Charter, there is some legal basis for the proposition that taking control of another nation's communications system or space assets may interfere in the internal affairs of that nation thus violating its rights under the UN Charter. This would be especially true if the interruption resulted in loss of life as noted above. It might also be true if the space system interrupted was particularly important to Nation B's defense, such as a missile early warning system. Any determination that rights under the UN Charter were violated or not will depend, as it will under the ITC, on the precise nature of the system that is interrupted. In this scenario, Nation A's interruption of one of Nation B's unclassified communication systems was temporary and it did not detract from sensitive military systems. Absent at least resulting moderate damage or injury, an armed response in self-defense by Nation B would not appear to be justified. Most likely, the primary costs of this scenario would be political in nature.

Scenario 3: Moving an Adversary's Satellite Out of Effective Orbit

Nation A knows that Nation B has a military reconnaissance satellite with high resolution capability that can provide Nation B with critical intelligence on the movements of Nation A's troops. Nation A is concerned about recent bellicose statements made by Nation B toward Nation A and wants to mobilize several thousand troops along their shared border. In anticipation of the outbreak of armed conflict, Nation A covertly obtains internal access to B's classified military computer system and uses information operations to send false data instructions to the Nation B satellite. While this false data does not damage the satellite, it does cause the satellite to move into another orbit where its surveillance capabilities are rendered completely ineffective.

Discussion

As in the prior two scenarios, there is no physical damage or destruction involved with the satellite or systems of Nation B and armed conflict has not yet arisen. Unlike Scenario 2 though, this interference with Nation B's military satellite will require Nation B to take steps to "recover" the satellite and restore its prior orbit before it can be effective. In effect, the satellite has been "kidnapped" at a militarily critical point, providing Nation A with a distinct military advantage should armed conflict occur.

Since this scenario involves a military satellite and not an INTELSAT system or asset, the INTELSAT Agreement does not apply. Therefore, there is no requirement under Article XIV(d) of the INTELSAT Agreement of prior consultation or to provide all relevant data regarding the interference. Furthermore, as

long as the satellite was not engaged in conducting Nation B's "national technical means of verification" of arms control obligations, the interference would not violate the ABM Treaty or similar arms control treaty verification provisions,[175] assuming A and B were Parties.

The problem raised in this scenario derives again from the UN Charter. Assuming Nation B's satellite is considered part of Nation B's "sovereignty" or "territorial integrity," Nation A's actions to involuntarily move it out of orbit could be viewed as a "threat . . . against the territorial integrity or political independence of any state" in violation of Article 2(4). If so, the Security Council, under Article 39, would be authorized to decide what appropriate measures to take against Nation A to restore international peace and security. Given the national security importance of this reconnaissance satellite to early warning, the Security Council might determine that this act rises to the level of an "armed attack" sufficient for Nation B to invoke its right of self-defense under Article 51 of the UN Charter. In addition, Nation B might determine independently that the action requires it to invoke its inherent right of self-defense without waiting for a UN determination.

Scenario 4: Destruction of Adversary's Satellite

As anticipated, armed conflict has now broken out between Nations A and B. Nation A's troops, previously amassed along Nation B's border and heavily armed, have crossed into Nation B. Numerous reports indicate Nation A's troops have been firing at Nation B's military forces as they approach the nearest town. An emergency session of the Security Council has been called to address the situation, but no UN response has yet been authorized. Moreover, since Nation A is a close ally of a permanent member of the Security Council, a veto of any UN action against it is anticipated. Nation B's targeteers propose to destroy a key hub in the space communications system of Nation A and render its connected computers useless. They plan to maneuver one of their own satellites within close range of one of Nation A's telecommunications satellite. This "killer" satellite has been equipped with a device that, when activated, will emit an electro-magnetic pulse which will disable all electronic devices within a ten-mile radius. Destruction of the targeted satellite, located in geosynchronous orbit over the area of armed conflict, will render Nation A's entire communication system inoperable.

Discussion

This scenario presents a clear armed conflict situation that very likely renders the Outer Space Treaty, the ITC, and any arms control agreements

inapplicable.[176] If there is any doubt as to whether these international agreements were intended to be suspended or terminated during armed conflict, Nation B could make a prior declaration that it considers each of them inapplicable during this period of armed conflict with Nation A.

Nation B could choose, for policy reasons, to treat this as an "armed attack" and exercise its right of individual self-defense, or it could treat A's incursion as "an act of aggression" under Article 39 of the UN Charter and seek Chapter VII sanctions through the UN. Before Nation B can exercise its right of self-defense through use of force, Article 33 of the UN Charter requires it to exhaust any available peaceful means of settlement, unless, of course, such efforts would be futile.[177] Seeking action through the Security Council would likely prove fruitless, since Nation A is a close ally of a permanent member with veto authority. Regardless, Nation B's armed response must be necessary, timely, and proportionate to the wrong suffered.[178]

Given the military value to Nation A of this satellite system, there would be a legitimate military necessity in attacking this space asset. Destruction of Nation A's satellite would put the military aggressors at a distinct disadvantage in obtaining and disseminating intelligence and communication data without resulting in loss of life. Additionally, since the targeted space communications system is used for military communications, even though it also has a civilian use, there is a legitimate military reason to attack it. The principle of proportionality requires Nation B's commanders to make their best estimate of the military advantage to be gained and weigh it against their best estimate of the effect on the civilian population. The extent of injury or damage to the civilian population from interruption of a communication system through information operations is likely to be significantly less than from kinetic weapons. Additionally, this particular information operation, used as a weapon, is neither illegal *per se* under international law, nor are its effects necessarily indiscriminate. Indiscriminate weapons are those whose effects cannot be controlled, such as chemical and biological weapons. The wide area in which this weapon's effects will be felt do not make it indiscriminate, especially since its effects will be short-term, and limited to disabling electronic devices.

Readily apparent from each of these scenarios is the importance of making a case-by-case assessment under international law, and more particularly, LOAC principles. As with any LOAC assessment, a proper determination of a specific information operation can only be obtained by applying the specific facts to the general legal framework. What makes the assessments of information operations directed at or from space systems more difficult is the lack of extensive State practice to rely on.

Practical Considerations in the Application of Information Operations in Space

In addition to the legal regime applicable to information operations in outer space, military planners should also factor the unique physical aspects of space and the political consequences of specific military decisions into their calculations. In this final section, we have attempted to set forth a few such considerations. Keep in mind however, that they are not based on legal constraints, but rather on the physical properties of outer space and the political climate of the international community. Additionally, these considerations are not intended to preclude a commander's discretion as to the appropriate military action to be taken given the specific military situation faced.

First, any attack upon a physical target in space should seek to disable the space object without resorting to its physical destruction. Absent the effects of gravity and friction, fragments from physical destruction of space objects present a significant problem in outer space. Those fragments will naturally spread throughout the orbital path they came from in an unavoidable pattern that may not dissipate. Their velocity and mass will make them a threat to our own space vehicles and satellites. Confining the effects of that debris will be difficult, if not impossible. Certain information operations in space can provide an alternative to the military planner to outright physical destruction of an adversary's space object by destroying the computer links and data (its life support). Thus, "killing" of the object may be possible without creating a dangerous spread of fragments to our own space systems.

Second, if a space system needs to be destroyed, consideration should be given to destroying it by attacking its ground segment, and thereby severing access to its "life support." Attacks on ground segments of communications systems have received long-standing public acceptance in the international community as an authorized means of conducting armed conflict as long as the target is a legitimate military target. A direct attack on a space segment in space, even if done consistent with international law, may not enjoy the same public acceptance. Given the importance of international opinion upon national leaders and their citizens, military action often attempts to avoid undue public outcry in making target selections. Therefore, if there is a choice, it may be better to take out an adversary's space object by attacking and destroying its ground segment.

Third, destruction through "jamming" of a communication signal is preferable to destruction of the adversary's space object and accomplishes the same result—the enemy's inability to use that system. Just as ground attacks have received public acceptance, so too has the technique of jamming. It is a common practice during

armed conflict and is clearly recognized as a legitimate means of attack. As such, and for reasons of avoiding undue public outcry, jamming should be considered as an alternative to the outright physical destruction of the space object. Additionally, jamming avoids the problem of unnecessary space debris.

Fourth, a less intrusive electronic means of attack is often preferable to a kinetic kill. Electronic attack can be a better means of avoiding detection while "masking" the identity of the perpetrator. When subtlety or plausible denial is desired for political reasons, or if there is a need to delay enemy detection of the attack, electronic means can be very effective. When an adversary's system goes down, they will not necessarily know it was the result of an intentional act by an enemy. This is especially so if the system is left operable, but has been manipulated so that the system data is, or appears to be, false. Depending on the system attacked, this manipulation can cause military planes to crash, artillery to miss its target, or enemy leaders to make poor decisions.

No doubt, many other practical approaches to the use of information operations in outer space or directed toward space objects have not been mentioned here. Those offered are but a limited start for planners and strategists when considering the unique aspects of these two technologically driven realms (information operations and outer space) during armed conflict.

Conclusion

We began this chapter with the observation that when the technological transformations inherent in outer space systems are combined with that of information operations, yesterday's science fiction can quickly become today's reality. The need for militaries to keep pace is obvious. These technological transformations will require innovative approaches to an ancient reality—armed conflict between belligerent nations. Information operations and modern space systems have created new warfighting scenarios that can, in turn, create confusion among military commanders and planners as to what is lawful and what is not. It is imperative that operators and lawyers forge a partnership to meet this challenge.

As for what is legal in the outer space environment, there are few surprises. Still relevant is traditional analysis under well-known principles of the law of armed conflict, customary international law, treaty obligations, and the UN Charter. Aside from the need to apply the existing analytical framework to new futuristic threats, there are few legal limitations impacting information operations in or through outer space.

The real challenge comes in understanding the expansion of international *political* sensitivities to weapons in space and information operations directed at or

from outer space. During times of armed conflict, those sensitivities will not create violations of international law, but they can impede our actions through the political and diplomatic process. We should not underestimate the degree to which politics and diplomacy place limits upon otherwise lawful military activity. Thus, with only a few exceptions, from a legal standpoint, information operations in space are virtually no different than those conducted on the ground, in the air, or at sea. The primary difference lies in the diplomatic and political response of the international community.

Moreover, the "CNN factor" has had a large role to play in the decisions of military commanders to employ ground, sea, and air assets in recent armed conflicts. We can expect the influence of the "CNN factor" to grow exponentially if military commanders choose to employ information operations against objects in outer space, a much more sensitive arena. Indeed, because of this, commanders may find their authority to choose targets and the means of attacking those targets withheld by the NCA in this arena more than any other.

All that aside, however, once the political decision has been made, commanders should apply the same principles of international law they do in more conventional settings. They must avoid the dizzying distraction created by the vast array of new technological tools available to the military in the space arena; they must resist the temptation of expecting that these apparent futuristic tools require a whole new set of laws; and they must be willing to apply old laws and principles to new military scenarios. If they can do that, then tomorrow's commanders can maintain the *legal* high ground of warfare, while controlling the *military* high ground of outer space. This is not a matter of science fiction; it is reality.

Notes

* The authors would like to thank the following people for their assistance in reviewing this chapter: Mr. Phillip Johnson (Colonel, USAF, (ret.)), Mr. Michael Schlabs (Colonel, USAF (ret.)), Colonel Kevin Kennedy, (USAF), Lieutenant Colonel Mark Yost (USAFR), Lieutenant Colonel Jolinder Dhillon (USAF), Lieutenant Colonel Jeff Walker (USAF), and Lieutenant Colonel Jeff Rockwell (USAF).

1. Nathaniel Borenstein, quoted from *Zeebo's Marvelous Quotes, Quotes about Computers* (Sept. 3, 2000) http://quotes.sterlingtechnology.com/key/key_Computers.html.

2. For instance, military parades of the future could be comprised of rank after impressive rank of glistening computer terminals passing in review instead of shiny tanks and rifle-carrying soldiers; the sides of military computers of the future may be painted with rows of mean looking Internet wires to represent each "kill" of tomorrow's computer aces; and recruiting posters may have a picture of a computer geek with lines of pencils sticking out of his pocket protector and a caption beneath saying, "We want you!" While these scenarios are a bit far-fetched, there is no denying the importance of computers in the battles of the future.

3. *Pentagon Officials Warn of Electronic Pearl Harbor*, MILITARY & C4I, March 11, 1999, at n.p.

4. Charlie Williamson, *Emerging Issues in Cyberdefense,* ABA NATIONAL SECURITY LAW REPORT, Aug. 1999, at 2; A REPORT OF THE PRESIDENT OF THE UNITED STATES, PRESERVING AMERICA'S PRIVACY AND SECURITY IN THE NEXT CENTURY: A STRATEGY FOR AMERICA IN CYBERSPACE, Sept. 16, 1999, at 6 [hereinafter referred to as REPORT OF THE PRESIDENT].

5. This rate of detection represents those that are reported. *See* Ted Uchida, School of Advanced Military Studies, US Army Command and General Staff College, Building a Basis for Information Warfare Rules of Engagement 8 (1997) (unpublished manuscript, on file with Naval War College Library), *cited in* Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework,* 37 COLUMBIA JOURNAL OF TRANSNATIONAL LAW 885, 893 (1999).

6. The intruding teenage hackers were from California and aided by an Israeli teenager acting as their advisor. They were able to exploit a well-known weakness in an operator system called "Solaris." USIS Washington File, *On Information Warfare Threat,* MILITARY & C4I, Infowar.com, Dec. 14, 1998; *See also* Bradley Graham, *U.S. Studies New Threat: Cyber Attack,* WASHINGTON POST, May 24, 1998 at A1; WALTER GARY SHARP, SR., CYBERSPACE AND THE USE OF FORCE 20 (1999); E. Anders Ericksson, *Information Warfare: Hype or Reality?* 6 THE NONPROLIFERATION REVIEW, n.13 (1999).

7. MILITARY AND C4I, *supra* note 3, at 3.

8. SHARP, *supra* note 6, at 19.

9. Schmitt, *supra* note 5, at 887.

10. Bob Brewin, *Kosovo Ushered in Cyberwar,* FEDERAL COMPUTER WEEK, Sept. 27, 1999, at 1.

11. White Paper, The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63 (May 1998).

12. Kevin Poulsen, *Info War or Electronic Saber Rattling?,* ZDNN TECH NEWS NOW, (Sept. 8, 1999), at 1–2.

13. *Id.* The JTF-CND Commander reports to the SECDEF through the Chairman of the Joint Chiefs of Staff. The Commander "has directive authority over assigned forces designated by Service components for execution of the CND mission, and coordinates with and supports commanders of combatant commands." Williamson, *supra* note 4, at 2.

14. USAF SCIENTIFIC ADVISORY BOARD, NEW WORLD VISTAS, AIR AND SPACE POWER FOR THE 21ST CENTURY (Information Applications Volume), at 3 (1995).

15. *Id.* A presence in space implies influence, power, and security.

16. *Id.* at 4.

17. Michael Loescher, *The Information Warfare Campaign, in* ALAN D. CAMPEN, DOUGLAS H. DEARTH & R. THOMAS GOODDEN, CYBERWAR 197 (1996).

18. REPORT OF THE PRESIDENT, *supra* note 4.

19. *See* Richard A. Morgan, *Military Use of Commercial Communication Satellites: A New Look at the Outer Space Treaty and "Peaceful Purposes,"* 60 JOURNAL OF AIR LAW AND COMMERCE 237, 248 (1994); SEAN P. KANUCK, *Recent Development: Information Warfare: New Challenges for Public International Law,* 37 HARVARD INTERNATIONAL LAW JOURNAL 272, 285 (1996).

20. GERALD R. HUST, TAKING DOWN TELECOMMUNICATIONS 4 (1994).

21. *Id.*

22. Of particular application is 18 USCode 1367, a federal criminal statute that prohibits the intentional or malicious interference with the authorized operation of a communications or weather satellite without the authority of the satellite operator. Also potentially applicable, in addition to US wiretap laws and depending on where the cyber attack originates, is 18 US Code 1030, which prohibits damaging protected computers by inserting viruses or other technological items; 47 US Code 333, which prohibits interference with licensed radio stations; and 47 US Code 502, which prohibits violation of international radio or communications treaties.

23. Air Force Doctrine Document (AFDD) 2-5, Information Operations, Aug. 5, 1998. As an example of the different terms used by the various military services, and as noted in the text, the Air Force is the only service to employ the term "information-in-warfare."

24. *Id.* Likewise, the Air Force definition of "information warfare" differs from that of DoD. For the Air Force, information warfare is a subcategory of information operations that is not confined to armed conflict. In contrast, the DoD sees "information warfare" as information operations "conducted during times of crisis or conflict." *Id.*, glossary.

25. John Deutsch, Testimony before the Senate Committee on Government Affairs (June 5, 1996).

26. JOHN ARQUILLA & DAVID RONFELDT, CYBERWAR IS COMING, RAND (1992).

27. Headquarters Air Force, International and Operations Law Division, Primer on Legal Issues in Information Operations, (draft), at 3 (1997). The term "offensive information operations" is intended to apply to the entire spectrum of military operations throughout peacetime through armed conflict, including military operations other than war. Offensive information operations embrace a great variety of activities, including psychological operations, military deception, jamming of enemy information systems, signals intelligence (SIGINT), and attacks on enemy information systems by physical destruction or by electronic means.

28. "Cyberwar refers to conducting, and preparing to conduct, military operations according to information-related principles." ARQUILLA, *supra* note 26, at 6.

29. *Id.* at 5.

30. Daniel Kuehl, What's New about Information Warfare?, at 10 (March 21, 1997), (unpublished NDU paper), cited in YuLin G. Whitehead, Information as a Weapon, Reality versus Promises 19 (January 1999), (unpublished School of Advanced Airpower Studies paper, Air University).

31. Interview by YuLin Whitehead with Daniel Kuehl, National Defense University, *cited in* Whitehead, *supra* note 31, at 19.

32. Joint Publication 3-13, II-9; Air Force Doctrine Document 2-5, Information Operations, at 9 (Aug. 5, 98); Air Force Doctrine Document 2-2, Space Operations, at 8 (Aug. 23, 1998). Winning the battle of information dominance requires that we achieve an edge in offensive exploitation of the enemy's vulnerabilities over its ability to penetrate our protective measures.

33. MAO TSE-TUNG, ON PROTRACTED WAR (1938), *cited in* NORMAN B. HUTCHERSON, COMMAND AND CONTROL WARFARE, PUTTING ANOTHER TOOL IN THE WAR-FIGHTER'S DATA BASE, at xiii (1994).

34. *See* HUTCHERSON, *supra* note 33, at xiii.

35. *See generally*, Department of Defense Space Policy contained in DoD Directive 3100.10, paragraph 4, specifically sub-paragraphs 4.3.1.4 and 4.3.1.7.

36. COLIN S. GRAY, EXPLORATIONS IN STRATEGY 102 (1996); *see also* Colin S. Gray and John B. Sheldon, *Space Power and the Revolution in Military Affairs*, AIRPOWER JOURNAL, Fall 1999, at 32.

37. Gray and Sheldon, supra note 36, at 32.

38. *Control of Space Key to Future War*, SPACE DAILY, May 10, 1999, at 1. There is also a political advantage to space forces over conventional forces. With conventional forces, policy makers have to contend with the possible loss of troops' lives when deploying them into battle. Use of space forces does not have that disadvantage. Major General DeKok, Air Force Space Command's Director of Operations and Plans, captured the difference when he remarked that, "Satellites have no mothers." Gregory Billman, *The Inherent Limitations of Spacepower: Fact or Fiction?* E-PRINTS, Sept. 22, 1999, at 21, www.fas.org/spp/eprint/billman.htm.

39. *Id.*

40. *Id.* The basic GPS consists of a constellation of 24 satellites, their navigation payloads, and associated ground stations, data links, and command and control facilities, and is operated by the DoD. It has become an integral part of US military operations.

41. The White House Fact Sheet, National Space Policy, Sept 19, 1996 at 1 [hereinafter Space Policy].

42. The following countries have communications satellites in orbit: Argentina, Australia, Brazil, Canada, China, Cuba, Finland, France, India, Indonesia, Italy, Japan, Malaysia, Malta, Mexico, New Guinea, Russia, Seychelles, Spain, Tonga, United Kingdom, and the US. Several other nations have access through cooperative agreements, such as the Association of Telecommunications State Enterprises of the Sub-Regional Andean Agreement (ASETA), comprised of Bolivia, Colombia, Ecuador, Peru, and Venezuela. *See* Morgan, *supra* note 19, at 247–248.

43. T. S. Twibell, *Note and Comment: Circumnavigating International Space Law*, 4 ILSA JOURNAL OF INTERNATIONAL & COMPARATIVE LAW, 259, 276 (Fall, 1997). In fact, as of November 21, 1999, China had successfully launched into orbit its first spacecraft designed to carry humans in an effort to join the US and Russia in the elite club of manned space flight. The unmanned module orbited the earth 14 times before it parachuted into a field in Inner Mongolia, 21 hours after taking off. Michael Laris, *China Launches New Spacecraft Designed for Manned Flight,* WASHINGTON POST, Nov. 22, 1999, at A1 .

44. Gerald Steinberg, *Dual Use Aspects of Commercial High-Resolution Imaging Satellites*, MIDEAST SECURITY AND POLICY STUDIES, Feb. 1998, at 3.

45. The latest of the SPOT imaging satellites, SPOT-4, has a 10 meter monochromatic resolution as well as an additional mid-infrared imaging capability. The French are presently working on SPOT-5A and 5B which they hope to launch in 2000 and 2003. *See* Steinberg, *supra* note 44, at 3. Satellites are now available to provide detailed images of any requested location in the world once every three days at a cost of as little as $100 per square mile. *See* Susan M. Jackson, *Cultural Lag and the International Law of Remote Sensing,* 23 BROOKLYN JOURNAL OF INTERNATIONAL LAW 853, 854 (1998).

46. Jackson, *supra* note 45, at 857.

47. *Id.* at 858.

48. On March 29, 1996, President Clinton announced a new policy to terminate the practice of degrading civil GPS signals within the next decade, allowing for a better signal for commercial and civilian users of the GPS. The policy expressly states that it is meant to reaffirm the US commitment to providing basic GPS services for peaceful civil, commercial, and scientific users. Press Release, President Opens Door to Commercial GPS Markets; Move Could Add 100,000 New Jobs to Economy by Year 2000, March 29, 1996.

49. Lane, The Satellite Revolution, *cited in* Steinberg, *supra* note 44, at 16.

50. G.A. Res. 1148, 12 U.N. GAOR Supp. (No. 18), at 195, U.N. Doc. A/3805 (1957), para. 1(f) ("the sending of objects through outer space shall be exclusively for peaceful and scientific purposes"); G.A. Res. 1348, 13 U.N. GAOR Supp. (No. 18), at 99, U.N. Doc. A/4090 (1958) ("outer space should be used for peaceful purposes only . . . .").

51. The words of a former Commander-in-Chief of USSPACECOM, General Howell M. Estes, are indicative of this view:

> I, as a military commander, have to say that somebody is going to threaten them (our space assets); and when they [do], we [should] have armed forces to protect them. . . . [I]f there was ever a threat to our national security [in space], the best – and only – way to solve the problem is to take weapons into space.

Cited in Jose Filho, *Total Militarization of Space and Space Law: The Future of Article IV of the '67 Outer Space Treaty*, PROCEEDINGS OF THE FORTIETH COLLOQUIUM ON THE LAW OF OUTER SPACE 358, 360 (1997).

52. G.A. Res. 1472 (Dec.12, 1959). Actually, COPUOS began as an Ad Hoc Committee on September 18, 1958. Its first report, adopted as Resolution 1348 on December 13, 1958, stressed that outer space should be used only for peaceful purposes. The next year, General Assembly Resolution 1472 made the Ad Hoc Committee a permanent UN committee.

53. Those four treaties are: (1) The Treaty on Principles Governing the Activities of States in the Exploration and Uses of Outer Space, including the Moon and Other Celestial Bodies (known as the Outer Space Treaty of 1967), *done* Jan. 27, 1967, 18 U.S.T. 2410, T.I.A.S. No. 6347; 610 U.N.T.S. 205, (*entered into force* Oct. 10, 1967); (2) Agreement on the Rescue of Astronauts, the Return of Astronauts, and the Return of Objects Launched into Outer Space (known as the Rescue and Return Treaty of 1968), *done* Apr. 22, 1968, 19 U.S.T. 7570, T.I.A.S. No. 6599, 672 U.N.T.S. 119, (*entered into force* Dec. 3, 1968); (3) The Convention on International Liability for Damage Caused by Space Objects (known as The Liability Convention of 1972), *done* Mar. 29, 1972, 24 U.S.T. 2389, T.I.A.S. No. 7762, 961 U.N.T.S. 187 (*entered into force* Sept. 1, 1972); and (4) The Convention on Registration of Objects Launched into Outer Space (known as The Registration Convention of 1975), *opened for signature* Jan. 14, 1975, 28 U.S.T. 695, T.I.A.S. No. 8480, 1023 U.N.T.S. 15 (*entered into force* Sept. 15, 1979). A fifth UN sponsored space treaty is The Treaty Governing the Activities of States on the Moon and Other Celestial Bodies (known as The Moon Treaty of 1979). It has only been ratified by 9 nations and none of the major space powers.

54. G.A. Res. 1721, U.N. Doc. A/5100 (1961). *See also* John E. Parkerson, Jr., *International Legal Implications of the Strategic Defense Initiative*, 116 MILITARY LAW REVIEW 67, 95 (1987).

55. U.N. Doc. A/5515 (1963).

56. The Committee has two standing Subcommittees of the Whole: the Scientific and Technical Subcommittee and the Legal Subcommittee. The Committee and two Subcommittees meet each year to discuss and study questions put to them by the General Assembly. They in turn make recommendations to the General Assembly and provide information from their meetings and studies in their annual reports. *See* the COPUOS web page at www.un.or.at/OOSA/copuos.html.

57. G.A. Res. 51/44 (Jan. 7, 1997).

58. *See* G.A. Res. 53/583 (Dec. 4,1998); G.A. Res. 52/56 (Feb. 12, 1998); G.A. Res. 51/123 (Feb. 10, 1997); G.A. Res. 51/122 (Feb. 4, 1997); and G.A. Res. 49/34 (Jan. 30, 1995). Also of interest is what these resolutions do not address: namely, the important contribution of military activity toward promoting international peace and security, such as reconnaissance satellite data that allows for the more effective verification of arms control agreements.

59. NATHAN C. GOLDMAN, AMERICAN SPACE LAW: INTERNATIONAL AND DOMESTIC 26 (2d ed. 1996). Goldman also notes that more nations became aware of the values of space and sought to join the committee to protect their interests. COPUOS tripled in size in 1982, from 18 members to 53. According to Goldman, the "drastic increase in size alone would guarantee a harder time for obtaining consensus."

60. *Id.* at 25.

61. The UN Charter does not grant the General Assembly legal authority to make binding substantive international law. *See* Andrei D. Terekhov, *UN General Assembly Resolutions and Outer Space Law,* PROCEEDINGS OF THE FORTIETH COLLOQUIUM ON THE LAW OF OUTER SPACE 97 (1997).

62. The following principles derived from the four major space treaties have also been generally accepted as reflecting customary international law:

(1) That outer space is free for exploration and use by all nations; that it is not subject to national appropriation by any means;

(2) That activities in outer space shall be conducted with due regard for the interests of other States;

(3) That States that launch space objects are liable for any damage they may do in space, in the air, or on the surface of the Earth. That there are two liability standards established for damage caused by "space objects;" a fault-based standard that applies to damage done to items in space and an absolute liability standard that applies to damage done on the surface of the earth or to aircraft in flight; and

(4) Outer space activities are subject to general principles of international law, including the UN Charter.

See Office of General Counsel, Department of Defense, An Assessment of International Legal Issues in Information Operations (Nov. 1999) [hereinafter DoD/GC Paper]. The paper is appended to this volume as the Appendix.

63. *See* Terekhov, *supra* note 61.

64. *See* the Conference on Disarmament web page at www.unog.ch/frames/disarm/disconf.htm.

65. P.K. MENON, THE UNITED NATIONS' EFFORTS TO OUTLAW THE ARMS RACE IN OUTER SPACE 65 (1988).

66. *Id.*

67. *Id.* at 66.

68. *Id.*

69. Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Limitation of Anti-Ballistic Missile Systems, *signed on* May 26, 1972, 23 U.S.T. 3435, 944 U.N.T.S. 13, TIAS 7503 (*ratified by the US on* Sept. 30, 1972); Rebecca Johnson, *Multilateral Arms Control: Can the CD Break the Impasse?*, www.armscontrol.org/ACT/novdec97/johnson.htm.

70. *See* Johnson, *supra* note 69, at 6.

71. *See* DoD/GC Paper, *supra* note 62.

72. China Defense White Paper, July 1998, http://russia.shaps.hawaii.edu/security/ china-defense-july1998.html (on file with authors).

73. *Id.* at 24.

74. *Id.*

75. In an article published in the *Liberation Army Daily*, official Chinese newspaper of the Communist Party-run political department of the Peoples Liberation Army (PLA), entitled "Bringing Internet Warfare Into the Military System Is of Equal Significance with Land, Sea, and Air Power," China seems to have changed its view about the use of information operations. According to the Beijing article, China is preparing to "carry out high-technology warfare over the Internet and could develop a fourth branch of the armed services devoted to information warfare." The article also stated:

> It is essential to have an all-conquering offensive technology and to develop software and technology for Net offensives so as to be able to launch attacks and countermeasures on the Net, including information-paralyzing software, information-blocking software, and information-deception software.

The article went on to apply this new means of warfare to outer space:

> Modern high-tech warfare cannot win without the Net, nor can it be won just on the Net. In the future there must be a coordinated land, sea, air, *space*, electronic and Net warfare, and the state's determination will be fully expressed in this mysterious theater space (emphasis added).

Quoted in Bill Gertz, *China Plots Winning Role in Cyberspace*, THE WASHINGTON TIMES, Nov. 17, 1999, at A1, A8.

76. Agenda item number 3, Report of the Conference on Disarmament to the General Assembly of the United Nations, at 2 (Sept. 8, 1998).

77. CD/1487, Working Paper Concerning CD Action on Outer Space (Jan. 21, 1998).

78. *Id.*

79. Space Policy, *supra* note 41, at 4 (Sept.19, 1996).

80. *See* Filho, *supra* note 51, at 358; *see also* Maurice N. Andem, *Implementation of Article IV of the Outer Space Treaty of 1967 During the 21st Century,* PROCEEDINGS OF THE FORTIETH COLLOQUIUM ON THE LAW OF OUTER SPACE 338 (1997).

81. Space Policy, *supra* note 41, at 1.

82. *Id.* at 5, para. (6)(b).

83. *Id.* at 5, para. (6)(a).

84. DoD Directive 3100.10, paragraph 4.3., states that "[t]he primary DoD goal for space and space-related activities is to provide operational space force capabilities to ensure that the United States has the space power to achieve its national security objectives . . . ." That includes assuring access to space (para. 4.3.1.2.) and ensuring that hostile forces cannot prevent our use of space (para. 4.3.1.4.).

85. Memorandum for Secretaries of the Military Departments, July 9, 1999, at 2 (on file with authors).

86. In September 1994, former Secretary of the Air Force Sheila Widnall stated, "Certainly, part of the Air Force mission is control of space, our ability to deny the use of space if necessary." Filho, *supra* note 51, at 359; General Joseph W. Ashy, former Commander-in-Chief of USSPACECOM, declared in 1996; "We are going to fight in space. Some people don't want to hear this, and it isn't in vogue. . . but – absolutely – we are going to fight in space." *Id.*

87. DoD Directive 3100.10, *supra* note 84, at para. 4.1.

88. Prohibited military activities in outer space that are specified in multilateral agreements include the following:

(1) placing nuclear weapons in earth orbit, on celestial bodies, or anywhere else in outer space (Article IV, paragraph 1, Outer Space Treaty);

(2) placing weapons of mass destruction in earth orbit, on celestial bodies, or anywhere in outer space (Article IV, paragraph 1, Outer Space Treaty);

(3) establishing a military base or installation on the moon or other celestial bodies (Article IV, paragraph 2, Outer Space Treaty);

(4) testing of any weapons on the moon or other celestial bodies (Article IV, paragraph 2, Outer Space Treaty);

(5) conducting military maneuvers on the moon or other celestial bodies (Article IV, paragraph 2, Outer Space Treaty);

(6) carrying out nuclear weapons explosions in outer space (Article I.1(a), Limited Test Ban Treaty);

(7) military or hostile use of environmental modification techniques that could produce a widespread adverse effect in either the earth's atmosphere or outer space (Articles I and II, Environmental Modification Convention).

89. Carl Rochelle, *Coming Soon: Global Navigation for Consumers,* March 29, 1996, www.cgi.cnn.com/US/9603/global_satellite/index.html.

90. White House Fact Sheet, U.S. Global Positioning System Policy, March 29, 1996, http://gauss.gge.unb.ca/policy/Fact_Sheet.

91. *Id.*

92. The Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space and Under Water ("The Test Ban Treaty"), *signed in Moscow* August 5, 1963, 14 U.S.T. 1313, 480 U.N.T.S. 43, T.I.A.S. 5433 (*entered into force* October 10, 1963).

93. 18 U.S.T. 2410, T.I.A.S. No. 6347, 610 U.N.T.S. 205, *signed in* Washington, London, and Moscow on January 27, 1967. Its full title is actually much longer: "The Treaty on Principles

Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies." This treaty was a byproduct of the Legal Subcommittee of COPUOS and was largely based on the Declaration of Legal Principles governing the Activities of States in the Exploration and Use of Outer Space, which had been adopted in 1963 by General Assembly Resolution 1962.

94. *See* Andem, *supra* note 80, at 339; *see also* MENON, *supra* note 65, at 43; Peter Jankowitsch, *Legal Aspects of Military Space Activities*, SPACE LAW DEVELOPMENT AND SCOPE 143, 146 (1992).

95. UN General Assembly Resolution 1884 (XVII) was approved by acclamation on October 13, 1963. *See* MENON, *supra* note 65, at 40. It was one of the earliest efforts to provide international legal guidance which related to the issue of interference with space systems. The Declaration was a UN effort to restrict a future arms race in space, even though the resolution had no binding legal effect. It set forth the principles of co-operation and mutual assistance, calling for nations to conduct their activities in outer space with due regard for the interests of other nations, it then stated the following about interference with space systems:

> If a State has reason to believe that an outer space activity or experiment planned by it or its nationals would cause potentially harmful interference with activities of other States in the peaceful exploration and use of outer space, it shall undertake appropriate international consultations before proceeding with any such activity or experiment. A State which has reason to believe that an outer space activity or experiment planned by another State would cause potentially harmful interference with activities in the peaceful exploration and use of outer space may request consultation concerning the activity or experiment.

While not prohibiting "harmful interference," the 1963 Declaration required prior consultations before a State could lawfully engage in that activity. The language of the Declaration, however, only protected activities from interference that were consistent with "the peaceful exploration and use of outer space." While clearly such general language could be seen as a limitation on some information operations, it would not preclude all information operations, especially those in response to an aggressive, hostile act of another State that was clearly outside the bounds of "peaceful exploration and use of outer space." Information operations in self-defense, for example, would not contravene the 1963 Declaration of Principles.

96. Gyula Gal, *The Peaceful Uses of Outer Space – After the Space Treaty*, PROCEEDINGS OF THE TENTH COLLOQUIUM ON THE LAW OF OUTER SPACE 129 (1967); *see also* BRUCE A. HURWITZ, THE LEGALITY OF SPACE MILITARIZATION 137 (1986); Mark G. Markoff, *The Judicial Meaning of the Term "Peaceful" in the 1967 Space Treaty*, PROCEEDINGS OF THE ELEVENTH COLLOQUIUM ON THE LAW OF OUTER SPACE 34 (1968).

97. HURWITZ, *supra* note 96, at 138.

98. Article 89, 1982 United Nations Convention on the Law of the Sea, U.N. Doc. A/CONF. 62/122 (1982), 21 I.L.M. 126–354 (1982).

99. This does not mean to imply that an assertion of sovereignty can only be done by means of an expressed statement. Certainly a nation can take actions which clearly express an intention to assert ownership over another nation's sovereign territory. However, the situation at issue here is a temporary interference with another nation's sovereign object. Actions that interfere with an object only *temporarily* are not likely to be construed as an assertion of sovereignty.

100. John C. Kunich, *Planetary Defense: The Legality of Global Survival*, 41 AIR FORCE LAW REVIEW 119, 129 (1997), *citing* W. Thomas Mallison, *The Laws of War and the Juridical Control of Weapons of Mass Destruction in General and Limited Wars*, 36 GEORGE WASHINGTON LAW REVIEW 308 (1967).

101. *See* Robert L. Bridge, *International Law and Military Activities in Outer Space*, 13 AKRON LAW REVIEW 649, 656 (1980) (referencing the Senate Foreign Relations Committee hearings on the Outer Space Treaty and the testimony of United Nations Ambassador Goldberg in response to

a question by Senator Carlson that a weapon of mass destruction "is a weapon of comparable ability of annihilation to a nuclear weapon, bacteriological . . . it does not relate to a conventional weapon.").

102. *See* Report of the Secretary-General, Developments in the field of information and telecommunications in the context of international security, U.N.G.A. 54/213 (Aug. 10, 1999). In response to an invitation to inform the Secretary-General of its views and assessments, the Russian Federation stated that "the use of information weapons against vital structures is comparable to the consequences of the use of weapons of mass destruction." Russia is also seeking support for a UN resolution "calling for new international guidelines and the banning of particularly dangerous information weapons. In comments submitted to the UN Secretary General published last month, Russia warned that information operations 'might lead to an escalation of the arms race.'" Bradley Graham, *Military Grappling With Guidelines For Cyber Warfare*, WASHINGTON POST, Nov. 8, 1999, at A10.

103. There is no official US government policy as to whether an information operation is a weapon of mass destruction. Anders Eriksson, a senior analyst with the Defence Research Establishment, Stockholm, Sweden, argues that information operations are neither weapons of mass destruction, nor disruption, but rather of "precision disruption." *See* Eriksson, *supra* note 6, at 1.

104. *See* Parkerson *supra* note 54 at 81. Within academic circles, there have been two primary views on whether the peaceful purposes language should have application at all to activities in outer space since the express reference to peaceful purposes is limited to "the moon and other celestial bodies." Those who advocate the broader interpretation look to other pertinent clauses in the preamble of the Outer Space Treaty. Advocates of a narrow interpretation note that when the treaty drafters wanted a provision to apply to outer space in other articles, they specifically used the words "outer space." Thus, the *absence* of the term "outer space" in the second part of Article IV, dealing with "peaceful purposes," is even more telling. *See* Morgan, *supra* note 19, at 300.

105. During the drafting of the Outer Space Treaty, delegations from India, Iran, Austria, Japan, Brazil, and Mexico tried to include language that would completely demilitarize outer space, but their proposals were rejected by both the Soviet Union and the US. Kunich, *supra* note 100, at 137; Parkerson, *supra* note 54, at 82.

106. *See* Morgan, *supra* note 19, at 240–241. The US view has been that use of outer space for self-defense constitutes a "peaceful purpose." *Id.* at n. 366. In addition, use of communication, navigation, remote sensing, and reconnaissance satellites have also become an accepted practice considered to be for "peaceful purposes." *Id.* at 308, 317.

107. *See* Douglas S. Anderson, *A Military Look into Space: The Ultimate High Ground*, ARMY LAWYER 19, 28 (1995); *see also* Morgan, *supra* note 19, at 299.

108. An excellent example is that cited by Parkerson *supra* note 54, at n. 99, referring to Professor Bin Cheng, who in stating that the treaty's language provides that "Antarctica shall be used for peaceful purposes only," fails to mention the additional clarifying language not included in the Outer Space Treaty. Antarctic Treaty, *done at* Washington, December 1,1959, 12 U.S.T. 794, 402 U.N.T.S. 71, T.I.A.S. 4780 (*entered into force* on June 23, 1961). Similarly, the UN Convention on the Law of the Sea also provides that the high seas shall be reserved for "peaceful purposes," yet there has been no attempt to prohibit military ships from the high seas. The practice of nation States demonstrates that the non-aggressive use of the high seas is consistent with a peaceful purpose. *See* Parkerson, *supra* note 54, at 84.

109. Parkerson, *supra* note 54.

110. Statement by the President of the United States on International Cooperation in Space, *reprinted in* Senate Committee on Aeronautics and Space Sciences; *see also* Kunich, *supra* note 100, at 136–137.

111. 42 US Code sec. 2451(a).

112. *See* Kunich, *supra* note 100, at 131; Anderson, *supra* note 107, at 27; Parkerson, *supra* note 54, at 82; Bridge, *supra* note 101, at 658.

113. See Bridge, *supra* note 101, at 658.

114. A more extreme view is held by Professor Mark G. Markoff, Professor of International Law, University of Fribourg, Switzerland, who believes that the Outer Space Treaty was intended to completely demilitarize space. According to Professor Markoff, all parties to the Outer Space Treaty have agreed, through Article I, not to engage in any space activity that is not in the common interest of all other nations. Since any military activity, even that for self-defense or other non-aggressive purposes, cannot be for the benefit of all nations, the Outer Space Treaty does not authorize any military activity in outer space. *See* Anderson, *supra* note 107, at 26; Parkerson, *supra* note 54, at 83.

115. *See* Parkerson, *supra* note 54, at 82; Morgan, *supra* note 19, at 303.

116. Rymn James Parsons, *The Fight to Save the Planet: U.S. Armed Forces "Greenkeeping" and Enforcement of the Law Pertaining to Environmental Protection During Armed Conflict,* 10 GEORGIA INTERNATIONAL ENVIRONMENTAL LAW REVIEW 441, 470 (1998). Historically, treaty obligations between belligerents were suspended during armed conflict between them. 2 OPPENHEIM'S INTERNATIONAL LAW: A TREATISE 302 (H. Lauterpacht ed., 7th ed. 1952). Currently, the compatibility of particular treaties during a state of armed conflict is assessed on a case-by-case basis. D. P. O'CONNELL, 1 INTERNATIONAL LAW 268 (2d ed. 1970); RESTATEMENT (THIRD), FOREIGN RELATIONS LAW OF THE UNITED STATES, sec. 336, Reporter's Notes, 221–22 (1986).

117. Many might argue that copying, diverting, modifying, or otherwise tampering with data of another does constitute "harm" and would be a violation of international law.

118. S.C. Res. 678 (Nov. 29 1990).

119. S.C. Res 1264 (Sept. 15 1999).

120. GOLDMAN, *supra* note 59, at 28. The organization had its beginnings in 1865 when co-operative regulations were initiated by the Geneva Telegraphic Convention in Paris. That first agreement was modified and extended, culminating in the ITU in 1932 as a result of the combining of similar conventions. *See* 1 MANUAL ON SPACE LAW 225, n. 1 (Nandasiri Jasentuliyana and Roy S.K. Lee eds., 1979).

121. GOLDMAN, *supra* note 59, at 28.

122. 1 MANUAL ON SPACE LAW, *supra* note 120, at 196.

123. SPACE LAW DEVELOPMENT AND SCOPE 23 (Nandasiri Jasentuliyana ed., 1992).

124. The US signed the Convention on December 22, 1992, and signed the 1994 amendments at Kyoto on October 14, 1994. For a discussion of the 1992 ITC and 1994 amendments, *see* Marian Nash (Leich), *Contemporary Practice of the United States Relating to International Law,* 91 AMERICAN JOURNAL OF INTERNATIONAL LAW 93 (1997).

125. Annex, para. 1003 of the 1992 ITC. This language is identical to that found in Annex 2, para. 2003 of the 1982 ITC.

126. Eilene Galloway, *International Institutions to Ensure Peaceful Uses of Outer Space,* IX ANNALS OF AIR & SPACE LAW 323 (1984).

127. The US position, according to Michael W. Zehner, Air Force Deputy General Counsel (International Affairs), follows the more restrictive language of the ITC provision. Interview with Mr. Zehner (Dec. 20, 1999).

128. *Supra* note 116. An interesting comparison can be made to virtually identical non-interference language contained in the 1982 UN Convention on the Law of the Sea (LOS Convention). In Article 19(2)(k), the LOS Convention prohibits "any act aimed at interfering with any systems of communication" during innocent passage in a foreign territorial sea. No one has argued that similar non-interference provisions contained in the LOS Convention apply during periods of lawful military activity.

129. GOLDMAN, *supra* note 59, at 50; *see also* Morgan, *supra* note 19, at 253.

130. GOLDMAN, *supra* note 59, at 53.

131. *Id.* at 50.

132. *Id.* at 53.

133. *Agreement Reached on Intelsat,* SPACE DAILY, Feb. 13, 1998, at 2; *see also* Morgan, *supra* note 19, at 293–94.

134. The former Defense Communications Agency (DCA), now called the Defense Information Systems Agency (DISA), concluded that although there is no restriction on the military use of "specialized" services, all currently offered INTELSAT services are considered "public telecommunications services" available to military forces for military purposes. Morgan, *supra* note 19, at 293–94.

135. Letter of Warran Y. Zeger, Vice President, Law Department, COMSAT World Systems Division (Feb. 3, 1989) (on file with authors). COMSAT is a public and private satellite corporation created by Congress in 1962 by the Communications Satellite Act, 47 US Code 701 *et seq,* and is the US representative to both INTELSAT and INMARSAT. *See* GOLDMAN, *supra* note 59, at 50. It is regulated by the Federal Communications Commission (FCC) and receives its instructions on how to vote on INTELSAT and INMARSAT issues from the US government. *See* Morgan, *supra* note 19, at n. 291.

136. Agreement Relating to the International Telecommunications Satellite Organization, 23 U.S.T. 3813, T.I.A.S. No. 7532 (1973).

137. For example, Article III sets forth the organization's prime objective to be that "the space segment required for international public telecommunications services . . . be available on a non-discriminatory basis to all areas of the world." Thus, interference through information operations with multidirectional channels such as telex, telephony, and data transmission would affect the availability on a non-discriminatory basis of international public telecommunications. *See,* Martin A. Rothblatt, *Satellite Communication and Spectrum Allocation,* 76 AMERICAN JOURNAL OF INTERNATIONAL LAW 56, 64 (1982).

138. *Supra* note 116.

139. SPACE LAW DEVELOPMENT AND SCOPE, *supra* note 123, at 102; *see also* 1 MANUAL ON SPACE LAW, *supra* note 120, at 441.

140. Unlike INTELSAT, which is limited in its membership to ITU members, INMARSAT is open to all nations. SPACE LAW DEVELOPMENT AND SCOPE, *supra* note 123, at 102.

141. *Id.* at 102; *see also* GOLDMAN, *supra* note 59, at 58.

142. Convention on the International Maritime Satellite Organization, *opened for signature* Sep. 3, 1976, 15 I.L.M.1051 (1976) (entered into force July 1976).

143. Guidelines for INMARSAT Convention, Article 3(3) (March 29, 1988), (filed with INMARSAT following consultation with Argentina, Belgium, Brazil, France, India, Italy, Japan, Netherlands, Oman, Singapore, UK, and USA), *reprinted in* Memorandum of Law on The "Peaceful Purposes" Requirement and Inmarsat use by Armed Forces, Wolf D. Von Noorden, Special Counsel to INMARSAT, June 29, 1994, *cited in* Walter Gary Sharp, Sr., *Revoking an Aggressor's License to Kill Military Forces Serving the United Nations: Making Deterrence Personal,"* 22 MARYLAND JOURNAL OF INTERNATIONAL LAW AND TRADE 1, n. 221 (1998).

144. Neal T. Kilminster, COMSAT General Counsel opinion (April 15, 1999) (on file with authors).

145. *Id.*

146. *Id.*

147. *Id.* at 2.

148. Article XV(2), Strategic Arms Limitation Talks (SALT II), Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Limitation of Strategic Offensive Arms, June 18, 1979; Article IX(2), Treaty Between the United States of America and

the Union of Soviet Socialist Republics on the Reduction and Limitation of Strategic Offensive Arms (START), July 31, 1991.

149. Roger D. Scott, *Legal Aspects of Information Warfare: Military Disruption of Telecommunications*, 45 NAVAL LAW REVIEW 57, 59 (1998).

150. Draft Joint Services Law of War Manual, para. 2.001 (unpublished 2d draft)[hereinafter LOW Manual]. Access to this draft is limited since it is still pending coordination and review.

151. Military necessity is codified in Article 23, para. (g) of the Annex to Hague IV, which forbids a belligerent "to destroy or seize the enemy's property, unless such destruction or seizure be imperatively demanded by the necessities of war." For an excellent discussion of this principle, including a historical perspective, see LOW Manual, *supra* note 150, at Chapter II.

152. DoD/GC Paper, *supra* note 62.

153. International and Operations Law Division, Office of The Judge Advocate General, Department of the Air Force, LAW OF ARMED CONFLICT TRAINING GUIDE (April 1993).

154. DoD/GC Paper, *supra* note 62.

155. Law of war treaties contain the caveat that the right of a party to a conflict is not unlimited in its selection and use of means or methods of war. The principle of avoiding the employment of arms, projectiles, or material of a nature to cause *superfluous injury,* also referred to as *unnecessary suffering,* is codified in Article 23 of the Annex to Hague IV. LOW Manual, *supra* note 150, at para. 2.003.

156. INTERNATIONAL LAW – THE CONDUCT OF ARMED CONFLICT AND AIR OPERATIONS, (AFP 110-31) 1–6, *cited in* Ariane DeSaussure, *The Role of the Law of Armed Conflict During the Persian Gulf War: An Overview*, 37 AIR FORCE LAW REVIEW 46–47 (1994).

157. DoD/GC Paper, *supra* note 62.

158. The Judge Advocate General's School, Operational Law Handbook 5-5 (2000).

159. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protections of Victims of International Armed Conflicts (Protocol I), art. 48, 1125 U.N.T.S.

160. *See* DoD/GC Paper, *supra* note 62. *See generally*, Protocol I, *supra* note 159, art. 43.

161. DoD/GC Paper, *supra* note 62. *See generally*, Geneva Convention Relative to the Treatment of Prisoners of War, art. 4(2)(b).

162. DoD/GC Paper, *supra* note 62.

163. AFP 110-31, *supra* note 156, para. 6-3a.

164. DoD/GC Paper, *supra* at note 62.

165. *Id.* at 6, 8.

166. Primer on Legal Issues in Information Operations, *supra* note 27, at 19.

167. DeSaussure, *supra* note 156, at 46–47.

168. LOW Manual, *supra* note 150, at para. 2.005.

169. DeSaussure, *supra* note 156, at 47.

170. DoD/GC Paper, *supra* note 62. Of course, ruses and the use of the element of surprise are not illegal acts. *See* LOW Manual, *supra* note 150, at para. 2.006.

171. Department of Defense, Doctrine for Joint Operations, JOINT PUB 3-0, (Feb. 1, 1995).

172. *See* Scott, *supra* note 149, at 60.

173. DoD/GC Paper, *supra* note 62. *But see* Roger D. Scott, *Territorially Intrusive Intelligence Collection and International Law,* 46 AIR FORCE LAW REVIEW 217 (1999); SHARP, *supra* note 6, at 125–133.

174. This is largely a recognition of the international law doctrine called *"tu quoque,"* in which "a nation has no standing to complain about a practice in which it itself engages." DoD/GC Paper, *supra* note 62.

175. This assumes that Nation A and Nation B are parties to those formerly bilateral agreements.

176. None of these agreements has any specific provision that indicates whether the parties intended that they apply during international armed conflict. It also appears that their provisions on harmful interference are inconsistent with a state of hostilities. *See* DoD/GC Paper, *supra* note 62.

177. RICHARD J. ERICKSON, LEGITIMATE USE OF MILITARY FORCE AGAINST STATE-SPONSORED INTERNATIONAL TERRORISM 144–145 (1989).

178. *Id.* at 144–146. The *Caroline* case is frequently cited as precedent in the customary international law of self-defense. A ship named the *Caroline* would periodically sail from the US to Canada to resupply the rebels there during Canada's 1837 revolt against the British. The British responded by entering the US, seizing the offending ship, and destroying it. The British claimed they acted in self-defense. Through correspondence with the British government on the incident, Secretary of State Daniel Webster set forth his understanding of the conditions necessary for self-defense. According to Webster, there "must be a necessity of self-defense, instant, overwhelming, leaving no choice of means and no moment for deliberation." Moreover, the act should involve "nothing unreasonable or excessive, since the act justified by the necessity of self-defense must be limited by that necessity and kept clearly within it." Webster's criteria of "necessity" and "proportionality" continue to form the basis of a lawful claim of self-defense. OPPENHEIM'S INTERNATIONAL LAW 420 (Robert Jennings and Arthur Watts eds., 9th ed. 1933); *see also* Richard G. Maxon, *Nature's Eldest Law: A Survey of a Nation's Right to Act in Self-Defense,* PARAMETERS, Autumn 1995, at 55, 56–57.

XV

Fourth Dimensional Intelligence

Thoughts on Espionage, Law, and Cyberspace

David M. Crane*

The enemy will be different. . . . No longer will it be the simple terrorist armed with an AK-47 or the Semtex bomb . . . the new threat will be groups who will bond in cyber space and attack using the new weapons of war: viruses, bugs, worms and logic bombs.[1]

The front cover of a recent *Armed Forces Journal* has an American soldier on a rope bridge suspended over a chasm with the title "Ready for What?"[2] This is a key question for national security policy makers regarding the mission of US Armed Forces as the world moves into the uncharted waters of the new millennium.[3]

Institutionally, the national security structure of the United States is facing many challenges. Configured to meet the Soviet threat, the Armed Forces, as well as the intelligence community, are realizing that changes must be made.[4] The question posed above, however, is relevant regarding the issue of being ready for the next threat. What are the threats that face our national security and how should we be organized functionally to meet those challenges, particularly as they relate to the dimension of cyberspace?

The geopolitical world of the 20th Century, drawn along colonial and ideological lines, is fading into the past. The threats faced by the United States today

are not just standing industrial age armies, but international criminals, terrorists, and State and non-State actors using relatively inexpensive and easily attained technology to manufacture weapons of mass destruction.[5]

Throughout history, man has waged warfare, conducted commerce, and established an international political regime in a three-dimensional environment. Mankind has faced and conquered the land, the sea, and the air above, moving freely about in these dimensions. Yet mankind has created another dimension which will shape its evolution well past the start of this millennium. That dimension is cyberspace. It is in this dimension that both the legal and intelligence communities, among others, will have to develop an ability to operate.

Among the practices of States, intelligence gathering is accepted as a necessity in conducting foreign relations.[6] Throughout history, State actors have been collecting information on the intentions, capabilities, and policies of both friendly and rival States.[7]

In the information age, intelligence plays an increasingly important role.[8] Information is the new strategic high ground. For the past fifty years or so the intelligence community of the United States focused on the Soviet Union and its allies, mainly the Warsaw Pact countries.[9] The mission was clear and the community organized itself accordingly to provide critical information to the National Command Authorities[10] on Soviet capabilities and intentions.[11] This organizational model, however, may no longer be valid.[12]

Due to the ever-increasing challenges in gathering that information against a hard target, the community began to rely more and more on its technical capabilities. Imagery intelligence and signals intelligence provided spectacular coverage and monitoring of Soviet communications and critical strategic targets.[13] At times this was at the expense of the other intelligence collection methods such as human-source intelligence (HUMINT).[14] In the asymmetric world of the 21st Century, HUMINT and open source intelligence (OSINT) will play a key role.[15] This role will not change in the dimension of cyberspace and computer network attack or defense.[16] Additionally, the computer will become a useful tool for an intelligence operative or analyst to use.[17]

Throughout our history, however, the role of intelligence in defending our nation has been misunderstood.[18] The methodologies of intelligence gathering can, to some citizens, appear to run counter to the basic principles of a free and open society.[19] Though Americans are fascinated by the capabilities of the community, they have an unrealistic romantic view of the often dangerous and dirty world of intelligence gathering.[20]

The Role of Intelligence in the United States

Until the Second World War, US intelligence played a minor role in protecting our national security. Only during time of war did an intelligence service emerge to support the commander in the field. After the emergency, the intelligence capabilities of the US diminished or were disbanded.[21]

Counterintelligence played even less of a role and was largely nonexistent prior to the First World War.[22] Domestically, the counterintelligence service became a profession in the 1920s with the advent of the Bureau of Investigation in the Department of Justice (later the Federal Bureau of Investigation) and the creation of various service counterintelligence organizations.[23]

The intelligence community has also had an awkward relationship with the Congress. Until the mid-1970s, Congress deferred to the executive branch on issues of national security as a constitutional prerogative of the President acting as Commander-in-Chief.[24] In the early 1970s, allegations of wrongdoing by the intelligence community caused a public outcry and resulted in long-term congressional and presidential scrutiny.[25] The result was the creation of the congressional intelligence oversight committees and presidential guidelines on the proper conduct of intelligence operations, particularly as they related to US persons.[26] Those policies and regulations are still in place and govern the intelligence activities discussed later in this chapter.

Thus, the US intelligence community truly was a creature of the Cold War designed to operate in three dimensions.[27] It was created and designed to counter Soviet hegemony, largely an industrial age threat. With the dissolution of the Soviet Union, and the advent of the information age, the intelligence community, a large and cumbersome bureaucracy, has to evolve into a quick reacting, forward thinking, and agile grouping of agencies ready to respond to various asymmetric threats, including computer network attack.[28]

The Challenges Ahead for US Intelligence and Cyberspace

The need for information by policy makers and warfighters will only increase. The National Command Authorities and the geographic Commanders-in-Chiefs will demand more real time intelligence for strategic and tactical planning.[29] The present reactive stance of the community will have difficulty providing current intelligence on the broad and diverse spectrum of transnational issues and threats. This reactive stance is exacerbated by two problems. The first is the organization of the community itself, the second, the management of the huge amount of data generated by the various intelligence agencies.[30] Overlaid on

these two problem areas is this fourth dimension of cyberspace, the battleground of the future.[31]

Though the current legal paradigm of international and domestic law regarding armed conflict was developed over the past few centuries, this evolved set of legal principles allows, for the time being, a practitioner sufficient leeway upon which to operate in the fourth dimension of cyberspace.[32]

In short, the major hurdles regarding espionage and computer network attack are not legal, but organizational and technical. Some of the legal challenges revolve around intelligence oversight and the collection of intelligence on US persons, as well as the law of war. The intrusive nature of computers and the Internet and their use as tools of espionage, and even warfare, cause legal scholars and practitioners in national security some concern, not from the lack of precedent, but of policy.

The Current Domestic Legal Framework

The current legal framework stems from statutory and regulatory guidance of the late 1970s, due to the improprieties by the US intelligence community in collecting information on US persons.[33] Centered on the National Security Act of 1947 and Executive Order 12333, intelligence organizations in the United States have been directed to follow certain prescribed procedures regarding the conduct of intelligence activities.[34]

The National Security Act of 1947, particularly Title V, gives authority for various departments and intelligence agencies to conduct intelligence gathering, laying out parameters as to what these organizations can or cannot not do in the process.[35] One of the key statutory conditions is to keep the Congress currently and fully informed on all intelligence activities being conducted.[36]

Executive Order 12333, signed by President Reagan, lays out the various missions of the intelligence community and gives specific guidance on how to conduct intelligence activities.[37] Each department promulgates and expands on this guidance through departmental regulations.[38] Additionally, there are internal policy directives that further refine the methods by which the intelligence community can collect this intelligence.[39]

These rules, coupled with international law, allow the intelligence agencies to operate properly in cyberspace. If given the proper mission and authority, intelligence organizations can collect information (conduct espionage) in this fourth dimension. These operations can be done in peacetime, pre-hostilities (intelligence preparation of the battlefield), and during armed conflict.

The challenge is developing policy that allows the community to conduct espionage in cyberspace. Proper guidance is essential to ensure that sources and methods are not compromised, the operational environment is secure, proper counterintelligence concerns are addressed and monitored, and there is proper oversight to ensure that the civil rights of US persons are not violated.

Some Policy Considerations

Operationally, cyberspace will pose the same challenges that a commander would face in a three-dimensional battle. Concepts of speed, mass, maneuver, surprise, taking the high ground, command and control, and forward support, among others, all apply in cyberspace. The Commander will need to be able to operate with as much familiarity and precision in this realm as he would on land, sea, or air— integrating all four dimensions seamlessly in achieving full spectrum dominance. He will also have to keep in mind, the four operational concepts espoused in the concept for future joint operations: dominant maneuver, precision engagement, full-dimensional protection, and focused logistics.[40]

Underlying all of the operational concepts listed above is the premise that new and emerging technologies will give joint US forces information superiority in any given mission. Information superiority is no longer a theory, but rather operational doctrine. Information superiority can be likened to the new high ground. A force that gains information dominance in the battlespace can shape it by making it not only more lethal for the adversary, but survivable for friendly forces.

A cornerstone in achieving this high ground is proper intelligence preparation of the battlespace itself using various methodologies, systems, and techniques to allow the commander to be dominant in his maneuver, precisely engaging the enemy in whatever dimension, supported by agile, innovative, focused personnel and organizations. Joint Publication 3-13, Joint Doctrine for Information Operations, describes intelligence preparation of the battlespace as ". . . the continuous process used to develop a detailed knowledge of the adversary system use of information and information systems."[41]

The intelligence community's challenge is to determine how far it can go to prepare that battlespace. Policy and operational concerns begin to surface as the transition takes place from a third dimensional conflict to operations in the fourth dimension of cyberspace. In attempting to understand the information environment, the operator will need knowledge of, *inter alia*, the adversary's information systems; political, economic, social, and cultural makeup; decision making process; geographic strengths and weaknesses; and biographical/psychological profiles.[42]

Methods to achieve proper intelligence preparation of the battlespace could be intrusive, thereby butting up against privacy and oversight restrictions that could hamper and even impede the gathering of this intelligence. Intelligence oversight and review organizations will have to be aware of, and add within their training and review methodologies, information operations, to include principles of computer network attack and defense.

The potential for the inadvertent violation of civil rights of US persons is great due to the intrusive capabilities of these tools.[43] It must be noted, however, that these intrusive techniques have existed for many years and the oversight rules are generally sufficient to ensure proper operational use. The term "least intrusive means" is a standard in intelligence collection, similar to the proportionality concepts found in the law of armed conflict.[44]

As intelligence organizations plan and execute operations to prepare the battlespace, policy makers will have to determine how far the intelligence operator can go to prepare for any situation along the conflict spectrum. Misinterpretation by a potential adversary that this preparation could be indeed an attack requires careful planning and oversight to ensure that there is no inadvertent response by an aggrieved party on our information or economic infrastructure.

Concluding Thoughts . . .

It is not constructive to change for change's sake. Faced with new issues, the law moves slowly, but in most instances the lapse of time allows for the controversy to ripen and be properly resolved.[45] In the past this could take years. In this day and age, where a "web-year" of three months governs the business of the information market, the law could quickly become irrelevant and certainly a hindrance to both commerce and possibly our national security.

Practitioners must balance the need for a careful development of the law in the area of information operations with the fast-paced reality of the information age. The intelligence community itself, like the legal profession, also must develop a strategic plan akin to the vision of the Department of Defense in order to move steadily forward in improving organizational structures and developing more collaborative and streamlined information systems to support operations in cyberspace.

Where all this will end up is anyone's guess. As in all things new, overreactive quick fixes will in the long run cause more confusion and potential harm to this nation's security. Additionally, treating information operations as a "different" operational tool for a commander in the field is a mistake. The doctrinal

and policy decisions by the Joint Staff to fully integrate information operations in operational planning are certainly steps in the right direction.

Operators and the legal community must continue to work for careful change domestically and provide leadership internationally to create appropriate rules in which future operations in cyberspace may be conducted within proper legal norms.

As former Secretary of Defense William Cohen declared:

> If you can shut down our financial system, if you could shut down our transportation system, if you could cause the collapse of our energy production and distribution system just by typing on a computer and causing those links to this globalization to break down, then you're able to wage successful warfare and we have to be able to defend against that.[46]

Notes

* The views expressed in this paper are solely the author's and do not reflect the position of the Inspector General or the Department of Defense.

1. JAMES ADAMS, THE NEXT WORLD WAR 15 (1998).

2. David L. Grange, *Ready for What?*, ARMED FORCES JOURNAL, Dec. 1999, at 42. The article itself focuses mainly on the readiness reporting system and how it reflects readiness to meet the challenging new missions facing US Armed Forces. For an excellent discussion of future warfare and the challenges facing the US Army, see ROBERT H. ECCLES, FUTURE WARFARE (1999).

3. *See generally*, The United States Commission on National Security/21st Century, New World Coming: American Security in the 21st Century (The Phase I Report on the Emerging Global Security Environment for the First Quarter of the 21st Century), Sept. 15, 1999. At page 7 the Commission states that the emerging security environment in the next quarter century will require different military and other national capabilities.

4. The Director of Central Intelligence, George Tenet, states in his (U)Strategic Intent for the Intelligence Community (S/NF) that "success in the 21st Century will require closer cooperation and more efficient use of our capabilities" (at 1).

5. There is an interesting development in the way nations/peoples prepare to fight technologically. The Tofflers in their book WAR AND ANTI-WAR, place these various methodologies in waves. Their premise is that throughout history man wages war the way he works. Consisting of three waves, the first wave centered around agriculture, the second wave on the industrial revolution, and the third on knowledge and information. Each had a profound affect on the way war was waged. *See generally*, ALVIN AND HEIDI TOFFLER, WAR AND ANTI-WAR (1993). Today all three waves exist simultaneously, a phenomenon generally not encountered in the past. For instance, in Somalia, information warriors have faced and have been challenged by agricultural workers fighting with spear and shield. This imbalance caused these highly technical soldiers to fight the Somalis on their terms, as technology/information operations proved ineffective against these first wave warriors. *See also* ROBERT W. CHANDLER, NEW FACE OF WAR (1998), which focuses on the impact of weapons of mass destruction and America's military strategy.

6. Espionage falls within the parameters of the inherent right of self- defense and is also lawful under the law of armed conflict. *See* NATIONAL SECURITY LAW 443 (John N. Moore et al., eds.

1990); Hague Convention IV Respecting the Law and Customs of War on Land, Oct. 18, 1907, Annex (Regulations), arts. 24, 29–31, 36 Stat. 2295, 1 Bevans 643.

7. JOHN P. FINNEGAN, THE MILITARY INTELLIGENCE STORY, at V (1994). *See generally*, GEORGE O'TOOLE, HONORABLE TREACHERY, (1991). In POWER SHIFT (1991), Alvin Toffler declares at page 289 that "Spies have been busily at work at least since the Egyptian Book of the Dead termed espionage a soul-endangering sin."

8. WAR AND ANTI-WAR, *supra* note 5, at 154. *See also* William Clinton, A NATIONAL SECURITY STRATEGY FOR A NEW CENTURY 24 (1998) and COMBATING PROLIFERATION OF WEAPONS OF MASS DESTRUCTION, Report from the Commission to Assess the Organization of the Federal Government to Combat the Proliferation of Weapons of Mass Destruction (1999), at 66.

9. *See* THE MILITARY INTELLIGENCE STORY, *supra* note 8, at 19. *See also* HONORABLE TREACHERY *supra* note 7, at 492–493; DAVID MURPHY ET AL., BATTLEGROUND BERLIN, at ix, 398 (1997).

10. The National Command Authorities (NCA) consist of the President and the Secretary of Defense collectively. *See generally*, 10 US Code § 162(b). The NCA is different than the National Security Council (NSC), created by the 1947 National Security Act, 50 US Code § 40. The NSC membership consists of the President, Vice President, Secretary of Defense, and the Secretary of State. Statutory advisors are the Chairman of the Joint Chiefs of Staff and the Director of Central Intelligence.

11. The intelligence community is composed of 13 agencies, including those in the Departments of Defense, Justice, Treasury, Energy, and State, as well as the Central Intelligence Agency (CIA). *See* OFFICE OF PUBLIC AFFAIRS, CIA, A CONSUMER'S GUIDE TO INTELLIGENCE, at vii and 28 (1999). The majority of assets and organizations are in the Department of Defense. These include the Defense Intelligence Agency, the National Imagery and Mapping Agency, the National Reconnaissance Office, and the National Security Agency, among others. The missions of the various agencies and intelligence components within the US intelligence community can generally be found in E.O. 12333, US Intelligence Activities, (December 4, 1981, 46 Federal Register 59941).

12. In WAR AND ANTI-WAR, *supra* note 5, at 154 the Tofflers state:

> Among all the "national security" institutions, none have a deeper need for restructure and reconceptualization than those devoted to foreign intelligence. Intelligence, as we've seen, is an essential component of any military knowledge strategy. But as the Third Wave war-form takes shape, either intelligence itself assumes a Third Wave form, meaning it reflects the new role of information, communication, and knowledge in society, or it becomes costly, irrelevant, or dangerously misleading.

See also THE NEXT WORLD WAR, *supra* note 1, at 258. Adams writes:

> As with so many things, the end of the Cold War and the advent of the Information Age caused a seismic shift in the world of espionage. Spy agencies needed a reason to be; although the need for intelligence had not lessened, the fact that most required knowledge was rapidly becoming available on the Internet meant that cloak and dagger was beginning to take second place to the drudge of reading and analyzing mountains of online reports.

13. *See generally*, VENONA: SOVIET ESPIONAGE AND THE AMERICAN RESPONSE 1939–1957 (Robert Benson and Michael Warner eds., 1996); THE MILITARY INTELLIGENCE STORY, *supra* note 7; HONORABLE TREACHERY, *supra* note 7; SHERRY SONTAG AND CHRISTOPHER DREW, BLIND MAN'S BLUFF (1998).

14. There are five basic intelligence sources, or collection disciplines: Signals Intelligence (SIGINT) includes information derived from intercepted communications, radar, and telemetry; Human-source Intelligence (HUMINT) derived information from both clandestine and overt

collections techniques; Imagery Intelligence (IMINT) which provides information from overhead and ground imagery; and Measurement and Signatures Intelligence (MASINT) is that information that comes from technical means other than imagery or SIGINT. A CONSUMER'S GUIDE TO INTELLIGENCE, *supra* note 11, at 2.

15. The Tofflers declare that "The Shift to a Third Wave intelligence system, paradoxically, means a stronger emphasis on human spies. . . . " WAR AND ANTI-WAR, *supra* note 5, at 158. They go on to say that "the Third Wave explosion of information and communication means that more and more of what decision makers need to know can be found in 'open' sources." *Id.* at 160. OSINT is information that is publicly available, as well as other unclassified information that has limited public distribution or access. Open source information also includes any information that may be used in an unclassified context without compromising national security or intelligence sources or methods.

16. WALTER GARY SHARP, SR., CYBERSPACE AND THE USE OF FORCE 124–125 (1999).

17. NATIONAL SECURITY LAW, *supra* note 6, at 438–42; Chairman of the Joint Chiefs of Staff, Joint Publication 3-13, Joint Doctrine for Information Operations, at I-9 & I-10 (1998) [hereinafter Joint Pub 3-13].

18. GEORGE CONSTANTINIDES, INTELLIGENCE AND ESPIONAGE 11 (1983).

19. HENRY L. STIMSON AND MCGEORGE BUNDY, ON ACTIVE SERVICE IN PEACE AND WAR 188 (1948). As Secretary of State, Stimson shut down the State Department's code breaking unit in 1929, remarking ". . . that gentlemen do not read other people's mail." *See also* HONORABLE TREACHERY, *supra* note 7, at 3. O'Toole asserts: "American gentleman have read other people's mail at every major turning of our national career. What is more, American gentlemen have proved to be very good at it." *Id.* at 3. President Harry Truman is attributed to have said during the signing of the National Security Act of 1947 that "intelligence and a free society do not mix."

20. Henry James captured the American attitude when he stated:

> American innocence contrasted with European subtlety and corruption. Americans are blunt, forthright, direct, ingenuous—all qualities acquired on the frontier and permanently incorporated in the American national character. Deviousness, secretiveness, indirection, and duplicity are, literally, foreign.

HONORABLE TREACHERY, *supra* note 7, at 3. Robert Gates, a former Director of Central Intelligence, writes:

> Presidents expect that, for what they spend on intelligence, the product should be able to predict coups, upheavals, riots, intentions, military moves, and the like with accuracy. . . . Presidents and their national security teams usually are ill-informed about intelligence capabilities; therefore they often have unrealistic expectations of what intelligence can do for them, especially when they hear about the genuinely extraordinary capabilities of U.S. intelligence for collecting and processing information.

Robert Gates, *An Opportunity Unfulfilled: The Use and Perceptions of Intelligence at the White House*, WASHINGTON QUARTERLY, Winter 1989, at 38–39.

21. *See generally*, THE MILITARY INTELLIGENCE STORY, *supra* note 7; HONORABLE TREACHERY, *supra* note 7; CHRISTOPHER M. ANDREW, FOR THE PRESIDENT'S EYES ONLY (1995).

22. Regarding the state of counterespionage in the US around the time of the First World War, Christopher Andrew states:

> No nation was less ready than the United States. Neither the Justice Department's Bureau of Investigation (the future FBI) nor the Treasury Department's Secret Service had much experience of counterespionage work. Each made matters worse by refusing to cooperate with the other.

FOR THE PRESIDENT'S EYES ONLY, *supra* note 21 at 30.

23. *See generally*, THE MILITARY INTELLIGENCE STORY, *supra* note 7; DAVID CRANE, COUNTERINTELLIGENCE COORDINATION (1995).

24. In 1966, Senator Daniel K. Inouye (Democrat, Hawaii), the first Chairman of the Senate Select Committee on Intelligence, declared:

> I recall when we came to classified programs, we would all look over at Richard Russell, the Chairman of the Armed Services Committee, and he would say, "I have discussed this matter with the appropriate officials and I have found everything is in order. . . ." But no one ever told us what was in order.

HONORABLE TREACHERY, *supra* note 7.

25. *See* Preparing for the 21st Century, An Appraisal of U.S. Intelligence, Report of the Commission on the Roles and Capabilities of the United States Intelligence Community, March 1, 1996, at A-14.

26. These committees are: The Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence. Both of these committees (generally known as the Intelligence Committees) were established in 1976.

27. HONORABLE TREACHERY, *supra* note 7, at 427. It is interesting to note that President Truman initially gave the job of creating a centralized organization to the Secretary of State, James Byrnes, who promptly tabled the idea where it languished for over a year. *See also*, FOR THE PRESIDENT'S EYES ONLY, *supra* note 21, at 149.

28. *See generally*, Joint Pub 3-13, *supra* note 17, at II-11. The Joint Staff pointedly declares that "offensive IO [information operations] require broad-based, dedicated intelligence support. Because intelligence support to offensive IO may require significant lead time and the effectiveness of many offensive capabilities is significantly improved by early employment, potential intelligence collection sources and access should be developed as early as possible." Computer network attack is defined in the same publication as "operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Also called CNA." *Id.* at glossary.

29. The combatant commands are statutorily created. 10 US Code § 161(a). Currently, there are nine combatant commands, five with geographic responsibility, e.g., Southern Command (SOUTHCOM), and four with functional responsibilities, e.g., Space Command (SPACECOM). 10 US Code § 164 lists the powers of a combatant commander who exercises combatant command (COCOM). *See* Chairman of the Joint Chiefs of Staff, Joint Publication 0-2, Unified Action Armed Forces (1995). The combatant commands are commonly referred to as the "warfighters." For an excellent overall summation of the roles and responsibilities of the NSC, NCA, and the combatant commands, see THE ARMY JUDGE ADVOCATE GENERAL'S SCHOOL, OPERATIONAL LAW HANDBOOK, Ch. 2, (2000).

30. *NIMA Infotech Retools U.S. Space Recon Ops*, AVIATION WEEK & SPACE TECHNOLOGY, Aug. 7, 2000, at 62.

31. Joint Vision 2010 states that information superiority is a key force multiplier and operational capability in future battlespace, providing full spectrum dominance to shape the strategic environment. *See* JOINT WARFIGHTER CENTER, CONCEPT FOR FUTURE JOINT OPERATIONS 35–36 (1997).

32. A concern is the attempt to create new rules for new technologies and ideas, without a proper understanding or consideration for the basic principles of international law and the law of armed conflict. Practitioners in the field of operational law in the armed services understand that in general the current legal regime allows for the proper conduct of information operations.

33. *See* Seymour M. Hersch, *Huge CIA Operations Reported in US Against Antiwar Forces*, NEW YORK TIMES, Dec. 22, 1974, at A1; The Evolution of the US Intelligence Community–An

Historical Overview, *in* Report of the Commission on the Roles and Capabilities of the United States Intelligence Community, at A-14 (1996).

34. E.O. No. 12333, *supra* note 11. In the introduction to E.O. 12333, President Reagan directs:

> Timely and accurate information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons, and their agents is essential to the national security of the United States. All reasonable and lawful means must be used to ensure that the United States will receive the best intelligence available.

35. 50 US Code 401 *et seq.* (cited as "National Security Act of 1947"). The preamble to the original act of July 26, 1947, declares:

> AN ACT to promote the national security by providing for a Secretary of Defense; for a National Military Establishment; for a Department of the Army, a Department of the Navy, and a Department of the Air Force; and for the coordination of the activities of the National Military Establishment with other departments and agencies of the Government concerned with the national security.

36. 50 US Code § 501.

37. Sect. 1.12, E.O. 12333, *supra* note 11.

38. The Department of Defense has published this guidance in DoD Directive 5240.1, DoD Intelligence Activities (Apr. 25, 1988); DoD Directive 5240.1R, Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons (July 1, 1982).

39. *See generally*, for example, Department of the Army Regulation 381-10, US Army Intelligence Activities (July 1, 1984), and Defense Intelligence Agency, Intelligence Law Handbook (Sept. 1995).

40. CONCEPT FOR FUTURE JOINT OPERATIONS, *supra* note 31, at Introduction.

41. Joint Pub. 3-13, *supra* note 17, at II-12. *See also* Chairman of the Joint Chiefs of Staff, Joint Publication 2-01.3, Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace (2000).

42. *Id.* at II-12-13.

43. A US person is defined as:

> . . . a United States citizen, an alien known by the intelligence agency concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments.

E.O. 12333, *supra* note 11, at para. 3.4.

44. For the principle of proportionality, *see generally*, US Army Field Manual 27-10, THE LAW OF LAND WARFARE at para. 41 (1956). Generally, the test is that the loss of life and damage to property incidental to attacks must not be excessive in relation to the concrete and direct military advantage expected to be gained. OPERATIONAL LAW HANDBOOK, *supra* note 29, at 7-4. Compare with the rule of least intrusive means found in E.O. 12333, *supra* note 11, at pt. 2.4 (implemented in DoD Directive 5240.1-R, *supra* note 38, Procedure 1, Sect. A.4, and Procedure 2, Sect. D), which states that the collection of information by a DoD intelligence component must be accomplished by the least intrusive means or lawful investigative technique reasonably available.

45. As Sophocles declared in *Oedipus Rex*, "Time eases all things."

46. Speech to the Veterans of Foreign Wars and the Ladies Auxiliary, *reported in* FEDERAL COMPUTER WEEK, Aug. 28, 2000.

XVI

Computer Network Attacks by Terrorists: Some Legal Dimensions

John F. Murphy*

Most of the contributions to this "Blue Book" focus on the possibility of computer network attacks by States as a methodology for so-called information warfare and the kinds of responses that may be taken consistently with the constraints of international law.[1] In this chapter, however, the focus shifts from the use of force by States to criminal acts committed by private individuals not under the sponsorship or control of a State. With this shift of focus, the applicable legal regime becomes international criminal law rather than provisions of the UN Charter governing the use of force and the maintenance of international peace and security.

To be sure, "international criminal law" is an area of considerable definitional ambiguity. Some eminent commentators have denied its very existence.[2] Other commentators, the majority, have defined international crimes as certain acts that constitute a crime against international law seeking only a tribunal with jurisdiction to apply that law and punish the criminal. Piracy is the prototypical example they cite. In response, the sceptics view piracy as solely a municipal law crime, the only question of international law being the extent of a State's jurisdiction to apply its criminal law to an accused foreigner acting outside the territorial jurisdiction of the prescribing State.[3]

Even for those crimes arguably constituting crimes under international as well as municipal law, it is necessary—in the absence of an international criminal court—to employ national law enforcement officials and national courts for purposes of apprehending, prosecuting, and punishing offenders. Accordingly, another dimension of "international criminal law" involves international cooperation in the enforcement of municipal criminal law. Although most efforts toward international cooperation in the enforcement of municipal criminal law have been on a bilateral or regional basis, the United Nations has played an increasingly important role in this area.

Considerable definitional ambiguity also surrounds the terms "terrorism" and "international terrorism." Despite strenuous efforts to do so, neither the United Nations nor its specialized agencies have been able to agree on a definition of "international terrorism."[4] Rather, as we shall see later in this chapter, the United Nations has adopted a piecemeal approach to the problem through the adoption of separate conventions aimed at suppressing particular manifestations of terrorism. Although these treaty provisions are often loosely described as "antiterrorist," the acts that they cover are criminalized regardless of whether, in a particular case, they could be described as "terrorism."

Even at the domestic level, as illustrated by the US experience, defining international terrorism is a tricky proposition. Under US law there are a variety of definitions that serve a variety of purposes.[5] Most important, at least at the federal level, there is no crime of "terrorism" per se. Rather, the Omnibus Diplomatic Security and Antiterrorism Act of 1986 provides US criminal jurisdiction over the killing of, or an act of physical violence with intent to cause serious bodily injury to or that results in such injury to, a US national outside the United States.[6] Although the relevant chapter of the Act is entitled "Extra-territorial Jurisdiction over Terrorist Acts Abroad against United States Nationals," there is no requirement that the killing or violent act include the traditional elements of a terrorist act. Instead, the legislation incorporates the elements of terrorism as a limitation on prosecutorial discretion:

> (e) LIMITATION ON PROSECUTION. No prosecution for any offense described in this Section shall be undertaken by the United States except on written certification of the Attorney General or the highest ranking subordinate of the Attorney General with responsibility for criminal prosecutions that, in the judgment of the certifying official, such offense was intended to coerce, intimidate, or retaliate against a government or a civilian population.

The conference report on the act makes it clear that the certification of the Attorney General or his designate is final and not subject to judicial review.[7] The report also clarifies the meaning of the term "civilian population" by noting that it "includes a general population as well as other specific identifiable segments of society such as the membership of a religious faith or of a particular nationality. . . ."[8] It is not necessary that either the targeted government or the civilian population be that of the United States.[9]

As a general working definition for this chapter, I shall employ the definitions of terrorism utilized by the US Government for statistical and analytical purposes since 1983:

- The term "terrorism" means premeditated, politically motivated violence perpetrated against noncombatant[10] targets by subnational groups or clandestine agents, usually intended to influence an audience.
- The term "international terrorism" means terrorism involving citizens or territory of more than one country.
- The term "terrorist group" means any group practicing, or that has significant subgroups that practice, international terrorism.[11]

International terrorism is not a new phenomenon, and it is a topic that has been subjected to substantial scholarly (and some not so scholarly) analysis. Accordingly, in preparing this chapter, I have asked myself what I would call the Monty Python question: does the prospect of computer network attacks by terrorists constitute something "completely different,"[12] or does it amount only to a new technique of attack for terrorists raising no new issues of law and policy? The answer, it appears, is that the possibility of computer network attacks does raise some new issues, although many of the old conundrums still pertain.

Efforts to combat international terrorism may take place at three different stages. The first, and ideal, stage is before a terrorist attack has occurred. Here the effort is to prevent a terrorist attack, either through the hardening of possible targets of terrorist attack or through intelligence work that allows law enforcement officials to learn of a planned attack in advance and intercept it.

The second stage involves responding to a terrorist attack while it is in progress, bringing it to an end, minimizing the damage it causes, and preventing panic among the general population. As we shall see, computer network attacks may present special challenges at this stage.

The third and last stage is where the perpetrators of the terrorist acts have succeeded in their mission, and it is necessary to apprehend them, submit them to prosecution before a tribunal with jurisdiction and fair procedures, and, if they are

found guilty, punish them. Here, too, computer network attacks may present special challenges.

In the sections that follow, I address some of the possible problems of combatting international terrorism at these three stages raised by the prospect of computer network attacks by terrorists. The final section sets forth some concluding observations.

Prevention

The Threat of Computer Network Attacks

Other chapters in this "Blue Book" discuss the nature of computer network attacks at great length and with substantial authority. No attempt is made to duplicate these efforts. Rather, this contribution attempts to discuss the concept of computer network attacks as a type of international criminal activity that might be engaged in by terrorists.

To this end it may be useful to distinguish, as Michael Schmitt has done in another context,[13] between computer network attacks and information operations. As explained by Schmitt, "information operations" should be defined expansively to "encompass, among an array of other activities, virtually any nonconsensual actions intended to discover, alter, destroy, disrupt, or transfer data stored in a computer, manipulated by a computer, or transmitted through a computer network."[14] Moreover, information operations are subdivided into defensive and offensive information operations. Computer network attacks fall within the latter category and consist of "(o)perations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."[15]

So defined, computer network attacks may take a variety of forms. They could be limited to the copying of sensitive data, which, depending on the circumstances, might constitute espionage, or include techniques for altering or destroying data and programs. Other computer network attacks might result in physical destruction, such as, most ominously, the "meltdown" of a nuclear reactor as a consequence of interference with its control system. Still other possible examples of computer network attacks have been suggested by Schmitt:

> 1. Trains are misrouted and crash after the computer systems controlling them are maliciously manipulated.
>
> 2. An information blockade is mounted to limit the flow of electronic information into or out of a target State.

3. Banking computer systems are broken into and their databases corrupted.

4. An automated municipal traffic control system is compromised, thereby causing massive traffic jams and frustrating responses by emergency fire, medical, and law enforcement vehicles.

5. Intrusion into the computer system controlling water distribution allows the intruder to rapidly open and close valves. This creates a hammer effect that eventually causes widespread pipe ruptures.

6. A logic bomb set to activate upon initiation of mass casualty operations is imbedded in a municipal emergency response computer system.[16]

As he recognizes, some of these examples are realistic while others may stretch credulity.

There is, moreover, the question of the technical capability of individual terrorists to engage in such computer network attacks without State support or sponsorship. In the past, the United States and other potential State targets of terrorist attack have benefitted from the relative technological incompetence of the terrorists.[17] For many years now, however, computer systems have been recognized as being especially vulnerable to terrorist attack.[18] And, in the words of one expert, "(t)he growing sophistication of high school students now entering college will ensure an ever greater pool of persons capable [of engaging in computer network attacks]."[19]

Another useful distinction to keep in mind is between those computer network attacks that (1) may cause disruption of vital systems leading to widespread inconvenience, possibly to some degree of public alarm, but that do not directly threaten life, and (2) those that directly threaten or appear directly to threaten human life.[20] Most computer network attacks are more likely to fall within the first category than within the second.[21]

A major difficulty facing all efforts to prevent or combat computer network attacks is that they can be carried out remotely and often from great distances. Since anyone can access the Internet from anywhere in the world, law enforcement officials may have no idea where the attacker is located. Under such circumstances, law enforcement officials will not know the motive behind the attack or the identity of the attackers. Even if they succeed in tracking the source of the attack to an Internet Service Provider (ISP), this ISP may be a mere conduit, or the attack may actually have originated with a subscriber to that service.

Hardening of Targets

Identification and hardening of critical targets of possible terrorist attack has long been recognized as a crucial step in preventing terrorist attack.[22] Virtually every major network—communications, electrical power, pipelines, and data—is vulnerable to terrorist attack. The vulnerability of many of these networks, however, depends on the would be attacker being able to identify the critical nodes. For example, taking out one refinery would have little effect on the oil industry. But attacks on certain pipelines could have devastating effects. Computer systems, on the other hand, are especially vulnerable, and "(i) it would not be difficult to seriously disrupt the Social Security System, nor would it be impossible to inflict vast harm to the Federal Reserve."[23]

This special vulnerability makes it especially difficult to harden computer networks against attack. Electronic vulnerabilities are often harder to guard than "traditional" vulnerabilities against terrorist attack. Part of the problem is the vastness and complexity of the information infrastructure. As of 1996, for example, the defense establishment reportedly had over 2.1 million computers, 10,000 local networks, and 100 long-distance networks.[24] Moreover, although it is clear that this infrastructure is subjected to a large number of attacks, the number of reported incidents is probably just the tip of the iceberg because, according to estimates, only about one in 150 attacks is actually detected and reported.[25] The same pattern is likely present in other sectors of the US Government and in the vast private sector.

Security technologies and products—such as, for example, firewalls[26] and smart cards[27]—may afford some protection, but they are hardly foolproof.[28] Additionally, as new security tools are developed, computer network attackers learn how to defeat them or exploit other vulnerabilities.

Human failings greatly compound the problem, as when inexperienced or untrained users accidentally publicize their passwords or weak passwords are chosen which can be easily guessed. Accordingly, it is generally agreed that training in information security for personnel, including top management, is a crucial element for a good information systems security program.[29]

Intelligence Operations

There is general agreement that the collection and use of intelligence is an effective tool in combating terrorism. Ideally, the gathering of intelligence serves a preventive role and enables law enforcement officials to intercept terrorists at an early stage, before they inflict injury on persons or property. However, even

with respect to terrorists who employ more conventional methods than computers, this has proven to be a difficult task to accomplish.

Problems may arise at the national level. In the United States, for example, there is evidence that constraints imposed on intelligence activities from 1975 to 1980 may have adversely affected the timing and availability of preventive intelligence to the extent that the proportion of cases in which violence or other crimes were prevented declined.[30]

The Fourth Amendment to the US Constitution prohibits unreasonable searches and seizures and clearly would apply to law enforcement searches of computer data bases in the United States.

The risk to privacy concerns would be especially great under such circumstances. The Foreign Intelligence Surveillance Act of 1978[31] regulates electronic surveillance of foreign powers and the agents of foreign powers and defines "foreign power" to include "a group engaged in international terrorism or activities in preparation therefor."[32] The act sets up a special court consisting of seven district judges who hear and determine applications for electronic surveillance warrants. The statute allows warrantless electronic acquisition of communications exclusively between foreign powers not involving a substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party.[33]

The United States Supreme Court has held that the Fourth Amendment does not apply to searches and seizures abroad of property owned by non-US citizens or permanent residents.[34] However, search and seizure of material located in computers abroad may be viewed by foreign sovereigns as a violation of their territorial sovereignty. Moreover, the standard techniques for obtaining criminal evidence abroad—letters rogatory and mutual legal assistance treaties, for example—are designed to assist in apprehending, prosecuting, and punishing those who have already committed crimes, not as a device to gather intelligence regarding the possible future commission of a crime.

Under these circumstances, then, cooperation between US and foreign intelligence officers would seem vital. Nonetheless, foreign laws protecting privacy are, if anything, more stringent than those of the United States. Therefore, in either the domestic or the international context, the challenge to balance privacy and individual rights concerns with the requirements of law enforcement is formidable.[35]

Management of an On-going Terrorist Incident

The goals of counter-terrorism efforts during an ongoing terrorist incident would at a minimum be threefold: (1) to bring the terrorist attack to an end;

(2) to minimize the damage caused by the attack; and (3) to prevent panic and restore order. A computer network attack by terrorists would probably complicate and make fulfillment of these goals more difficult.

This would especially be the case if the computer attack was widespread and well coordinated and involved both governmental and private sector targets. Suppose, for example, that simultaneous computer attacks disrupted the US command and control infrastructure so that individual military units were unable to communicate with each other or with a central command; air traffic control systems were also disrupted, causing planes to crash with substantial loss of life; a "computer worm" or "virus" traveled from computer to computer across a network, damaging data and causing systems to crash. Assume further that the sources of these attacks could not be easily located. The challenges facing authorities seeking to bring the attacks quickly to a halt and to prevent panic would be monumental.

Panic might be particularly pronounced because many otherwise informed people tend to dismiss the prospect of computer network attacks as a minor risk. According to Richard Clarke, the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism at the National Security Council:

> [CEOs of big corporations] think I'm talking about a 14-year-old hacking into their Web sites. I'm talking about people shutting down a city's electricity, shutting down 911 systems, shutting down telephone networks and transportation systems. You black out a city, people die. Black out lots of cities, lots of people die. It's as bad as being attacked by bombs. . . . Imagine a few years from now a President goes forth and orders troops to move. The lights go out, the phones don't ring, the trains don't move. That's what we mean by an electronic Pearl Harbor.[36]

Apprehension, Prosecution, and Punishment

Apprehension

Before a suspect can be apprehended, he or she must be located. As has often been noted elsewhere in this "Blue Book," computer network attackers can frustrate investigatory efforts by "looping and weaving" their attacks through several foreign countries, thus greatly complicating the efforts of investigators to follow their trail. If the suspect is located, it then becomes necessary to induce law enforcement officials of the place where he is located to take him into custody. They will not do so unless the computer network attack in question would

be a crime under their local law.[37] This requirement would also have to be met as a condition of extradition because of the "double criminality" requirement in virtually all extradition treaties.[38]

Prosecution and Punishment

If the suspect is apprehended abroad, the issue arises whether, and if so where, he will be prosecuted. At present, no multilateral antiterrorism convention expressly covers computer attacks.[39] However, depending on the circumstances, it is possible that one of the existing conventions—e.g., the Convention for Suppression of Unlawful Acts Against the Safety of Civil Aviation[40] or even the not yet in force International Convention for the Suppression of Terrorist Bombing[41]—could apply. If so, the extradite or prosecute approach that is the keystone of these conventions would govern the rights and obligations of the States parties.

Under this approach a State party that apprehends an alleged offender in its territory must either extradite him or submit his case to its own authorities for purposes of prosecution.[42] Strictly speaking, none of the antiterrorism conventions alone creates an *obligation* to extradite; by requiring the submission of alleged offenders for prosecution if extradition fails, they contain an *inducement* to extradite. Moreover, a legal basis for extradition is provided either in the convention or through incorporation of the offenses mentioned in the convention into existing or future extradition treaties between the parties. To varying degrees, the conventions also obligate the parties to take the important practical step of attempting to apprehend the accused and hold him in custody.[43]

The most important goal of these provisions is to ensure prosecution of the accused. To this end, the conventions state quite strongly the alternative obligation either to extradite or to submit the accused for prosecution. The obligation, however, is not to try the accused, much less to punish him, but to submit the case to be considered for prosecution by the appropriate national prosecuting authority. If the prosecuting State's criminal justice system lacks integrity, the risk of political intervention in the prosecution or at trial exists. Such intervention may prevent the trial or conviction of the accused, or act as a mitigating influence at the sentencing stage.

Even if the prosecuting State's criminal justice system functions with integrity, it may be very difficult to obtain the evidence necessary to convict the accused when the alleged offense was committed in another country. This very practical impediment to conviction can be removed only by patient and sustained efforts to develop and expand "judicial assistance" and other forms of

cooperation between the law enforcement and judicial systems of different countries. The conventions create an obligation to cooperate in this regard, but, as will be demonstrated in greater detail later, this obligation is often difficult for countries with different types of legal systems to meet, even assuming that they act in complete good faith. The difficulty may be even greater when cybercrime is involved.

Many, perhaps most, instances of computer network attack would not be covered by the antiterrorist conventions. In such cases, the United States would need to engage in a process of rendition to get the suspect before a US court. Besides extradition, the forms of rendition include exclusion, deportation, and abduction.[44] Subject perhaps to very limited exceptions, abduction is illegal,[45] and exclusion and deportation involve unilateral action by the State of refuge and are relatively informal measures subject to a relative lack of legal limitations. Extradition is generally recognized as the only process of rendition that satisfactorily protects the rights of an accused. Assuming that the United States did not wish or could not convince the State of refuge to deport the accused, it would try to extradite her. The obstacles to the success of this endeavor, however, could be considerable.

Barriers to Extradition

First, the requested country would be under no obligation to extradite absent an extradition treaty between it and the United States.[46] Although the United States is a party to more than 100 bilateral extradition treaties and to the Inter-American Convention on Extradition with 13 parties,[47] the absence of an extradition treaty has been a problem in some high profile cases.[48] Moreover, although the United States would be entitled to use most of the antiterrorist conventions for purposes of extradition, it has chosen not to do so.[49] The United States also will not itself extradite a person to a requesting country in the absence of an extradition treaty.[50]

Even with an extradition treaty, the extradition process is often fraught with difficulties. As already noted, many, if not most, US extradition treaties require that the action in question be a crime in both the requesting and requested country for extradition to take place. This dual criminality requirement can pose major problems in computer crime cases. Although the United States has amended its criminal code to penalize a wide range of computer crimes, other countries have been slow in doing the same.[51] This has resulted in cases where the United States has identified the location of a perpetrator of a computer crime, but has been unable to secure her extradition because the act in question was not a crime under the law of the country where the perpetrator was

found and the extradition treaty between the United States and the country in question contained a dual criminality requirement.[52] Although there is widespread recognition that countries need to reach a consensus as to which computer related activities should be criminalized, this is a process that will take some time.[53]

Under the extradition law of a number of countries, it is necessary for a requesting country to present the requested country with satisfactory (to the requested country) evidence that a crime covered by the treaty has been committed.[54] This has especially been the case with common law countries. Great Britain, for example, traditionally required prima facie evidence of a crime covered by the extradition treaty. For countries on the continent of Europe, which had no such requirement, this posed a "mystery" as to precisely how much evidence was required to meet this standard.[55] In 1982, approximately a third of the applications made to the United Kingdom under its extradition treaties failed and the most common cause of failure was the requesting State's inability to satisfy the prima facie requirement.[56] Because of this record of failure in the extradition process, Great Britain amended its extradition law in 1989 to exclude selectively the prima facie requirement in relation to certain States, and then ratified the European Extradition Convention, which has no such requirement.[57] Instead, the convention requires only that the request be accompanied by a certificate of conviction or the warrant for arrest, a statement of the offense and a copy of the necessary laws.[58] The US test of "probable cause," which requires only that there be reasonable grounds to make it proper that an accused be tried for the crime, has not proven to be a barrier to extradition.[59]

The prima facie requirement has been defended on the ground that it operates as a necessary protection for the individual who otherwise may be removed to another State merely because he is suspected of having committed a crime covered by the extradition treaty.[60] Be that as it may, there is no doubt that the prima facie requirement makes extradition more difficult. This difficulty may be especially great if computer network attacks are involved because the barriers to gathering evidence in such cases, as already noted, may be substantial.

Another barrier to the extradition of international terrorists may be the refusal of some countries, especially those with a civil law background, to extradite their nationals.[61] One of the grounds advanced by Libya in refusing to surrender two Libyan members of the Libyan secret service who were indicted by a grand jury of the District of Columbia in November 1991 for the December 1987 explosion of Pan Am flight 103 over Lockerbie, Scotland that killed 270 persons, including 189 Americans, was that the Libyan Constitution prohibited the extradition of Libyan nationals.[62]

The Austrian Supreme Court has gone so far to claim that the provision in the Austrian Constitution prohibiting the extradition of nationals reflected "a generally recognized rule of international law."[63] Even the government of the United Kingdom reserves the right not to extradite nationals where there is no extradition treaty with the requesting State and the latter is seeking the fugitive's return under a multilateral, antiterrorist convention.[64]

At least in Europe, however, the situation changed substantially in 1996, when the European Union concluded a Convention Relating to Extradition of Nationals.[65] The first paragraph of Article 7 of that convention provides that extradition may not be refused on the ground that the "person claimed is a national of the requested Member State." But the second and third paragraphs of Article 7 of the convention permit a five year rolling reservation allowing member States to refuse extradition of their nationals. According to Geoff Gilbert, the Explanatory Report "makes clear several matters:"

> [F]irst, that the Nordic members of the European Union will no longer classify domiciled aliens as nationals for the purposes of intra-EU extradition; secondly, that the protection of nationals might be achieved by those States which do not ordinarily extradite nationals, by entering a reservation that any sentence imposed by the requesting State will be served in the requested State; next, that given that some States are constitutionally prohibited from extraditing their own nationals, that they review the scope of the restriction at least once every five years; and, finally, that reservations are not indefinite and can lapse.[66]

In other words, even with the conclusion of the 1996 convention civil law countries resist extraditing their own nationals.

On the other hand, as to certain international crimes, there is some evidence that civil law States are beginning to relax their previous practice of never extraditing their nationals, at least in their extradition relations with common law States. For example, the 1983 extradition treaty between the United States and Italy specifically provides that extradition shall not be refused on grounds of nationality and is aimed at combatting the coordinated organized crime in the two countries.[67] Further, the increasing practice of repatriating prisoners to serve their sentences in their own country has reportedly convinced some civil law countries in Europe to extradite their nationals to common law countries.[68]

Outside of Europe there has also been some movement, albeit it slow and tentative. In 1979 the United States and Colombia concluded an extradition treaty that allowed for the surrender of nationals.[69] The treaty was a response to the inability of the United States to secure the extradition of Colombian

nationals who had imported illegal drugs, especially cocaine, into the United States and who had so corrupted Colombian law enforcement officials that trial in Colombia was not possible. The new extradition treaty was extremely unpopular in Colombia, however, and in 1988 the Colombia Supreme Court declared the treaty unconstitutional.[70] Repeated efforts by the United States resulted in Colombia passing a new law allowing for the extradition of its nationals in 1997,[71] and at this writing Colombia has extradited two drug suspects to the United States.[72]

Relations between the United States and Mexico concerning the possible extradition of Mexican nationals have been especially tortuous.[73] Under the US-Mexican Extradition Treaty,[74] neither party is required to extradite its nationals. Rather, Article 9 of the treaty gives both parties the option to prosecute as an alternative to extradition, and from 1978 until 1996 Mexico, as a matter of policy, refused to extradite its citizens to the United States.[75] Moreover, allegedly as a result of corruption among Mexican law enforcement officials, persons that the United States sought to extradite, especially for drug trafficking, were often not prosecuted in Mexico. Finally, in 1996, Mexico surrendered four of its citizens to the United States for prosecution, two of them for drug trafficking.[76] Nonetheless, since that time, Mexico's record, from the US perspective, has been unsatisfactory,[77] and there have been recent court challenges to the extradition of Mexican nationals that may have to be resolved by Mexico's highest court.[78]

Recognition by the requested country that the requesting country has jurisdiction to try the accused is a prerequisite to extradition. The complexity of civil and criminal jurisdictional issues in cyberspace, however, is just beginning to be recognized.[79]

In recent years, at both the state and the federal level, the United States has extended the death penalty to more and more crimes, including terrorist crimes.[80] By contrast, since World War II, opposition to the death penalty has resulted in many countries including clauses in extradition treaties that exclude extradition where the requesting State retains the death penalty and is unwilling or unable to provide assurances that this penalty will not be carried out if the accused is extradited.[81] This development has greatly complicated US extradition relations with other countries, including cases involving terrorist crimes.[82]

Another important development in recent years has been the increasing importance of human rights considerations as a limitation on extradition.[83] Opposition to the death penalty in the Western European States is based in large part on the belief that it violates fundamental human rights values. On the other hand, as noted by John Dugard and Christine Van den Wyngaert, "[t]oday states are irreconcilably divided over the morality and effectiveness of the death

penalty,"[84] and as a result its imposition is not prohibited by general international law. Under certain circumstances, however, according to some authorities, imposition of the death penalty may constitute cruel, inhuman, or degrading treatment or punishment, and thus violate general international law norms.

The best known of these authorities is the decision of the European Court of Human Rights in *Soering v. United Kingdom*.[85] Soering, a West German national, murdered his girlfriend's parents in Virginia and fled to the United Kingdom. In response to a US request, the United Kingdom ordered his extradition to the United States. Soering, however, petitioned the European Commission of Human Rights, which referred his case to the European Court of Human Rights. The court held that the United Kingdom had an obligation under Article 3 of the European Convention of Human Rights, which prohibits torture and inhuman or degrading treatment or punishment, not to extradite Soering to the United States where there was a real risk that he would be subjected to inhuman or degrading treatment by being kept on death row for a prolonged period in the state of Virginia. Eventually Soering was extradited to the United States when the United Kingdom received assurances from US officials that he would not be subjected to the death penalty.[86]

Although it is not a judicial body with authority to hand down a decision binding on parties to a dispute, the Human Rights Committee, which is the body established by the International Covenant on Civil and Political Rights[87] to supervise implementation of the covenant by States parties, found in *Ng v. Canada*[88] that California's practice of executing by gas asphyxiation, which might take over ten minutes to cause death, resulted in prolonged suffering constituting cruel and inhuman treatment within the meaning of Article 7 of the covenant. On the basis of this finding, the committee was of the opinion that Canada, which could reasonably have foreseen that Ng would be executed in this way, had violated its obligations under the covenant by extraditing him to the United States.

In 1980 Alona Evans identified the political offense exception, which is grounded, at least in part, in human rights considerations,[89] as the "hot issue" of extradition law.[90] At that time, the political exception was regarded as perhaps the primary barrier to the extradition of international terrorists.[91] But in recent years States have taken a variety of steps to limit or even to eliminate the political offense exception as a defense to extradition,[92] and it is unclear whether the political offense exception remains a major barrier to extradition at the present time.[93]

As an alternative to or a substitute for the political offense exception, extradition treaties may permit the accused to claim that he will not receive a fair trial in the requesting country. Article 3(a) of the United States-United Kingdom

Supplementary Extradition Treaty of 1985,[94] for example, expressly permits a judicial inquiry into whether the extraditee will be "prejudiced at his trial or punished, detained or restricted in his personal liberty by reason of his race, religion, nationality or political opinions." This so-called "humanitarian exception" was inserted because of the concern of some US Senators that the elimination of the political offense exception effected by the supplementary extradition treaty would result in inadequate protection for extraditees. By giving the courts the responsibility of ruling on allegations of an unfair trial, the treaty waters down the rule of noninquiry US courts normally apply, under which the courts defer to the executive branch to make the decision as to the validity of such allegations.[95] In practice, however, courts in the United States have been extremely reluctant to make a finding that would reflect on the standards of justice in the United Kingdom.[96] On the other hand, courts in both the United States and Canada have held that the rule of noninquiry is not absolute and that it will not be followed if the likely treatment in the requesting State would be shocking or simply unacceptable.[97]

As a result of these many barriers, the extradition process has been described as "a creaking steam engine of an affair."[98] Former US Attorney General Benjamin R. Civiletti was of the view that extradition laws belong to "the world of the horse and buggy and the steamship, not in the world of commercial jet air transportation and high speed telecommunications."[99] It is therefore not surprising that law enforcement officials have often turned to alternative forms of rendition in their efforts to bring alleged offenders to a forum for prosecution.

Alternatives to Extradition

One alternative to extradition that has been employed with some frequency in Europe is "hot pursuit."[100] This approach allows the police authorities of one State to cross the borders of a neighboring State in hot pursuit of a fleeing fugitive, and it is consistent with the policy of internal open borders that the European Union has followed since 1993. Also, the Schengen Accord of 1990,[101] concluded among Belgium, the Federal Republic of Germany, France, Luxembourg, and the Netherlands, allows the police agencies of the States parties to cross borders in hot pursuit, although the precise scope of this authority is a matter of dispute.[102] Outside of Europe, the doctrine of hot pursuit is apparently not widely utilized as a method of rendition.[103]

The methods of rendition most often utilized as alternatives to extradition are exclusion and deportation.[104] Exclusion may occur when fugitives are apprehended as they attempt to enter a country, and deportation may be an option

when fugitives are arrested within a country's territory. In US practice, not surprisingly, many of these exclusions and deportations have involved Canada and Mexico and have been directed towards persons accused of drug trafficking.[105] Both exclusion and deportation are civil processes, designed for immigration control and dominated by the executive. As a consequence, exclusion and deportation proceedings utilized for rendition purposes do not apply criminal justice standards, either with respect to the interests of the States involved or to protection of the accused. Unlike extradition, exclusion and deportation rarely involve a formal request by a State seeking a return of the alleged offender. On the contrary, exclusion and deportation are effected at the instance of a territorial State.[106]

Perhaps the most controversial use of deportation as an alternative to extradition was the case of Joseph Doherty. After unsuccessful attempts to extradite Doherty, a member of the Provisional Irish Republican Army, from the United States to the United Kingdom, where he was wanted for his role in the death of a British soldier and for his escape from prison, because of decisions by US courts that his offenses fell within the political offense exception in the US-UK extradition treaty,[107] the United States Supreme Court upheld his deportation to Northern Ireland after long and complicated legal proceedings.[108] Apparently, the deportation of Doherty was handled as a purely internal matter and not in response to a request from the United Kingdom that he be deported. Although some commentators have argued that it is improper for one State to request another to deport an individual as a means of circumventing extradition procedures, US courts have repeatedly held that the existence of an extradition treaty between the United States and another country does not bar the use of other means to obtain custody over a criminal located abroad.[109] In contrast, complicity between the French government and another government to use deportation as an alternative to extradition may reportedly be the basis for dismissal of the prosecution.[110]

The most controversial alternative to extradition has, of course, been abduction or kidnaping of alleged offenders. Both commentators and State practice support the general proposition that international law prohibits a State from sending its agents into another State to abduct an individual residing there without that other State's permission.[111] Abductions would seem prima facie to violate a principal rule of international law, which states that a nation is absolutely sovereign within the boundaries of its own territory.

There is at least an argument, however, that abduction may be consistent with international law under certain extraordinary circumstances. Despite the prohibition against the use of unilateral force in Article 2(4) of the UN Charter, Article 51 allows a victim of an armed attack to use force to defend itself pending

action by the Security Council.[112] Justification of a government sponsored abduction of a fugitive necessarily requires characterizing the actions of the fugitive as an "armed attack" within the meaning of Article 51.[113] This characterization has most often been applied to cases of terrorism and drug trafficking. In 1989, expressly repudiating an earlier opinion to the contrary in 1980,[114] then Assistant Attorney General William Barr produced a legal opinion that international law allowed US law enforcement officials to make extraterritorial arrests under certain circumstances.[115] Testifying before Congress, Barr stated on behalf of the Department of Justice:

> [T]here are instances where extraterritorial arrest without the host sovereign's consent may be justified under international law. For example, in response to an actual or threatened terrorist attack, we would have good grounds under general principles of international law to justify extraterritorial law enforcement actions over a foreign sovereign's objections. Moreover, in appropriate circumstances we may have a sound basis under international law to take action against large-scale drug traffickers being given safe haven by a government acting in complicity with their criminal enterprise. Thus, it may well be that the President will choose to direct extraterritorial arrests only when he believes that he is justified in doing so as a matter of self-defense under international law.[116]

The validity of Mr. Barr's proposition has been subject to sharp debate.[117] In practice, however, at least as of this writing, the US Government has made no extraterritorial arrests of alleged terrorists without the consent of the territorial sovereign. The 1987 sting operation that resulted in the apprehension of Fawas Younis took place on a US ship in the Mediterranean after Younis had been lured there by US agents.[118]

In contrast, the US Government has made extraterritorial arrests in drug trafficking cases.[119] The most controversial of these was the 1990 apprehension and deportation to the United States of Dr. Humberto Alvarez-Machain by Mexican agents paid by the US Drug Enforcement Agency (DEA). Dr. Alvarez-Machain was a prominent Mexican gynecologist who had been indicted for the kidnap and murder of Enrique Camarena, a DEA agent stationed in Guadalajara. After strong protests by the Mexican Government, and a circuit court opinion holding that the abduction violated the US-Mexico extradition treaty,[120] the US Supreme Court ruled that the abduction was not barred by the extradition treaty and that US courts could exercise jurisdiction over the case.[121] Although the majority opinion all but conceded by way of dicta that the abduction violated norms of customary international law,[122] the court did not address the issue

of whether this might constitute a basis for US courts to decline jurisdiction. Courts in several other countries have ruled that they have discretion in such circumstances to refuse to exercise jurisdiction.[123]

The Supreme Court's decision in *Alvarez-Machain* has been subjected to sharp criticism.[124] Be that as it may, Geoff Gilbert has suggested that, paradoxically, the Court's decision may "hasten the demise of State sponsored kidnaps of alleged international criminals, for it has brought to the fore this attempt to authorize the 'manifestly illegal.'"[125] Indeed, in the wake of *Alvarez-Machain*, the Bush Administration quickly responded with assurances that it had no intention of either increasing or institutionalizing the practice of extraterritorial abductions.[126] Also, in 1994, the United States and Mexico concluded a Treaty to Prohibit Transborder Abductions[127] (which, however, as of this writing has not yet been sent to the Senate for its advice and consent to ratification).

Mutual Assistance in Criminal Matters

Regardless of what method of rendition is used, once an accused is before a US court, it is necessary to prove his guilt beyond a reasonable doubt. But if the evidence to do this is located abroad, and cannot be obtained, the successful rendition of the accused may be a pyrrhic victory.

Moreover, the legal mechanisms for obtaining evidence abroad for use in criminal proceedings are less than satisfactory.[128] Letters rogatory, the standard mechanism, are especially ill-suited for obtaining evidence regarding computer crimes. Letters rogatory require an application to a foreign court and usually provide for advance notice and participation by opposing parties. Hence, the procedure is relatively public, as compared to the US practice of conducting criminal investigations under the veil of grand jury secrecy. It is, moreover, even under the best of circumstances extremely slow, and foreign tribunals may give limited or no assistance at the pre-indictment phase of a case. In any event, the decision of foreign tribunals to respond favorably is purely discretionary, since the letters rogatory practice is based on comity considerations rather than on binding international legal norms.

Because they create binding international legal obligations for the States parties, Mutual Legal Assistance Treaties (MLATs) may be of greater value. As of November 15, 1997, the United States had 23 MLATs in force.[129] They provide prosecutors with a channel for sending requests for assistance in obtaining evidence through a Central Authority in one country[130] to a corresponding prosecutorial authority in the other country, which oversees the prompt execution of the request. Under MLATs, foreign prosecutorial authorities will normally seek

mandatory process under their law, when necessary, to execute the request and keep it confidential to the extent possible.

The US MLATs contain a provision that obligates a requested country to conduct searches and seizures on behalf of a requesting country if the request includes information justifying such action under the laws of the requested country. Only a few of these MLATs, however, apply broadly to all law enforcement investigations and prosecutions, rather than only to certain types of offenses such as drug trafficking and money laundering. Additionally, the political offense exception is often available in MLATs and can be a barrier to obtaining the necessary evidence. Finally, even though the MLAT process is usually much faster than letters rogatory, as we have seen, evidence of computer crime can be rapidly transferred out of the jurisdiction of the requested country to other countries with whom the United States has no MLAT.

Especially for the collection of electronic evidence, MLATs, while an improvement on letters rogatory, are unequal to the task. The problem has been aptly posed by Michael Sussmann: "How does law enforcement collect electronic evidence that may be scattered across several different countries, can be deleted or altered with one click of a mouse, may be encrypted, and will ultimately need to be authenticated in another country's court?"[131] The ability to delete or alter electronic evidence with the click of a mouse renders even the relatively rapid procedures available under MLATs hopelessly slow and cumbersome. Accordingly, in Sussmann's view:

> [W]hen electronic evidence is sought, there may be a need for mechanisms such as a "preservation of evidence request" or "protected seizure," which would work as follows. Where there is a particularized concern about the loss of electronic evidence, a country would make an informal international request that the data immediately be preserved. This could be accomplished in a number of ways, from having a telecommunications carrier or ISP [Internet Service Provider] copy and store a customer's data, to actually seizing a criminal's computer and securing, but not searching, it for a short period of time. Once data is (sic) protected from loss, expedited processes would provide the foreign country with formal documentation to authorize the issuance of a domestic search warrant or similar process.[132]

As Sussmann notes, the US Code provides for a form of "preservation of evidence" request.[133] Most other countries apparently do not have such provisions in their laws, although the need for them has recently been recognized, at least in principle. Once such provisions are in place, it may be necessary to revise the

MLATs to ensure that the law enforcement officials of the other party to the treaty will be able to take advantage of them.

Transborder searches and seizures are an especially difficult problem when electronic evidence is involved. Although paper documents are normally located in the same country as the person being investigated, this is not necessarily the case with electronic evidence. To the contrary, electronic data may be stored in another country or countries to keep them beyond the reach of law enforcement.

Transborder searches consist of a law enforcement officer in his or her own country accessing a computer in another country to obtain electronic evidence.[134] Such searches may take place unknowingly. For example, if an investigator searches the computer of a domestic corporation, the data accessed through that search may be located in another country unbeknownst to the investigator. Unconsented to transborder searches of electronic evidence may be viewed by the country where the search occurs as a violation of its sovereignty or even of its criminal law, subjecting the individual investigator to possible criminal liability. From a law enforcement perspective, it is necessary for countries to agree on principles permitting transborder searches under clearly defined but broad circumstances.[135] Others may be of the view that the need to protect data in a particular country outweighs law enforcement concerns. Although this issue is currently being debated in several international forums, its outcome is far from certain.[136]

If an investigator succeeds in accessing electronic evidence, wherever it may be located, the evidence may be unintelligible because it is encrypted, i.e., scrambled to protect its confidentiality. The need for encryption is widely recognized as necessary to protect the confidentiality of e-mail traffic, stored data, and commercial transactions. However, when criminals use encryption for communications or data storage, they may severely hamper criminal investigations by preventing timely access to the content of seized or intercepted data. Hence, law enforcement officials are concerned that they be able to obtain the "keys" to decrypt encrypted data.[137] In contrast, privacy advocates, cyber-rights groups, and defense counsel, among others, oppose granting law enforcement broad authority in this area.

Moreover, according to Phillip Reitinger, the principal legal obstacle to law enforcement access to "plaintext" (i.e., unencrypted or decrypted text) and keys is the Fifth Amendment privilege against self-incrimination.[138] Reitinger concludes that a grand jury subpoena can order the production of the plaintext of encrypted documents and the production of documents that reveal keys. He further concludes, however, that whether law enforcement

can compel production of keys that are only known, rather than recorded, is an open question.[139]

At this writing, Congress has passed, and the President has signed, the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001."[140] This highly controversial legislation, which critics have argued could be used overzealously and harm innocent people,[141] provides, for the first time, for federal monitoring of computer communications, allowing investigators to track the sending and receiving of e-mail and Internet connections. They will not, however, be able to read the content of such computer communications without first obtaining a warrant. The legislation will also, among other things, allow investigators to conduct unannounced searches of property owned or occupied by terrorism suspects and to share information from federal criminal investigations with intelligence agencies for the first time.

There is also controversy over the efforts of law enforcement officials to secure laws that would permit them to sidestep encryption.[142] Regardless of how this debate is resolved, there is a need to reach agreement at the international level on decryption support services. As Michael Sussmann has pointed out, only the more modern of US MLATs contain provisions that are flexible enough to accommodate such newer forms of assistance as decryption services.[143] Even these MLATs do not specifically address the subject of decryption, and there currently are no international commitments to provide decryption support. Although there are discussions and negotiations underway in various international forums designed to resolve the problems of access to computers by law enforcement persons and encryption along with related issues, the final outcome of these efforts is uncertain at this writing.[144]

Some Concluding Observations

From the foregoing discussion, one may safely conclude that the prospect of computer network attacks by terrorists has only recently begun to receive the attention—from statesmen, law enforcement officials, and scholars—that it deserves. Moreover, although international terrorism has long been a subject of intense scrutiny, the prospect of computer network attacks by terrorists introduces legal and operational complications for those engaged in efforts to prevent, contain, and punish terrorist attacks.

Law and the legal process has traditionally lagged technological developments and the computer revolution is no exception. In particular, the speed with which computers operate and the anonymity of their operators create

challenges for the "snail pace" of traditional law enforcement methods. Also, as we have seen, at the domestic level in the United States there is currently a significant tension between the perceived needs of law enforcement and protection of the privacy rights of US citizens. At the international level this tension is likely to be as intense, perhaps even more, than it is in the United States, since the Europeans, for example, strongly emphasize the protection of privacy in their law and practice.[145]

Although there are strenuous efforts in various international fora to resolve these problems, including the adoption of a draft convention on computer crime under the auspices of the Council of Europe, the success of these endeavors is by no means assured. Nonetheless, it has long been a truism that international cooperation is crucial to successful efforts to combat international terrorism.[146] This truism applies *a fortiori* to efforts to combat computer network attacks by terrorists.

Moreover, international cooperation in combating terrorism has often taken the form of informal arrangements and liaisons between law enforcement officials in several countries, rather than the use of formal arrangements spelled out in treaties or national legislation. In view of the speed with which law enforcement personnel need to act to cope with a computer network attack, informality is likely to be required to give law enforcement the flexibility it needs to operate successfully. At the same time, the need for appropriate restraints on law enforcement of the kind provided by legal regulation is also great in the field of computer crime. The struggle to find the right balance is likely to continue for some time to come.

Notes

* The author would like to thank Brian T. Gorman, a graduate of Villanova University School of Law, for research assistance on this paper and Gregory Schaffer of the Division of Computer Crimes and Intellectual Property in the US Department of Justice for providing him with a copy of an article by his colleague, Michael Sussmann, prior to publication.

1. Although not appearing in this "Blue Book," Gregory Shaffer spoke on the "International Aspects of Computer Crimes" at the symposium on "Computer Network Attack and International Law" held at the Naval War College from June 25–29, 1999.

2. *See* Georg Schwarzenberger, *The Problem of an International Criminal Law*, 3 CURRENT LEGAL PROBLEMS 263 (1950).

3. For further discussion, see John F. Murphy, *International Crimes*, *in* 2 UNITED NATIONS LEGAL ORDER 993 (Oscar Schachter & Christopher C. Joyner eds., 1995); ALFRED P. RUBIN, THE LAW OF PIRACY 319–37 (1988).

4. *See* John F. Murphy, *Defining International Terrorism: A Way Out of the Quagmire*, 19 ISRAEL YEARBOOK OF HUMAN RIGHTS 13 (Yoram Dinstein ed., 1989).

5. *Id.* at 25–29.

6. 18 US Code §2331(c).

7. H.R. Rep. 99-783, 99th Cong., lst Sess. 88 (1986).

8. *Id.*

9. The reasons the Omnibus Diplomatic Security and Antiterrorism Act of 1986 dropped any reference to terrorism as an element of the offense itself are enlightening. These reasons have been well summarized by Geoffrey Levitt, formally an attorney in the Office of the Legal Adviser, Department of State, who worked on the act. Levitt first suggests that the political intent element characteristic of a "generic" definition of terrorism is inherently vague, and then states:

> In the US legal context, this flaw poses fundamental constitutional problems. The due process clause requires that criminal statutes "give a person of ordinary intelligence fair warning that his contemplated conduct is forbidden by the statute." When first amendment concerns are also involved, as they would of necessity be in any statute that included a politically oriented intent element, this requirement has even greater force. Even were such problems somehow resolved, the breadth of a generic intent element would severely complicate the task of prosecutors, who would be required to prove beyond a reasonable doubt the presence of a particular political motivation. Consequently, this would leave the Government open to accusations of selective prosecution based on the political views of defendants. A separate but substantial problem would be the likely absence of a similar intent element in the penal law of extradition treaty partners, thus removing the factor of dual criminality, a prerequisite to extradition—and one must wonder what the point would be of an international terrorism offense for which the United States could not successfully request the extradition of a suspected offender. . . .

Geoffrey Levitt, *Is "Terrorism" Worth Defining*, 13 OHIO NORTHERN UNIVERSITY LAW REVIEW 97, 113 (1986).

10. Under the US Government approach, the term "noncombatant" is "interpreted to include, in addition to civilians, military personnel who at the time of the incident are unarmed or not on duty. . . . We also consider as acts of terrorism attacks on military installations or on armed military personnel when a state of military hostilities does not exist at the site, such as bombings against US bases in Europe, the Philippines, or elsewhere." US Department of State, Patterns of Global Terrorism: 1998, April 1999, at vi, note 2.

11. *Id.* at vi–vii.

12. Monty Python fans will remember that their television show began with the proclamation "and now for something completely different."

13. *See* Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUMBIA JOURNAL OF TRANSNATIONAL LAW 885, 890 (1999).

14. *Id.* at 890.

15. *Id.* at 888.

16. *Id.* at 892–93.

17. *See, e.g.*, the summary of the remarks of J. Christian Kessler *in* JOHN F. MURPHY, LEGAL ASPECTS OF INTERNATIONAL TERRORISM; SUMMARY REPORT OF AN INTERNATIONAL CONFERENCE 45 (1980).

18. Summary of Remarks of Robert Kupperman *in id.* at 41–42.

19. Lawrence G. Downs, Jr., *Digital Data Warfare: Using Malicious Computer Code as a Weapon, in* ESSAY ON STRATEGY XIII (Mary A. Sommerville ed., 1999).

20. *See* MURPHY, *supra* note 17, at 35.

21. *See* Brian M. Jenkins and Alfred P. Rubin, *New Vulnerabilities and the Acquisition of New Weapons by Nongovernmental Groups, in* LEGAL ASPECTS OF INTERNATIONAL TERRORISM 221, 240 (Alona E. Evans and John F. Murphy eds., 1978).

22. Summary of Remarks of Robert Kupperman, *supra* note 18, at 42.

23. *Id.*

24. Information Security: Computer Attacks at Department of Defense Pose Increasing Risks, Abstracts of GAO Reports and Testimony, May 22, 1996, www.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=gao&docid=f:ai96084.txt, at 5.

25. *Id.*

26. "Firewalls are hardware and software components that protect one set of system resources (e.g., host systems, local area networks) from attack by outside network users (e.g., Internet users) by blocking and checking all incoming network traffic." *Id.* at 4, note 2.

27. "Smart cards are access cards containing encoded information and sometimes a microprocessor and a user interface. The encoded information and/or the information generated by the processor are used to gain access to a computer system or facility." *Id.* at 4, note 3 ¶ 28. On the contrary, according to a recent article, "there is no such thing as a secure computer network." Charles C. Mann, *The Mole in the Machine*, THE NEW YORK TIMES MAGAZINE, July 25, 1999, at 32. In this article, Mann quotes Eugene H. Spafford, Director of the Purdue Center for Education and Research in Information Assurance and Security, as stating: "The only system that is truly secure is one that is switched off and unplugged, locked in a titanium safe, buried in a concrete vault on the bottom of the sea and surrounded by very highly paid armed guards." *Id.*

29. *See* Abstracts of GAO Reports and Testimony, *supra* note 24, at 19, 23–24.

30. BRIAN JENKINS, SORREL WILDHORN & MARVIN LAVIN, INTELLIGENCE CONSTRAINTS OF THE 1970'S AND DOMESTIC TERRORISM (1982).

31. 50 US Code §§ 1801–08 (1994).

32. *Id.*, § 1801(a)(4).

33. *Id.*, § 1802(a)(1) (A)(1) and (B).

34. *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990).

35. To be sure, there are success stories. For example, according to the Washington Post, after the embassy bombings in Nairobi and Dar es Salaam, the United States revealed that, in 1997, it had successfully prevented two terrorist attacks on US embassies by infiltrating terrorist cells and intercepting electronic communications. *See* Walter Pincus & Vernon Loeb, *CIA Blocked Two Attacks Last Year, Washington Post*, Aug. 11, 1998, at A16.

36. Tim Weiner, *The Man Who Protects America From Terrorism*, NEW YORK TIMES, Feb. 1, 1999, at A3.

37. *See* Henry H. Perritt, Jr., *Jurisdiction in Cyberspace*, 41 VILLANOVA LAW REVIEW 1, 88 (1996). According to Michael Sussmann, a Senior Attorney in the Computer Crime and Intellectual Property Section of the US Department of Justice, in 1992 US efforts to get help from the Swiss in a case involving hackers from Switzerland who attacked the San Diego Supercomputer Center were stymied because of a lack of dual criminality. *See* Michael A. Sussmann, *The Critical Challenges from International High-Tech and Computer Related-Crime at the Millennium*, 9 DUKE JOURNAL OF COMPARATIVE & INTERNATIONAL LAW 455, 463 (1999).

38. For discussion, see GEOFF GILBERT, TRANSNATIONAL FUGITIVE OFFENDERS IN INTERNATIONAL LAW 104–16 (1998).

39. On June 29, 2001, however, a Draft Convention on Cyber-Crime was adopted under the auspices of the Council of Europe, and on September 19, 2001, was approved by the Council of Europe's Ministers' Deputies. The Convention will be open for signature by nonmember states that participated in the four year drafting exercise, including the United States, which has observer status at the Council of Europe. The convention is controversial, and it remains to be seen how many states become parties. See Council of Europe, *Draft Convention on Cyber-Crime and Explanatory Memorandum Related Thereto, Draft Explanatory Report* (June 29, 1001), http://www.conventions.coe.int/treaty/en/projects/finalcyberrapex.htm.

40. Convention for Suppression of Unlawful Acts Against the Safety of Civil Aviation, Sept. 23, 1971, 24 U.S.T. 565, T.I.A.S. No. 7570, 974 U.N.T.S. 177, 10 INTERNATIONAL LEGAL MATERIALS 1151 (1971).

41. The International Convention for the Suppression of Terrorist Bombing, 37 INTERNATIONAL LEGAL MATERIALS 249 (1998).

42. *See, e.g., id.*, art. 8.

43. *See, e.g., id.*, art. 7.

44. For further discussion, see John F. Murphy & Jon Michael Dumont, *The Rendition of International Criminals: Hard Cases Make Bad Law, in* FESTSKRIFT TILL JACOB W.F. SUNDBERG 171 (1993).

45. *See id.* at 179.

46. *See* JOHN F. MURPHY, PUNISHING INTERNATIONAL TERRORISTS 36 (1985).

47. *See* 18 US Code § 3181(1998) (listing treaties of extradition).

48. The absence of an extradition treaty between the United States and Libya was a complicating factor in US efforts to induce Libya to surrender two Libyan members of the Libyan secret service who were indicted by a grand jury of the District of Columbia in November 1991. See Christopher C. Joyner & Wayne P. Rothbaum, *Libya and the Aerial Incident at Lockerbie: What Lessons for International Extradition Law*, 14 MICHIGAN JOURNAL OF INTERNATIONAL LAW 222, 250–51 (1993).

49. *See* MURPHY, *supra* note 46, at 43.

50. *See* 18 US Code § 3181 and *Factor v. Laubenheimer*, 290 U.S. 276 287 (1933).

51. *See* Sussmann, *supra* note 37, at 464–65.

52. *Id.* at 463–64.

53. *Id.* at 464–65.

54. *See* GILBERT, *supra* note 38, at 119–27.

55. *Id.* at 119.

56. *Id.* at 120.

57. *Id.* at 120–21.

58. *Id.* at 121.

59. *Id.* at 123.

60. *Id.* at 126.

61. *Id.* at 175–84.

62. *See* Joyner & Rothbaum, *supra* note 48, at 250–51.

63. As quoted *in* GILBERT, *supra* note 38, at 176.

64. *Id.* at 177.

65. European Union Convention Relating to Extradition between the Member States of the European Union, Sept. 27, O.J. (C313) 02.

66. *Id.* at 179.

67. *See* US-Italy Extradition Treaty, Oct. 13,1983, art. IV, T.I.A.S. No. 10837 (entered into force Sept. 24, 1984).

68. GILBERT, *supra* note 38, at 180.

69. US-Colombia Extradition Treaty, Sept. 14, 1979, (entered into force March 4, 1982), Hein's No. KAV 338.

70. *See* GILBERT, *supra* note 38, at 179–80.

71. *Id.* at 180, note 19.

72. *See Colombia Extradites Drug Suspect to the U.S., the Second in Days*, NEW YORK TIMES, Nov. 26, 1999, at A25.

73. For discussion, see Argiro Kosmetatos, *U.S.-Mexican Extradition Policy: Were the Predictions Right about Alvarez?*, 22 FORDHAM INTERNATIONAL LAW JOURNAL 1064 (1999); Bruce Zagaris & Julia Padierna Peralta, *Mexico-United States Extradition and Alternatives: From Fugitive*

Slaves to Drug Traffickers—150 Years and Beyond the Rio Grande's Winding Courses, 12 AMERICAN UNIVERSITY JOURNAL OF INTERNATIONAL LAW & POLICY 519 (1997).

74. US-Mexico Extradition Treaty, May 4, 1978, 31 UST 5059; T.I.A.S. No. 9,656, entered into force Jan. 25, 1980.

75. *See* Kosmetatos, *supra* note 73, at 1066.

76. *Id.*

77. *Id.*

78. *See* Rodrigo Labardini, *Mexico Extradites Major Drug-Trafficker to the U.S. and Recent Developments in the U.S.-Mexico Extradition*, 15 INTERNATIONAL ENFORCEMENT LAW REPORTER 315 (1999).

79. For an excellent discussion of these issues, see PERRITT, *supra* note 37.

80. *See* Jeffrey C. Matura, *When Will It Stop: The Use of the Death Penalty for Non-Homicide Crimes*, 24 JOURNAL OF LEGISLATION 249, 259 (1998).

81. *See* GILBERT, *supra* note 38, at 155–69.

82. In the *Venezia* case, an Italian court suggested that the assurances by the United States that the death penalty would not be imposed was an insufficient guarantee, since such assurances by the executive could not bind the judiciary. *Venezia v. Ministero di Grazia e Giustizia*, Corte cost., June 27, 1996, n. 223, 79 *Rivista Di Diritto Internazionale* 815 (1996). For discussion, see Andrea Bianchi, case note, 91 AMERICAN JOURNAL OF INTERNATIONAL LAW 727 (1997).

83. *See* John Dugard & Christine Van den Wyngaert, *Reconciling Extradition with Human Rights*, 92 AMERICAN JOURNAL OF INTERNATIONAL LAW 187 (1998).

84. *Id.* at 197.

85. 161 Eur. Ct. H.R. (ser.A) (1989).

86. *See* FRANK NEWMAN & DAVID WEISSBRODT, INTERNATIONAL HUMAN RIGHTS 477 (2d ed. 1996).

87. 999 U.N.T.S. 171, 6 INTERNATIONAL LEGAL MATERIALS 368 (1967).

88. 98 INTERNATIONAL LAW REPORTS 479 (1993).

89. As Christine Van den Wyngaert has pointed out, the political offense exception has a humanitarian basis in that it is viewed as protection against an unfair trial in the requesting State which, as the target of the political crime, might be inclined to function as both judge and jury. CHRISTINE VAN DEN WYNGAERT, THE POLITICAL OFFENSE EXCEPTION TO EXTRADITION 2 (1980). At the same time, she criticizes this rationale on the ground that it is not always true that political offenders are likely to be subject to an unfair and partial trial. *Id.* at 4.

90. Alona E. Evans, *International Procedures for the Apprehension and Rendition of Fugitive Offenders*, [1980] AMERICAN SOCIETY OF INTERNATIONAL LAW PROCEEDINGS 244.

91. For further discussion, see MURPHY, *supra* note 46, at 45–70.

92. *See* International Law Association: Helsinki Conference 216, 224 (1996) (Committee on Extradition and Human Rights Second Report).

93. According to the ILA Report, "today the political offence exception is not accepted in a wide range of circumstances." *Id.* at 224.

94. June 25, 1985, T.I.A.S. No. 12,050, as amended.

95. *See* Dugard & Van den Wyngaert, *supra* note 83, at 190.

96. *Id.*, noting *In re Requested Extradition of Smyth*, 61 F. 3d 711,722 (9th Cir. 1995); *In re Extradition of Howard*, 996 F. 2d 1320,1331–33 (1st Cir. 1993).

97. *Id.*, noting several US and Canadian decisions.

98. *See* GILBERT, *supra* note 38, at 1, *quoting* THE OBSERVOR, April 29, 1979, at 4.

99. *Quoted in id.* at 1.

100. *Id.* at 363.

101. *See* 30 INTERNATIONAL LEGAL MATERIALS 84 (1991).

102. GILBERT, *supra* note 38, at 363.

103. There is no discussion of cases outside of Europe in GILBERT, and the doctrine of hot pursuit is not even mentioned by Nadelmann in Ethan Nadelmann, *The Evolution of United States Evolution in the International Rendition of Fugitive Criminals*, 25 NEW YORK UNIVERSITY JOURNAL OF INTERNATIONAL LAW & POLICY 813 (1993), perhaps the most extensive recent examination of methods of rendition.

104. GILBERT, *supra* note 38, at 376.

105. Nadelmann, *supra* note 103, at 860.

106. *See generally*, GILBERT, *supra* note 38, at 364–77.

107. *See In Re Doherty*, 599 Supp. 270 (S.D.N.Y. 1984), appeal dismissed *sub nom. United States v. Doherty*, 615 F. Supp. 755 (S.D.N.Y.1985), aff'd, 786 F. 2d 491 (2d Cir. 1986).

108. *INS v. Doherty*, 502 U.S. 314 (1992). For discussion of this extraordinary case, see Joseph Kelley, *The Empire Strikes Back: The Taking of Joe Doherty*, 61 FORDHAM LAW REVIEW 317 (1992).

109. *See, e.g., United States v. Reed*, 639 F.2d 896, 902 (2d Cir. 1981).

110. CHRISTOPHER L. BLAKESLEY, TERRORISM, DRUGS, INTERNATIONAL LAW, AND THE PROTECTION OF HUMAN LIBERTY 279 (1992).

111. In the words of the Restatement (Third) of the Foreign Relations Law of the United States: "A state's law enforcement officers may exercise their functions in the territory of another state only with the consent of the other state, given by duly authorized officials of that state." RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES, § 432(2).

112. UN CHARTER art. 2(4):

> All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.

UN CHARTER art. 51:

> Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security. Measures taken by Members in the exercise of self-defense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.

113. The International Court of Justice, in *Nicaragua v. United States*, 1986 I.C.J. Rep. 14, para. 195, stated, "[i]n the case of individual self-defense, the exercise of this right is subject to the State concerned having been the victim of an armed attack."

114. Extraterritorial Apprehension by the Federal Bureau of Investigation, 4B Opinion, Office of Legal Counsel 543 (1980), reprinted in FBI Authority to Seize Suspects Abroad: Hearing Before the Subcommittee On Civil and Constitutional Rights of the Committee On the Judiciary, House of Representatives, 101st Cong., 1st Sess. 75 (1989).

115. Authority of the Federal Bureau of Investigation to Override Customary or Other International Law in the Course of Extraterritorial Law Enforcement Activities, 13 Opinion, Office of Legal Counsel 195 (1989). *See* FBI Authority to Seize Suspects Abroad, *supra* note 114, at 2-21, 59–71.

116. FBI Authority to Seize Suspects Abroad, *supra* note 114, at 2–21 (Statement of William Barr, Assistant Attorney General).

117. *See, e.g.*, Andreas F. Lowenfeld, *U.S. Law Enforcement Abroad: The Constitution and International Law*, 84 AMERICAN JOURNAL OF INTERNATIONAL LAW, 444, 488 (1990) ("There

is no suggestion in any of the background of Article 51 or the massive writing on that article that it can be used to justify law enforcement directed against individual suspects located in another state.").

118. For a brief discussion of the Younis case, see Nadelmann, *supra* note 103, at 866.

119. *Id.* at 870–74.

120. *United States v. Alvarez-Machain*, 946 F. 2d 1466 (9th Cir. 1991).

121. *United States v. Alvarez-Machain*, 504 U.S. 655 (1992).

122. *Id.* at 669. ("Respondent and his Amici may be correct that respondent's abduction was 'shocking' . . . and that it may be in violation of general international law principles . . . Mexico has protested the abduction of respondent through diplomatic notes . . . and the decision of whether respondent should be returned to Mexico, as a matter outside of the Treaty, is a matter for the Executive Branch.")

123. *See* Murphy & Dumont, *supra* note 44, at 206–08; GILBERT, *supra* note 38, at 352–60.

124. *See generally, Agora: International Kidnaping*, 86 AMERICAN JOURNAL OF INTERNATIONAL LAW 736 (1992); Murphy & Dumont, *supra* note 44. *Per contra*, see Malvina Halberstam, *In Defence of the Supreme Court Decision in Alvarez-Machain*, 86 AMERICAN JOURNAL OF INTERNATIONAL LAW 736 (1992).

125. GILBERT, *supra* note 38, at 352.

126. Tim Golden, *Bush Gives Mexico Limited Pledge on Abductions*, NEW YORK TIMES, July 2, 1992, at A5.

127. Treaty to Prohibit Transborder Abductions, Nov. 23, 1994, US-Mex., 31 U.S. T. 5059, *reprinted in* MICHAEL ABBELL & BRUNO A. RISTAU, 4 INTERNATIONAL JUDICIAL ASSISTANCE: CRIMINAL 13-4-1, at A-676.3 (Supp.1995).

128. For general discussion of MLATs, see ETHAN A. NADELMANN, COPS ACROSS BORDERS 312–96(1993).

129. US Department of State, Bureau for International Narcotics Control and Strategy Report vii (1998).

130. The Criminal Division's Office of International Affairs of the Department of Justice serves as the Central Authority for all US MLATs.

131. Sussmann, *supra* note 37, at 472.

132. *Id.* at 473.

133. *Id.* The US Code provision is 18 US Code § 2703(f)(1) (1994).

134. *Id.* at 474.

135. *Id.* at 475.

136. *Id.*

137. *Id.* at 475–76.

138. Phillip R. Reitinger, *Compelled Production of Plaintext and Keys*, UNIVERSITY OF CHICAGO LAW FORUM 171 (1996).

139. *Id.* at 173. *See also* David Goldstone & Betty-Ellen Shave, *International Dimensions of Crimes in Cyberspace*, 22 FORDHAM INTERNATIONAL LAW JOURNAL 1924 (1999).

140. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56,115 Stat. 272 (2001).

141. *See, e.g.*, the October 19, 2001, report of Silicon Valley.com, http://www.siliconvalley.com/bin/printpage.pl.

142. Robert O'Harrow, Jr., *U.S. Wants Authority to Disable PC Security*, PHILADELPHIA INQUIRER, Aug. 21, 1999, at A 1 (reprinting article from the Washington Post).

143. Sussmann, *supra* note 37, at 476, note 78. As an example, Sussmann notes that Article 1, paragraph 2(h) of the US-UK MLAT provides for "such other assistance as may be agreed between Central Authorities."

144. *Id.* at 478–90.

145. *See, e.g.*, the European Union's Council's Directive 95/46/EC on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L281) 31. For an analysis of the EU directive, see Rosario Imperiali d'Afflitto, *European Union Directive on Personal Privacy Rights and Computerized Information*, 41 VILLANOVA LAW REVIEW, 305 (1996).

146. For an exploration of this theme, see John F. Murphy, *The Need for International Cooperation in Combatting Terrorism,* 15 TERRORISM 381 (1990).

XVII

Meeting the Challenge of Cyberterrorism: Defining the Military Role in a Democracy

Charles J. Dunlap, Jr.*

Headline grabbing events like the denial of service attacks[1] on "dot com" companies[2] in early 2000 and the excitement over 1999's Y2K fears[3] have served to turn public and governmental attention to the vulnerability of computers in an increasingly network-dependent, information-oriented society. For their part, militaries—and especially the US armed forces—have for some time been grappling with the implications of the metamorphosis spawned by the enormous advances in computer technologies of the last twenty years. A general consensus exists that emerging digital capabilities are stimulating what is popularly known as a "Revolution in Military Affairs," or RMA.[4] There are many aspects to the RMA,[5] but few would dispute that one progeny is the rise of information operations (IO)[6] as a specific military discipline.

In fact, the threat of cyberattack as a form of IO is a major concern of the US armed forces. In its doctrine, the military gives the defense of information systems open and prominent attention.[7] In military circles, IO is viewed as an asymmetric strategy because it presents an opportunity for an adversary with a narrow capability to successfully strike a seemingly more powerful opponent like the United States. One commentator explains this phenomena as follows:

> No other country or group can approach the US conventional-weapon superiority. This is why many terrorists find information terrorism an attractive alternative to traditional forms of terrorism. Cyber-terrorism allows terrorists—both foreign and domestic—to inflict damage with no harm to themselves and little chance of being caught. It is a way for the "weak" to attack the "strong," particularly to disrupt a stronger force at a key time during an operation.[8]

The threat of cyberterrorism as a form of IO is especially troublesome to the US armed forces because it can strike at vital systems not under military control. The Department of Defense (DoD) has officially acknowledged that today it is "dependent upon non-DoD assets—the international and national infrastructures, [and] other facilities and services of the private sector,"[9] and these could be targets of cyberattacks. The Air Force admits that this "Achilles' heel of the United States can be the great equalizer for a militarily inferior adversary."[10]

Still, "cyberterrorism" as a term of art does not, per se, find a home in the Pentagon's lexicon.[11] "Terrorism," however, is explicitly defined. The DoD describes it as "the calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological."[12] Cyberterrorism might therefore be understood as using digital technologies to achieve the aims of traditional terrorism.

The purpose of this essay is to briefly outline the military's response to the threat of cyberterrorism, and to examine some of the emerging policy issues attendant to that response. In addition, I will discuss a few issues associated with using the tools of the cyberterrorist *against* America's enemies, and the complications that doing so presents to democratic societies. In addressing both these perspectives, I will be more concerned with identifying areas for further study than with presenting refined solutions. Having said that, I will attempt to anchor the discussion wherever possible in the context of American democracy and how it should shape the role of the military in addressing the dangers of cyberterrorism.

The Military Response

For at least five years, uniformed leaders have publicly discussed the vulnerability to cyberattack on the digital networks upon which the military relies.[13] Yet according to policy in place since 1995, the responsibility for the security of critical non-DoD "information systems and computer-based systems and networks that can be distributive in nature" remains with civilian law enforcement

authorities.[14] Nevertheless, the DoD "must be prepared, in concert with the appropriate authorities and within defense priorities, to assist in their protection" if the attack on the systems "seriously degrades or threatens DoD operations."[15]

Presidential Decision Directive (PDD) 63, issued in May of 1998,[16] provides a conceptual basis to expand DoD's responsibility. In that document DoD was designated as the "lead agency" in the area of "national defense" with responsibility for "coordinating all of the activities of the United States Government in that area."[17] PDD 63, however, left the scope of "national defense" undefined. In addition, PDD 63 established the National Infrastructure Protection Center (NIPC), an organization physically located within the Federal Bureau of Investigation (FBI).[18] NIPC brings DoD together with "representatives from the FBI, other US government agencies, state and local governments, and the private sector."[19] NIPC also serves as the US Government's "focal point for threat assessment, warning, investigation, and response for threats or attacks against our critical infrastructures."[20]

Paralleling these developments, the individual military services have taken steps to enhance defenses against cyberattacks. In 1993 the Air Force established the Air Force Information Warfare Center with the explicit mission of protecting friendly command and control systems.[21] The other services have likewise planned to confront a cyberadversary.[22] Further, the National Security Agency (NSA), an element of the Department of Defense, is tasked with an "information assurance mission."[23] In executing that mission, NSA "conducts defensive information operations, to achieve information assurance for information infrastructures critical to US national security interests." [24]

In order to further coordinate the military response, Joint Task Force Computer Network Defense (JTF-CND) was formed in early 1999[25] with a charter to orchestrate the protection of all DoD computer systems.[26] In a move to bolster its effectiveness, JTF-CND was placed under the control of US Space Command (USSPACECOM) in October of 1999.[27] At the same time, the Joint Information Operations Center was placed under SPACECOM control.[28] In another effort to increase its resources against cyberattack, the Defense Computer Forensics Lab was established in September 1999.[29] It aims to facilitate, among other things, the tracing across the Internet of hackers who threaten DoD systems.[30]

Finally, Joint Task Force-Civil Support (JTF-CS), an organization assigned to US Joint Forces Command, was established not to defend DoD systems per se, but to assist civilian authorities in managing the *consequences* of any catastrophic act of terrorism, including cyberterrorism. In announcing the new task force,

DoD conceded that the benign title of "civil support" and the selection of a National Guardsman instead of a Regular officer as the commander were both intended to quell the concerns of civil libertarians who feared that the "DoD was out to take over and would trample people's civil liberties" with the new organization.[31]

Although the armed forces were quietly developing an *offensive* IO capability for some time, it has only recently been discussed openly. Offensive IO embodies activities such as "operations security, military deception, psychological operations, electronic warfare, physical destruction and special information operations, and could include computer network attack."[32] These types of operations present a plethora of complex legal issues, and practical problems as well. DoD has admitted to Congress that during Operation ALLIED FORCE in Kosovo "the conduct of integrated information operations was hampered by the lack of advance planning and necessary strategic guidance."[33] In order to better focus the offensive information operations effort, General Richard Meyers, the commander of USSPACECOM, announced in January 2000 that effective October 1, 2000 the command will "pick up the computer network attack mission."[34]

The Emerging Policy Issues

Clearly, the US military aims to protect itself against cyberterrorism, facilitate a broader defense of US interests against that threat, and employ cybertechnology as a means and method of warfare, albeit for a presumably more righteous purpose than the cyberterrorist. What kind of policy issues should we expect to see?

Background

Before considering the specific issues associated with the role of the military in defending against cyberattacks, it is important to understand that in the US there is a generally accepted division of labor on security issues. As a rule, civilian law enforcement agencies handle internal security, while the primary purpose of the military is, as the Supreme Court put it in *Toth v. Quarles*, "to fight or be ready to fight wars should the occasion arise"—ordinarily an *externally* focused endeavor.[35] The tradition of ordinarily excluding the military from performing policing duties is traceable to the Founding Father's deep-seated suspicion of professional militaries.[36] That suspicion resulted from their cognizance of the excesses of Cromwell's New Model Army in England, as well as their loathing of

British regulars used to suppress the colonists' growing protests against imperial rule. For these and other reasons, the scheme for national security found in the Constitution principally contemplates not the large standing forces we have today, but a rather small number of regulars augmented by huge state militias.[37] In short, in practical terms it is doubtful that the Founding Fathers ever envisioned a standing army large enough to function as any kind of police force on a regular basis.

While the US military has been used successfully from time to time to quell civil disorders that overwhelm civilian resources, the record of the relatively few times it has been used for an extended period for a law enforcement-type mission is less than sanguine. Indeed, it was the intemperate behavior of Federal occupation troops during the post-Civil War Reconstruction Era that led to the passage of the Posse Comitatus Act in 1878.[38] The Act—which criminalizes the use of the military to enforce the law absent specific authority—remains the principle limitation on the employment of the armed forces for internal security purposes.

Of course, the Posse Comitatus Act is not intended to frustrate the military's ability to engage in bona fide national security-related activities. Exactly what constitutes a national security activity appropriate for military attention, however, became blurred during the Cold War, and especially during the domestic unrest of the Vietnam era. The result was an unwholesome involvement of the military establishment in the personal affairs of thousands of law-abiding US citizens. Professor Loch Johnson reports, for example, that "NSA computers were fed every single cable sent overseas by Americans from 1947 until 1975 [and] Army intelligence units conducted investigations against 100,000 Americans during the Vietnam War."[39]

The excesses of military and civilian intelligence agencies during this period led to Senate investigations in the 1970s (the Church Committee)[40] and substantial restrictions on the ability of military organizations to scrutinize US citizens.[41] Nevertheless, by the early 1980s the nation's drug crisis led Congress to enact a number of measures to involve the military in efforts to halt the tide of narcotics flowing into the country and to help stem the crime explosion catalyzed by illicit drugs.[42] While the armed forces are still generally prohibited from such activities as conducting searches and seizures and effecting arrests, the military counterdrug effort—especially in technical support and border surveillance activities—amounts to billions of dollars and involves thousands of uniformed personnel.

As a result of such initiatives, the traditional reluctance to employ the military in a domestic security role appears to be eroding. [43] Regrettably, however,

incidents occur that demonstrate that the skills of the soldier are not necessarily coterminous with those of the policeman. For example, the tragic 1997 shooting of a Texas high school sophomore by a Marine Corps border surveillance patrol may well illustrate that the orientation of the armed forces leads its members to deal with perceived threats differently than do law enforcement personnel.[44] This difference produces a very distinct approach to security problems.

As a general rule, soldiers move on threats by fire and maneuver with a view towards permanently eliminating them; police forces attach the presumption of innocence towards suspected lawbreakers and seek to resolve incidents peacefully with the ultimate disposition left to the courts. It should be no surprise, therefore—given the military's perspective—that a Pentagon-sponsored report argued that the Pentagon's "policy of prohibiting DoD from mounting a counter cyberattack if its computers are attacked puts the military at risk."[45] In responding to the report's proposal to allow the military to immediately launch a counterattack, John Pike of the Federation of American Scientists quipped, "Does this mean that the Pentagon will start frying the home PCs of American teen-age hackers?"

According to a 1999 Harris poll,[46] the armed forces enjoy a status as the most trusted institution in American society. In my opinion, few activities could jeopardize that trust more than an increased involvement in law enforcement and related activities that cause military personnel to intrude into the lives of everyday Americans. It would not seem to make sense, therefore, to involve military personnel in controversial proposals such as the Federal Intrusion Detection Network (FIDNET).[47] In an era when the US remains obliged by world events to maintain a still sizeable military establishment, and one that is now an all-volunteer professional force, the maintenance of harmonious civil-military relations ought to be a prime concern of democratic leaders. This is especially so given the troubling reports of a growing estrangement of the US armed forces from the nation it serves, notwithstanding the public's evident affection for those in uniform.[48]

Defending Against Cyberthreats

These lessons of the past are worth considering as we develop policies on the military's role in fighting cyberterrorism. Most experts agree that the nature of cyberterrorism is such that it is extremely difficult—at least initially and often later, if ever—to distinguish between the teenage hacker on a digital joy ride, the high-tech felon on a crime spree, the non-State cyberfanatics seeking to intimidate, and the nation-State waging information warfare. Moreover,

the clever cyberterrorist can often employ techniques that make it appear that innocent parties are the instigators of whatever chaos they manage to wreak. Thus, a military organization involved in investigating an attempted act of cyberterrorism could well find itself mistakenly probing innocent persons. Even when the guilty party is correctly identified, it may often be one more properly falling within the jurisdiction of a law enforcement agency, not a military force.

Consequently, the current policy that assumes—at the outset anyway—that an act of cyberterrorism is a criminal matter subject to law enforcement modalities as opposed to a hostile attack calling for a response by the armed forces seems appropriate. Moreover, military leaders—to include former Deputy Secretary of Defense John Hamre—have repeatedly emphasized that DoD is *not* seeking an active role in law enforcement in response to the terrorist threat.[49] Still, relative to the military, police resources are limited and diffused over thousands of jurisdictions. While this state of affairs may be satisfactory in the context of ordinary crime fighting requirements, it may be unacceptable if cyberterrorism presents a threat of truly catastrophic dimensions as some have claimed.

The magnitude of the cyberthreat has much to do with the appropriateness of a military response. A recent study[50] of the Posse Comitatus Act in relation to the protection of military and civil infrastructure against digital attack concluded that the military may conduct what might otherwise be considered prohibited law enforcement activities under certain circumstances. Specifically, action against civilians consistent with the act can occur when, *inter alia*, an "emergency" exists or when the activity is primarily in pursuit of a "military purpose."[51] Accordingly, "if the primary purpose of an action is to resolve or avert a problem with a strong tie to national security, the military purpose exception [to the Posse Comitatus Act] may be invoked."[52]

This brings us almost full circle to the central issue: when does cyberterrorism rise to the level of a true national security threat? We seem to accept almost without question the assertion that the US is "extraordinarily vulnerable" and that "an enemy could systematically disrupt banking, transportation, utilities, finance, government functions and defense."[53] To listen to many pundits, the US is virtually at the mercy of any teenager with a Radio Shack computer. The reality, I contend, is much different. Specifically, I believe that cyberterrorism—particularly when conceived exclusively in terms of computer network attack intended to cripple the nation's economy or military forces—is much more difficult to accomplish.

To put it bluntly, if cyberterrorism were so easy and cheap to do, why have we not seen a *catastrophic* event? If not in the US, anywhere? This is much the

same point that Rand analyst and cyberwar expert Martin Libicki wrote about in *Foreign Policy*.[54] In this regard, I think it would be a mistake to make too much of the past denial-of-service attacks on commercial sites. In the first place, most sites were impeded for only a short time, leading many experts to characterize the incidents as "little more than criminal mischief."[55] Ironically, the attacks may have caused little revenue loss. *Newsweek* wryly noted that since "dot-coms typically lose money on every sale they make, they might come out ahead" as a result of the attacks.[56]

As Libicki observes, there is a great difference between public commercial websites, and the sensitive military and civilian infrastructure operating systems whose incapacitation on a grand scale might stagger even a country like the United States. However vulnerable the former, the latter are much more secure and, in any event, often operate in a closed loop, independent mode requiring unique expertise even if access is somehow achieved. This is a key reason why, for example, Bruce F. Wollenberg, a professor of electrical engineering at the University of Minnesota, insists that the US power grid "isn't hacker friendly."[57]

Dan Kuehl, a respected professor at the National Defense University, argues that the reason a full-fledged cyberattack has not been launched is "solely because no state or non-nation state actor has yet seen sufficient strategic advantage to be gained by doing so—and this condition will not last indefinitely."[58] I disagree because I believe the requisite expertise is much rarer than many assume, and much of that expertise is on the side of the good guys. We live in a world of Saddam Husseins, Slobodan Milosevics, and Osama bin Ladens, who are hell-bent to inflict harm upon us in any way they can. These are people to whom the logic of "strategic advantage" is expressed in the most savage acts of terror they can manage to accomplish. They are smart, ruthless, moneyed, and motivated, yet have not achieved a crushing cyberassault.

We tend to discount too readily our own defensive capabilities. Recall that much was made of the supposed "hacker" capabilities of the allegedly computer-literate Serbs and others during the Kosovo campaign. Evidently, they tried hard. According to Lieutenant General William J. Donahue, "hackers came at us daily, hell-bent on taking down NATO networks."[59] Yet, the end result was failure: no NATO combat deaths, and a near-zero effect on the ultimate military outcome. Similarly, despite all the allegations of rampant, damaging attacks in the private sector, the reality is that the US economy continues to roar. Are we to believe that there are thousands of malicious people with diverse agendas at scores of locations around the globe fully capable of devastating us with keystrokes who are collectively refraining from doing so because of some serendipitously uniform appraisal of "strategic advantage"? My assessment of

human nature leads me to conclude otherwise. In short, they "would if they could—but they *can't.*"

Let me emphasize that I certainly do not counsel indifference; I recognize that cyberattacks will succeed occasionally. Collectively, they are costly—$7.6 billion in 1999 by one estimate.[60] Thus, I think the Clinton Administration's proposal to spend some $2 billion on various computer security programs is a prudent and affordable insurance policy for the nation.[61] I merely point out that as sizeable as the estimated cyber losses are, they must be understood in the context of a country that each year suffers more than $150 billion in costs from motor vehicle crashes alone[62]—not to mention over 40,000 deaths, and in excess of 6 million injured.[63] I simply caution that we should not unnecessarily divert resources from other pressing needs based on what may be an mistaken analysis of the threat.

Moreover, in calculating the dimensions of our potential cyberterrorism problem we should not underestimate the power of our capitalistic free market system to find solutions. In a very real way, America's military prowess is largely the product of its economic success. Given that business to business online sales are expected to grow to $1.3 trillion by 2003,[64] there is a immense incentive for the commercial development of reliable computer security technology for online transactions.

I believe the tremendous market imperative for secure transactions—and the incentive it creates for effective computer security products[65]—will rapidly outstrip the resources of individuals or even governments to create methodologies capable of circumventing improved defensive measures. In discussing the long-term threat after the denial-of-service attacks in early 2000, one commentator maintained that "[w]ith money at stake, e-businesses will fix this glitch."[66] Overall, I find persuasive Libicki's view that our "enemies best time to conduct information warfare has clearly come and gone."[67] All of this is yet more evidence that it is unnecessary at the present time to involve the military in cyberdefense any more than it is presently tasked.

To me, the real danger is not so much that cyberterrorists will use the Web as a vehicle for destructive computer network attacks, but rather that they will employ it as a convenient source of information useful for a variety of nefarious purposes. For example, I am convinced that cyberterrorists could gather enough personal information from Web sources to intimidate and harass individuals or even groups of individuals in the military and elsewhere. This is one reason that the DoD has begun to limit the amount of information available on public sites.[68] At least in the near term, however, the damage has been done. There is sufficient information already on the Internet for those disposed for whatever purpose to engage in such crimes as identity theft.[69] In fact, I believe

this problem is getting so difficult to rectify that in the not too distant future, courts will be adjudicating "identity replacement" much as they now do in bankruptcy cases. Still, these cyberthreats are, in my view, properly within the responsibility—and growing capability—of law enforcement agencies to resolve.[70]

Avoiding the Cyberterrorist Label

As important as it is to defend against cyberattacks, it is equally important to ensure that our own security activities avoid accusations that we ourselves are engaging in cyberterrorism. In a very real sense, the flip side of cyberterrorism is the use of cybertechniques for *legitimate* offensive IO. From the military perspective, the means and methods of the cyberterrorist are not necessarily *malum in se*; rather, they must be tested against existing domestic and international law applicable *ante bello* as well as *in bello*. Along this line, in 1999 the Office of the DoD General Counsel issued its first unclassified assessment of the legal aspects of information operations.[71] In other words, to the military way of thinking, cyberterrorism is objectionable because of its purposes and the *manner* in which it is employed (e.g., against noncombatants and noncombatant objects), not, per se, because of the techniques themselves.

Still, there are many legal and policy questions yet to be resolved. For example, what constitutes, in the layman's vernacular, the proverbial "act of war"? That is, what measure of peacetime cybermanipulation is tolerable before it amounts to a "use of force" or "armed attack" that plunges a nation into conflict?[72] While the definitive answer yet eludes us, there is a growing consensus that once the cyberassault creates consequences indistinguishable from that of a traditional kinetic attack, the legal status of the cyberevent becomes likewise the same.[73] Conversely, it appears cyberevents that do not reach that threshold would not therefore constitute aggression within the meaning of the UN Charter (although they may be violative of other aspects of international or domestic law).[74]

Reference to the UN Charter raises the larger issue of the wisdom of various suggestions for an international agreement addressing cyberterrorism. Some of these, like the Stanford proposal,[75] explicitly exclude "activities undertaken by military forces of a State party, or State party activities during armed conflict."[76] Others, like the reported Russian proposal, contemplate banning certain information weapons altogether.[77] Many would agree that there is a need for greater international cooperation to confront the unique issues presented by cyberterrorism[78] and that cooperation may need to take the form of an international agreement. That said, we ought to be cautious about entering into legal regimes that may unnecessarily hamper what is, after all, an area where the US, as the

world's foremost digital power, may itself have an asymmetric advantage across the spectrum of conflict.

To the extent news reports are reliable, the Kosovo conflict raised a number of interesting issues about the use of cybertechniques during armed conflict. For example, early in the campaign it was reported that a civilian US hacker sent a denial-of-service e-mail "bomb" that flooded the Serb Government website with 500,000 e-mails, crashing the site.[79] Is this person an unlawful combatant under international law? Likely. A cyberterrorist? Perhaps.

Additionally, it was widely reported in the press that senior policymakers did not approve a planned cyberassault of Milosevic's personal bank accounts.[80] I do not know if such a plan ever existed, let alone the reasons it was not executed.[81] If it did exist, however, one can imagine that a key issue would be the propriety of striking the private property of a civilian,[82] notwithstanding his position as the head of State of a belligerent. Given the growing aversion in the international community to the use of destructive, kinetic weapons in war that may cause civilian deaths, it may be useful to re-examine the prohibition against targeting of civilian objects via cybertechniques if bloodshed can be avoided through this kind of coercion. John Markoff, writing in the *New York Times*, argues that "cyberwarfare raises a fundamental philosophical question . . . the biggest challenge that such warfare may pose for democratic societies is that it further blurs the distinction between military and nonmilitary targets."[83]

There are other complex issues occasioned by emerging cyber capabilities for the armed forces of a democracy. In the US military, IO embraces a wide range of technology-empowered activities. Psychological operations, for example, are important to the military commander imbued in the Clausewitzean tradition to believe that the ability of an adversary to wage war depends upon the support of the "remarkable trinity" of the people, the government, and the armed forces.[84] Disassembling the enemy's trinity, that is, undermining his *will* while preserving one's own, is an accepted military objective.[85]

Some emerging cybertechniques present exciting opportunities for the military professional to sap an enemy's resolve with relatively little violence.[86] As Hollywood has repeatedly demonstrated, the ability to use digital means to morph or otherwise create extremely convincing—but false—images is now widely available.[87] Considering such capabilities, Thomas Czerwinski, then a professor at the National Defense University, posed an interesting question: "What would happen if you took Saddam Hussein's image, altered it, and projected it back to Iraq showing him voicing doubts about his own Baath Party?"[88] Quite obviously, it could deceive a population about its leaders, as Professor Czerwinski indicates.

Few would call such efforts against a totalitarian or wholly depraved regime "cyberterrorism." A different issue arises, I believe, when the hostile government is a genuinely democratic one. Consider that if Internet-based voting—which the US military is experimenting with today[89]—becomes widespread, the potential exists to manipulate elections in enemy countries during armed conflict via cybersubversion of the voting process itself.

Would such an operation be appropriate in light of US national security policy that promotes democracy?[90] I do not think so, even though I am not an adherent to the democratic peace theory.[91] Based on my own experience in Somalia and elsewhere, I find Professor Samuel P. Huntington's "clash of civilizations" thesis far more convincing.[92] I accept that there are entire societies that hold values fundamentally different from our own—and they would freely vote to retain those values—even though the policies they produce may lead to conflict with the US or other Western nations.[93] Nevertheless, I also believe that democracy ought not to be asked to "pay for itself," so to speak, by necessarily producing peace.

Democracy as an expression of the principle of self-determination found in the UN Charter[94] and elsewhere has an intrinsic human value independent of any peace-generating quality. Accordingly, is it right to apply cybertechniques against an adversary's democratic *processes*, even in time of war? Certainly it is appropriate to act to control the hostile acts of any government, democratic or otherwise. It seems to me, however, that care must be taken to distinguish between the use of cyberweapons to address the *actions* of a democratic government, and employing them to undermine the democratic *processes* that produced it.

Michael Walzer, perhaps the premier ethicist on issues of war and peace, gives us another matter to consider. He points out that, excluding exceptional cases like Nazi Germany, war aims "don't legitimately reach to the transformation of the internal politics of the aggressor state or the replacement of its regime."[95] In other words, we must be very cautious in employing advanced digital methodologies that may destroy the confidence of people in democratic processes.

Consider also the other vital part of the Clausewitzean trinity: maintaining the will of the publics of *friendly* countries.[96] This is especially a concern for democratic countries, and it was raised during the Kosovo operation. You may recall that Serb radio and television stations were bombed in attacks highly criticized by Human Rights Watch[97] and others.[98] In my opinion, the attacks were warranted[99] since it appears that the facilities were used to whip up ethnic hatred for years.[100] As Air Commodore David Wilby, a NATO spokesman, explained on April 8, 1999, "Serb radio and TV is an instrument of propaganda and repression. . . . It is . . . a legitimate target in this campaign." [101] Since, *inter alia*,

incitement to genocide may itself be a war crime,[102] Wilby's assertions seem to have merit, assuming the other prerequisites of the law of armed conflict were met.

If cybertechniques can neutralize the facilities without the physical destruction conventional munitions cause, we should embrace netwar as a development that could reduce the misery of war. Suppose, however, that the enemy radio and television stations were transmitting not propaganda, per se, but accurate information about US operations that nevertheless was eroding support among our public or that of allied democracies?[103] For example, in a report on the attacks on Serb television stations, Patrick L. Sloyan observed that while bombing stopped the "diet of lies fed Serb viewers," it also served to "curb transmission to the West of those disturbing 'collateral damage' pictures that could erode public support for NATO's escalating strikes in the Balkans."[104] If addressing the latter concern were the *sole* aim—as opposed to, for example, the limited notion of preserving operational security in a particular circumstance—would the attacks be justified? Probably not.

Censorship and exclusion of the press from military operations has long been tolerated in liberal democracies during wartime.[105] Essentially, where there is a demonstration that the information would present a clear and present danger to national security, it could be suppressed.[106] That concept, however, would not seem to permit the suppression of news reports—via cyberassault or other means—simply because the information conveyed would tend to demoralize public opinion in our own country, or that of our allies. Democracy, I believe, has its price.

Concluding Observations

If this brief survey has succeeded, the reader will appreciate that the issues raised by cyberterrorism are many and complex. At the present time, law and policy carefully circumscribe the military's role, and to date DoD has been careful to stay within those limits.[107] There are, however, calls for expanded responsibility. Some suggest a relaxation of the policy that presumes at least initially that a cyberattack is a civilian law enforcement problem, not a national security issue.[108] Doing so, it is contended, would allow that application of the considerable resources of the military and intelligence communities that currently are barred from use in most domestic cases involving US persons.[109]

To this end, one innovative proposal calls for a policy that presumes the digital "intruder is *not* a US person," thus permitting "the full capabilities of the United States' investigative and intelligence assets" to be brought to bear.[110] However, this reversal of the present presumption would apply only to attacks

against specified systems that are deemed by statute to be critical to the nation's economic and national security interests.[111] Whether such an approach is politically feasible depends upon public perceptions. As already indicated, what role, if any, the military should play in defending against domestic cyberattacks is embedded in the larger issue regarding the extent to which Americans believe their way of life is put at risk by the potential of cyberterrorism.

In this regard, I would add one final note of caution. I have often heard a variety of senior Pentagon[112] and national security officials[113] insist that the US is susceptible to an "electronic Pearl Harbor." Conjuring up emotional images of the infamous sneak attack that pulled the US into World War II is certainly an effective way to hype the interest of persons both in and out of uniform towards greater vigilance and preparedness. The analogy is one plainly worth pondering, especially as our society becomes increasingly digitally dependent.

There is, however, a very dark side of the Pearl Harbor story that we should also keep in mind. As a result of the fears generated, the US military—acting in a domestic security role—rounded up thousands of loyal American citizens and placed them in detention camps, all in the name of responding to a threat to national security. We know today that the sacrifice of the rights of Japanese-Americans was wholly unnecessary. Although it may be fashionable these days to say that the roundups were simply racism run amok, those that have actually read *Korematsu v. United States*,[114] as well as Chief Justice Rehnquist's discussion in his recent book[115] may conclude otherwise. From those sources one can reasonably conclude that principled men struggling with a real fear of invasion by an enemy who had already demonstrated his treachery at Pearl Harbor made what they sincerely believed was a unavoidable decision—however wrongheaded it appears with the benefit of hindsight.

But, in a sense, the fact that *respectable* people were nevertheless responsible for the treatment of Japanese-Americans that we now find so objectionable should itself give us pause. As we consider the growing involvement of the military in countering cyberterrorism, we must never forget that the armed forces is the least democratic and most unapologetically authoritarian element of our society. I hasten to add that this does not presume anything sinister about those in uniform or those that advocate an enhanced role for the military in fighting cyberterrorism. I merely submit that in a democracy, and especially American democracy, the machinations of the truly evil are, somewhat paradoxically, frequently more readily corrected than are the misdirected efforts of well-intentioned, honorable citizens.

Pearl Harbor and the sacrifices that followed in its aftermath remain a lesson for us as we consider what role, if any, the military should play in countering

cyberterrorism. On a deeper level we must accept that perfect security is fundamentally at odds with democratic values. This applies as much to cyberterrorism as to any other threat against us. We must be prepared to take prudent risks in order to have a free society. The inescapable truth is that we must likewise acknowledge that from time to time our freedom will exact a harsh price from us and those we love.

Nevertheless, we must not allow the dread of digital terror to drive us to take counsel of our fears. As Martin Van Creveld and others have pointed out, terrorism has not succeeded in developed States because it is a characteristic of modernity to have a robust level of technological redundancy and political resiliency so as to make individual terrorist attacks relatively futile in terms of real effect on capability.[116] While cyberterrorists might be able to inflict costly losses periodically, they cannot physically imperil our continued existence as a free nation. Indeed, the *real* risk is upon those who challenge the forces of freedom. As Professor Victor Hanson explains in his book, *Soul of Battle*,[117] history shows that the forces of democracies *once aroused* are extraordinarily fearsome combatants who, notwithstanding the seeming empowering militarism of the opposing forces, tend to not merely defeat the armies of despots, but to pulverize them *and everything that supports them*. So profound is such defeat that the very societies that produced the forces of tyranny are left fundamentally changed and virtually unrecognizable to their former masters. The enemies of democracies ought to take note.

In summary, the true threat is not what damage cyberterrorists can inflict upon our digital systems, but what freedoms they can force us to forfeit. The *San Francisco Chronicle*, citing a report by the Commission on National Security/21st Century,[118] editorialized that "terrorist hackers" and other threats "will probably put pressure on the military to move into domestic law enforcement, blurring the line between domestic and foreign threats."[119] It soberly warned "it is better to live with danger than in the security of a police State."[120] Although we are certainly not yet living in the shadow of a police State, it is a timely reminder of what is really at stake.

Notes

* The views and opinions expressed in this chapter are those of the author alone and do not necessarily represent those of the US Government or any of its components.

1. *See, e.g.*, Brendan I. Koerner, *The Web's Bad Week*, U.S. NEWS & WORLD REPORT, February 21, 2000, at 19 ("The intruder used an elementary method know as a denial of service attack, which cripples a network by flooding it with too much information.").

2. "Dot com" is a generic name for companies whose business is integrated with the Internet.

3. "Y2K" is shorthand for "Year 2000" and refers to the anomaly in some software programs that causes dates after 1999 to be misread resulting in erroneous calculations. For information on the Department of Defense program to address Y2K, see www.defenselink.mil/issues/y2k.html.

4. For a discussion as to how the "Revolution in Military Affairs" (RMA) interplays with cyberwar, see Sydney J. Freedberg, *Future-Shock Troops*, NATIONAL JOURNAL, December 11, 1999, ebird.dtic.mil/Dec1999/s19991212future.htm.

5. For an overview of how the military intends to incorporate the RMA, see Chairman of the Joint Chiefs of Staff, Joint Vision 2010 (1996), www.dtic.mil/jv2010/jvpub.htm.

6. "Information operations" is defined as "actions taken to affect adversary information and information systems while defending one's own information and information systems." *See* Chairman of the Joint Chiefs of Staff, Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms (2001), www.dtic.mil/doctrine/jel/ref.htm, [hereinafter JP1-02]. "Information warfare" is "information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries." *Id.*

7. *See, e.g.*, Chairman of the Joint Chiefs of Staff, Joint Publication 3-13, Joint Doctrine for Information Operations, ch. III (1998).

8. Tom Regan, *When Terrorist Turn to the Internet*, CHRISTIAN SCIENCE MONITOR, July 1, 1999, at 1.

9. US Department of Defense Directive, Critical Asset Assurance Program (CAAP) 5160.54, January 20, 1998, para. 4.2.

10. Department of the Air Force Doctrine Document 2-5, Information Operations, August 5, 1998, at 6.

11. Barry Colin, a senior research fellow at the Institute for Security and Intelligence, claims to have coined the term "cyberterrorism." *See* Pacific Air Force News, *Terror Can Be Just a Computer Away*, Release No. 98013, February 5, 1998, www2.hickam.af.mil/news/newsarchive/1998/98013.htm.

12. JP 1-02, *supra* note 6.

13. *See, e.g.*, General Ronald R. Fogleman, Information Operations: The Fifth Dimension of Warfare, DEFENSE ISSUES, April 25, 1995, defenselink.mil/speeches/1995/s19950425-fogleman.html.

14. *Id.* at para. 4.3.

15. *Id.*

16. The White House, White Paper, The Clinton's Administration Policy on Critical Infrastructure Protection: Presidential Decision Directive 63, May 22, 1998, [hereinafter PDD 63], press release summary available at www.pub.whitehouse.gov/uri-res/I2R?urn:pdi://oma.eop.gov.us/1998/5/26/1.text1.

17. *Id.* at 4 & 8.

18. *Id.* at 10.

19. Michael Vatis, Director of the National Infrastructure Protection Center, Message from Michael Vatis, www.fbi.gov/nipc/welcome.htm.

20. *Id.*

21. The AFIC home page is available at www.aia.af.mil/common/homepages/pa/bios/iwcfact.html.

22. The Navy has the Fleet Information Warfare Center website available at www.fiwc.navy.mil/html/home.html, and the Army has the Information Assurance Directorate website available at www.army.mil/disc4/isec/c2p/mission/mission.htm.

23. National Security Agency, Mission Statement, available at www.nsa.gov/about_nsa/mission.html.

24. *Id.*

25. Office of the Assistant Secretary of Defense (Public Affairs), Joint Task Force On Computer Network Defense Now Operational, December 30, 1998, (press release), www.defenselink.mil/news/Dec1998/b12301998_bt658-98.html.

26. *See* Frank Wolfe, Joint Task Force To Direct Pentagon's Cyber Defense, DEFENSE DAILY, January 26, 1999, at 1.

27. US Space Command, USSPACECOM Takes Charge of DoD Computer Network Defenses, Release No. 19-99, October 1, 1999 (press release), www.spacecom.af.mil/usspace/new19-99.htm.

28. US Space Command, Joint Information Operations Center Joins USSPACECOM, Release No. 20-99, October 1, 1999 (press release), www.spacecom.af.mil/usspace/new20-99.htm.

29. Douglas J. Gilbert, High-Tech Lab Ties Computers to Crimes, American Forces Press Service, November 1999, www.defenselink.mil/news/Nov1999/n11021999_9911023.html.

30. *Id.*

31. Linda D. Kozaryn, DoD Helps Hometown USA Confront Terrorism, American Forces Press Service, January 2000, www.defenselink.mil/news/Jan2000/n01132000_20001133.htm.

32. JP 1-02, *supra* note 6.

33. Department of Defense, Report to Congress: Kosovo/Operation Allied Force After-Action Report, January 31, 2000, at 99, www.defenselink.mil/pubs/kaar02072000.pdf.

34. General Richard Myers, Special Briefing re: Current Activities of U.S. Space Command, January 5, 2000 (DoD News Briefing), www.defenselink.mil/news/Jan2000/t01052000_t104myer.html.

35. *Toth v. Quarles*, 350 U.S. 11, 17 (1955).

36. For a discussion of the author's views of this issue, see generally Charles J. Dunlap, Jr., *Revolt of the Masses: Armed Civilians and the Insurrectionary Theory of the Second Amendment,* 62 TENNESSEE LAW REVIEW 643 (1995).

37. *Id.* at 648649.

38. Act of June 18, 1878, ch. 263, § 15, 20 Stat. 152 (current version at 18 US Code § 1385 (Supp. 1999)).

39. LOCH K. JOHNSON, A SEASON OF INQUIRY 223 (1985).

40. *See generally, id.*

41. *See, e.g.*, Foreign Intelligence Act of 1978, 50 U.S.C.A. §§ 1801-1811 (1991) and Exec. Order No. 12,333, 46 FEDERAL REGISTER 59,941 (1981) (limiting, *inter alia*, the use of intelligence agencies including those of the armed forces to collect information on persons within the US).

42. *See, e.g.*, Department of Defense Authorization Act, Pub. L. No. 97-86, § 905(a)(1), 95 Stat. 1099, 1115 (1981), amended by National Defense Authorization Act, Pub. L. No. 100-456, § 1104(a), 102 Stat. 1918, 2043 (1988); National Defense Authorization Act for Fiscal Year 1990 and 1991, Pub. L. No. 101-189, § 1216(a), Nov. 29, 1989, 103 Stat. 1352, 1569 (codified at 10 US Code § 371-380 (1988).

43. *See generally,* Charles J. Dunlap, Jr., *The Police-ization of the Military*, 27 JOURNAL OF POLITICAL AND MILITARY SOCIOLOGY 217 (1999).

44 *Id.*

45. *See* Bob Brewin, *Report: Allow Cyberwar Response*, FEDERAL COMPUTER WEEK, March 29, 1999 (citing a report by the National Resource Council), www.fcw.com/fcw/articles/1999/FCW_032999_255.asp.

46. *See* www.usarec.army.mil/hq/apa/slides/VIPRecruitingbrief/tsld006.htm. *See also* Robert Burns, *Poll: Americans Appreciate the Armed Forces*, PACIFIC STARS AND STRIPES, October 19, 1999, at 1.

47. FIDNET is designed to "protect vital systems in federal civilian agencies, and to ensure the rapid implementation of system 'patches' for known software defects." *See* White House, Office of the Press Secretary, Cyber Security Budget Initiatives, February 15, 2000, www.whitehouse. gov/WH/New/html/20000215_1.html. FIDNET is controversial becomes some believe it would be improperly monitoring citizens, a charge the government has denied. *See* Tim Weiner, *Author of Computer Surveillance Plan Tries to Ease Fears*, NEW YORK TIMES, August 16, 1999, ebird.dtic.mil/Aug1999/s19990817author.htm.

48. *See, e.g.*, Triangle Institute for Security Studies, Project on the Gap between Military and Civil Societies, Digest of Findings and Studies, October 1999, www.unc.edu/depts/tiss/CIVMIL.htm.

49. John J. Hamre, *U.S, Military Wants No Domestic Law Enforcement Role*, USA TODAY, October 5, 1999, at 16 (letter).

50. Gregory Grove, Center for International Security and Cooperation, Stanford University, The U.S. Military and Civil Infrastructure Protection: Restrictions and Discretion under the Posse Comitatus Act 23 (1999).

51. *Id.*

52. *Id.* at 25.

53. Bob Drogin, *In Theory, Reality, U.S. Open to Cyber-Attack*, LOS ANGELES TIMES, October 9, 1999, at 16, www.latimes.com/archives/, *quoting* Richard Clarke, National Coordinator for Security, Infrastructure Protection and Counterterrorism.

54. Martin Libicki, *Rethinking War: The Mouse's New Roar?*, FOREIGN POLICY, Winter 1999/2000, at 30 (abstract available at www.foreignpolicy.com/articles/winter1999-2000/Libicki.htm).

55. *See* Anne Plummer, *Pentagon Response To Commercial Denial-of-Service Attacks Limited*, DEFENSE INFORMATION AND ELECTRONICS REPORT, February 18, 2000, at 1.

56. Steven Levy & Brad Stone, *Hunting the Hackers*, NEWSWEEK, February 21, 2000, at 38, 44, newsweek.com/nw-srv/printed/us/st/a16375-2000feb13.htm.

57. Bruce F. Wollenberg, *The U.S. Power Grid Isn't Hacker-Friendly*, WASHINGTON TIMES, April 22, 1998, at 18 (letter).

58. Vernon Loeb, *Cyberwar's Economic Threat*, WASHINGTON POST, February 24, 2000, at 19, *quoting* Dan Kuehl.

59. Bob Brewin, *General: Cyberattacks against NATO traced to China*, FEDERAL COMPUTER WEEK, September 1, 1999, www.fcw.com/fcw/articles/1999/fcw_09011999_china.asp.

60. John J. Stanton, *Rules Of Cyberwar Baffle U.S. Government Agencies*, NATIONAL DEFENSE, February 2000, at 29, ebird.dtic.mil/Feb2000/s20000208rules.htm.

61. *See* White House, Cyber Security Budget Initiatives, *supra* note 47.

62. *See* National Highway Traffic Safety Administration, The Economic Cost of Motor Vehicle Crashes, 1994 (1995), www.nhtsa.dot.gov/people/economic/ecomvc1994.html.

63. Per e-mail with Michael Baxter, Insurance Institute of Indiana, March 15, 2000 (on file with author).

64. Deborah Shapley, *Dr. E-Mail Will See You Now*, TECHNOLOGY REVIEW, January/February 2000, at 42, 44 (*citing* Forrester Research), www.techreview.com/articles/jan00/shapley.htm.

65. In the aftermath of the denial-of-service attacks, Philip H. Karns, an engineer at Qualcom Corp., reports that the "Internet industry experts are rushing the development of software that will locate, trace, and block future denial-of-service attack. . . ." David E. Rovella, *Preparing for a New Cyberwar*, NATIONAL LAW JOURNAL, March 13, 2000, www.lawnewsnetwork.com/stories/A18373-2000Mar10.html.

66. Allan Sloan, *Why the Market Will Rule*, NEWSWEEK, February 21, 2000, at 49, newsweek.com/nw-srv/printed/us/st/a16331-2000feb13.htm (visited March 15, 2000).

67. *See* Libicki, *supra* note 54.

68. *See* John Diamond, *Pentagon Reconsidering What To Make Available on Web*, PACIFIC STARS AND STRIPES, February 18, 1999, at 1.

69. *See, e.g.*, Thomas Ricks, *The Pentagon Says Web Site Made Credit-Card Scam Easier*, WALL STREET JOURNAL, December 8, 1999, at 1.

70. *See, e.g.*, Eric Yoder, *The CyberForce*, GOVERNMENT EXECUTIVE, February 2000, at 45 (describing the growing number of specially trained federal employees involved in Internet law enforcement), www.govexec.com/features/0200/0200s5.htm.

71. *See* Office of General Counsel, Department of Defense, An Assessment of International Legal Issues in Information Operations (Nov. 1999) [hereinafter DoD/GC Paper]. The paper is appended to this volume as the Appendix.

72. The UN Charter requires members to "refrain from the use of force threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations." UN CHARTER art. 2, para. 4. In addition, members are authorized to use force in self-defense if they are the victims of an armed attack. *Id.*, art. 51.

73. *See, e.g.*, WALTER GARY SHARP, SR., CYBERSPACE AND THE USE OF FORCE (1999) and Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUMBIA JOURNAL OF TRANSNATIONAL LAW 885 (1999).

74. *See generally*, James N. Bond, *Peacetime Data Manipulation as One Aspect of Offensive Information Warfare: Questions of Legality under the United Nations Charter Article 2 (4)* (1996) (unpublished paper, Naval War College) (on file with author).

75. Center for International Security and Cooperation, Stanford University, Draft International Convention to Combat Cyber Crime and Cyber Terrorism (1999), www.stanford.edu/group/ CISAC/test/research/Draft.html.

76. *Id.*, art. 20.

77. *See* Bradley Graham, *Military Grappling With Rules for Cyber Warfare*, WASHINGTON POST, November 8, 1999, at 1 (discussing Russian efforts to "gather support for a United Nations resolution calling for new international guidelines and the banning of particularly dangerous information weapons").

78. *See, e.g.*, Richard Hill, *Legal Obstacles Compound Pentagon's Cyberwar Challenges*, DEFENSE INFORMATION AND ELECTRONICS REPORT, March 12, 1999, at 1, ebird.dtic.mil/Mar1999/ s1999/s19990315legal.htm.

79. Patrick Riley, E-Strikes and Cyber-Sabotage: Civilian Hackers Go Online to Fight, April 15, 1999, Foxnews Online, available at www.foxnews.com/world/041599/ Kosovoside_hackers.sml.

80. *See, e.g.*, Gregory L. Vistica, *Cyberwar and Sabotage*, NEWSWEEK, May 31, 1999, at 38.

81. *See* William Arkin, *Cyber Bomb in Yugoslavia*, WASHINGTON POST (Electronic Edition), Oct. 25, 1999, and Bradley Graham, *Military Grappling With Rules For Cyber Warfare*, WASHINGTON POST, Nov. 8, 1999, at 1.

82. *See* Protocol Additional I to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, art. 51, 1125 U.N.T.S. 3, 16 INTERNATIONAL LEGAL MATERIALS 1391, 1413 (forbidding attacks on civilian objects). While the US has not ratified Protocol I, the US recognizes many of its provisions as customary international law or accepted practice. This acceptance includes the provisions of Article 51 with the exception of paragraph 6 regarding reprisals. International and Operational Law Department, The Judge Advocate General's School, United States Army, OPERATIONAL LAW HANDBOOK, 5-2 (2000).

83. John Markoff, *Cyberwarfare Breaks the Rules of Military Engagement*, NEW YORK TIMES, October 17, 1999, at 23.

84. CARL VON CLAUSEWITZ, ON WAR 89 (Michael Howard and Peter Paret eds. and trans., 1976) (1832).

85. Clausewitz observed that war is an act intended "to compel our enemy to do our will." *Id.* at 75.

86. The author has previously discussed this theme. *See* Charles J. Dunlap, Jr., *Technology: Recomplicating Moral Life for the Nation's Defenders*, PARAMETERS, Autumn 1999, at 24, 37–38.

87. *See generally*, William M. Arkin, *When Seeing and Hearing Isn't Believing*, WASHINGTON POST (online edition) February 1, 1999, www.washingtonpost.com/ wp-srv/ national/dotmil/ arkin020199.htm.

88. *As quoted by* Peter Grier, *Information Warfare*, AIR FORCE MAGAZINE, March 1995, at 35.

89. *See, e.g.*, Lisa Hoffman, *U.S. Troops Serving Abroad To Try Out Cyber-Voting Option*, WASHINGTON TIMES, Nov. 28, 1999, at C4, ebird.dtic.mil/Feb1999/e19990217web.htm.

90. The White House, A National Security Strategy for a New Century 19 (May 1997).

91. *See, e.g.*, R.J. RUMMEL, POWER KILLS: DEMOCRACY AS A METHOD OF NONVIOLENCE (1997).

92. Huntington's original thesis (first published in 1993), together with thoughtful critiques have been published. *See* COUNCIL ON FOREIGN RELATIONS, THE CLASH OF CIVILIZATIONS? THE DEBATE (1996). His book-length treatment is entitled THE CLASH OF CIVILIZATIONS AND THE REMAKING OF WORLD ORDER (1995).

93. The author has discussed this theme on several occasions including: Charles J. Dunlap, Jr. *Preliminary Observations: Asymmetrical Warfare and the Western Mindset*, in CHALLENGING THE UNITED STATES SYMMETRICALLY AND ASYMMETRICALLY: CAN AMERICA BE DEFEATED? (Lloyd J. Matthews, ed., 1998), carlisle-www.army.mil/usassi/ssipubs/pubs98/ chalngng/chalngng.htm.

94. *See* UN CHARTER art. 1, para 2. *See supra* note 72.

95. MICHAEL WALZER, JUST AND UNJUST WARS xvii (2d ed. 1992).

96. *See supra* notes 84 and 85, and accompanying text.

97. Human Rights Watch (HRW), Civilian Deaths in the NATO Air Campaign, HRW Report, February 7, 2000, at 22-23, xmail.hrw.org/nato/Matbm200-01.htm.

98. *See, e.g.*, Walter J. Rockler, *War Crimes Law Applies to the U.S. Too*, CHICAGO TRIBUNE, May 23, 1999, ebird.dtic.mil/May1999/e19990525warcrimes.htm.

99. According to the DoD General Counsel, "[w]hen it is determined that civilian media broadcasts are directly interfering with the accomplishment of the military force's mission, there is no law of war objection to using minimum force to shut it down." *See* DoD/GC Paper, *supra* note 71.

100. *See, e.g.*, Jamie F. Metzl, *Information Intervention*, FOREIGN AFFAIRS, November/ December 1997, at 15.

101. *See* William M. Arkin, *Changing the Channel in Belgrade*, WASHINGTON POST (online edition), May 25, 1990, *quoting* Air Commodore David Wilby, www.washingtonpost.com/ wp-srv/national/dotmil/arkin052499.htm.

102. *See generally*, LAWRENCE T. GREENBERG, SEYMOUR E. GOODMAN, & KEVIN J. SOO HOO, INFORMATION WARFARE AND INTERNATIONAL LAW 36 (1998).

103. With respect to *adversary* news outlets, the DoD General Counsel states that the "extent to which force can be used for purely psychological operations purposes, such as shutting down a civilian radio station for the sole purpose of undermining the morale of the civilian population, is an issue that has yet to be addressed authoritatively by the international community." *See* DoD/GC Paper, *supra* note 71.

104. Patrick L. Sloyan, *The Fog of War*, AMERICAN JOURNALISM REVIEW, June 1999, ebird.dtic.mil/Jun1999/s19990608fog.htm.

105. *See generally*, John Calvin Jeffries, Jr. *Excluding the Press from Military Operations, in* NATIONAL SECURITY LAW 993 (John Norton Moore, Frederick S. Tipson, & Robert F. Turner eds., 1990).

106. *See generally*, Donald L. Robinson, *National Security*, *n* THE OXFORD COMPANION TO THE SUPREME COURT 574 (1992).

107. *Cf.* Robert L. Deitz, *NSA Obeying the Law*, WASHINGTON POST, Dec. 7, 1999, at 30, ebird.dtic.mil/Dec1999/s19991207nsa.htm.

108. *See, e.g.*, Catherine MacRae, *Cybercrime Vs Cyber Terrorism, DoD Official Says U.S. Has Been Victim Of Cyber Crimes, Not Terrorism*, DEFENSE INFORMATION AND ELECTRONICS REPORT, Oct. 1, 1999 (*citing* James Christy, law enforcement and counterintelligence coordinator for the DoD Information Assurance Program), www.infowar.com/ mil_c4i/99/ mil_c4I_j.shtml.

109. *See supra* note 41, and accompanying text.

110. Walter Gary Sharp, Sr., *Balancing Our Civil Liberties with Our National Security Interests in Cyberspace*, 4 TEXAS REVIEW OF LAW & POLITICS 69, 72–73 (1999) (emphasis in the original).

111. *Id.*

112. *See* Jim Garamone, Hamre "Cuts" Op Center Ribbon, Thanks Cyberwarriors, American Forces Information Services, Aug. 1999, www.defenselink.mil/news/Aug.1999/ n08241999_9908241.html, quoting former Deputy Defense Secretary Hamre ("Several times I've testified and talked about the future electronic Pearl Harbor to the United States.")

113. Tim Weiner, *Author of Computer Surveillance Plan Tries to Ease Fears*, NEW YORK TIMES, August 16, 1999, ebird.dtic.mil/Aug1999/s19990817author.htm. ("[Richard] Clarke, whose formal title is National Coordinator for Security, Infrastructure Protection and Counterterrorism, has been warning for years about the threat of an 'electronic Pearl Harbor. . . .'").

114. 323 U.S. 214 (1944).

115. *See* WILLIAM REHNQUIST, ALL THE LAWS BUT ONE: CIVIL LIBERTIES IN WARTIME 220–243 (1998).

116. *See generally*, MARTIN VAN CREVELD, TECHNOLOGY AND WAR: FROM 2000 B.C. TO THE PRESENT (1991).

117. VICTOR DAVIS HANSON, SOUL OF BATTLE: FROM ANCIENT TIMES TO THE PRESENT DAY, HOW THREE GREAT LIBERATORS VANQUISHED TYRANNY (1999).

118. U.S. Commission on National Security/21st Century, New World Coming: American Security in the 21st Century, Sept. 15, 1999, www.nssg.gov/Reports/New_World_ Coming/new_world_coming.htm.

119. *New Terrorism Vs Individual Liberties*, SAN FRANCISCO CHRONICLE, Sept. 22, 1999, at 22, ebird.dtic.mil/Sep1999/s19990923threats.htm.

120. *Id.*

XVIII

"Weapons like to Lightning"[1] US Information Operations and US Treaty Obligations

Jeffrey H. Smith and Gordon N. Lederman

The increasing prevalence of computers in the world economy creates new opportunities for the US to conduct offensive military operations and espionage. However, the US is increasingly vulnerable to computer attack, requiring the United States to defend its military and civilian electronic infrastructure. As a nation committed to the rule of law, the United States must remain within the bounds of international law in the conduct of both offensive and defensive information operations.

This chapter explores the opportunities and restraints offered by international law for the conduct of US information operations. We both summarize and critique the 1999 analysis of these issues by the Office of General Counsel, US Department of Defense (DoD), entitled "An Assessment of International Legal Issues and Information Operations" (hereinafter DoD/GC Paper).[2] The DoD/GC Paper surveys international legal issues ranging from the law of war, to obligations under the United Nations Charter, to a host of treaties signed by the United States. This chapter will explore the impact of US international obligations concerning outer space, international communications, and other issues on the conduct of information operations. It will not

address the law of war[3] or the UN Charter,[4] as they are addressed elsewhere in this "Blue Book."[5]

First, this chapter provides a general overview of the development and conduct of information operations. Second, it briefly outlines the structure of international law, including the existence of treaties and the formation of customary international law. Third, US obligations under international law regarding the use of outer space and the impact of these obligations on the conduct of information operations are examined. Fourth, we will explore treaties and international agreements related to the international communications network and their impact on US information operations. Fifth, a survey of possible treaties and other US obligations under international law is offered as a checklist for military commanders and officials deciding whether to authorize a particular information operation. The chapter concludes by offering some thoughts on the merits of an international treaty concerning information operations. In sum, the international legal obligations analyzed herein complicate US information operations but present no insurmountable barriers to them.[6]

It must also be understood that any information operation may well be taken under the extreme pressure of international conflict, without adequate time to weigh all of the legal and political considerations that ought to be considered. Consequently, careful thought must be given to the host of problems raised by these emerging technologies. Moreover, the rate of change in the information technology world means that the legal and political questions presented may be dramatically altered by new technological developments.

In addition, information warfare presents an interplay between domestic and international law not previously seen. For example, the authority of the United States to detect, track, and respond to an information operation is driven as much by the law governing electronic surveillance of US citizens as by international law governing the use of force. Similarly, the questions of what legal authority authorizes an agency to act—and which agency—are very difficult questions. Although beyond the scope of this chapter, these questions must also be answered well in advance of an international crisis.

Finally, it may be difficult to determine whether an information operation is a hostile attack or a criminal act. This ambiguity raises a multitude of questions about how the US should respond to such an event. Furthermore, a response from the US may have unintended consequences, as decision-makers may not be able to predict the collateral damage that may result. An information operation against one nation's infrastructure may have collateral damage, such as destroying bank records, that is much more severe than was intended. Given the interconnectivity of the Internet, a US information operation may blowback

into the United States. Such a possibility raises several questions concerning the privacy and rights of US citizens.

In sum, information operations present many complex legal and operational issues. To first address them in the heat of an information operation is to risk answering them inappropriately.

The Emergence of Information Operations as a Weapon in the Arsenal of Democracy and as a Threat to Democracy Itself

The benefits of increased efficiency and greater speed brought by the infusion of computer technology—particularly the Internet—into the modern economy come at the price of increased vulnerability to disruption and economic ruin as the result of a computer attack.[7] The United States, as the world's most technologically advanced nation, is best situated to develop mechanisms that import information technology into weapons systems[8] and to exploit other countries' reliance on information technology. Simultaneously, however, the United States itself is vulnerable to economic paralysis resulting from the crippling of key US information technology systems. Indeed, as the Federal Bureau of Investigations' former information technology security director, Jim Settle, has stated, the United States could be brought to its knees within 90 days by 10 hackers.[9] Information warfare could eventually usurp the position of biological and chemical weapons as "the poor man's nuclear weapon" because, like biological and chemical weapons, information warfare does not require sizeable financial investment but, unlike biological and chemical weapons, is potentially easier to use—all that is needed for information warfare is a computer and a modem.

As with any concept of sudden importance, the terms and definitions of information warfare have yet to coalesce into an established lexicon. The most succinct definition of information warfare is offered by Winn Schwartau: "Information warfare is an electronic conflict in which information is a strategic asset worthy of conquest or destruction."[10] The US military uses the term "information operations," which involves "actions taken to affect adversary information and information systems, while defending one's own information and information systems."[11] The term "information systems" refers to "the entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information."[12] "Information operations" thus refers to attacks against such infrastructure, organization, personnel, etc.

The military also uses the term "computer network attack," defined as "operations to disrupt, deny, degrade, or destroy information resident in computers

and computer networks or the computers in computer networks themselves."[13] Information operations include a whole host of weapons, including Electro Magnetic Pulse (EMP) and directed energy weapons (such as lasers and high-energy radio frequency guns).

Bureaucratic barriers may have obstructed the conduct of US information operations during the Gulf War and the Bosnia operations.[14] However, the United States did conduct information operations in the 1999 NATO air campaign against Serbia. Army General Henry H. Shelton, Chairman of the Joint Chiefs of Staff, confirmed that the US used information warfare against Serbia during the Kosovo campaign when he stated that "you can assume that we in fact employed some of our systems, yes."[15] Yet, the DoD's after-action report on the air war noted that "the conduct of an integrated information operations campaign was delayed by the lack of both advanced planning and strategic guidance defining key objectives."[16] Indeed, the DoD apparently was concerned about the legalities of full-scale information operations against Serbia, as well as the untested nature of the information warfare arsenal; as a result, the information operations were apparently constrained. Also, the relative decentralization of Serbian computer systems limited the potential for success of information operations. US military forces apparently did confuse and disable the Serbian air defense system using information operations, but these attacks originated with electronic jamming aircraft rather than over computer networks from ground-based sources.[17]

The United States, of course, is a prime target of foreign information operations. Lieutenant General William Donahue, the Air Force's Director of Communications and Information, reportedly stated that, during the Kosovo air campaign, hackers from Chinese Internet addresses targeted NATO networks after NATO's accidental bombing of the Chinese Embassy in Belgrade.[18]

Other countries also recognize the growing and critical importance of information operations. For example, the Chinese military reportedly recognizes and hopes to exploit the potential offered by information operations. On November 2, 1999, Major General Chang Chia-Sheng, director of the simulation center under the Chinese Ministry of National Defense, stated at a news conference that China would be able to launch information warfare against Taiwan by 2005.[19] An article entitled "Bringing Internet Warfare Into the Military System is of Equal Significance with Land, Sea, and Air Power," in *Liberation Army Daily*, the official daily newspaper of the People's Liberation Army's General Political Department, reportedly stated that it was likely that another Chinese military branch, a so-called net force, would be needed to conduct information operations. The article was quoted as saying, "Modern High-Tech Warfare

cannot win without the net, nor can it be won on the net. In the future, there must be coordinated land, sea, air, space, electronic and net warfare. . . ."[20] Other news reports indicate that China and Taiwan are particularly involved in a growing arms race regarding information warfare.[21]

Information operations are thus growing in importance for military operations. It is likely that the United States will utilize information operations in future warfare and peace-enforcement operations. Thus, military and civilian decision-makers must understand the opportunities and restraints offered by international obligations on the conduct of such operations.

A Brief Survey of the Process of International Law

Before looking at specific treaties, it is helpful to have an appreciation for how international obligations arise. Two principles of international law are that, first, sovereign States are equal and independent actors in the international system, and, second, States assume legal obligations only by actually agreeing to do so. States may enter into international treaties and agreements binding the signatory parties. There also exists a body of "customary" international law, composed of practices that are so widely followed by the majority of nations that they are considered obligatory for all. For example, the first satellites launched by the Soviet Union and the United States were seen as benign, and nations lacked the technological ability to interfere with satellites; as a result, it became customary international law that objects in orbit were beyond territorial claims of any nation and that outer space was open to all nations. These concepts were later embodied in international treaties concerning outer space, which will be discussed later in this chapter. As a side note, the development of international law concerning outer space contrasts with that concerning aviation, in which nations produced a highly restrictive legal structure creating the concept of air space and rendering illegal the entrance of aircraft into another nation's airspace.[22]

Countries usually cannot unilaterally withdraw from a treaty unless the treaty provides for such an action, and treaties can only be modified by the agreement of the parties. It should be noted that both treaties ratified by the Senate and executive agreements entered into by the President are equally binding on the United States. Also, many treaties are silent on whether they continue to be in force in the event of conflict or hostilities between the signatory parties; this is important for discerning whether the US is bound by a particular treaty's obligations in the event of an outbreak of hostilities and a US desire to conduct information operations.[23]

US Information Operations in Space

International law concerning activities in outer space is critical for information operations because outer space is a vital battleground for information operations. Space-based systems "perform such functions as communications relay, image recollection, missile warning, navigation, weather forecasting, and signals intelligence."[24] As a result, US information operations will be aimed in part against space-based systems. Such attacks could manifest themselves in attacks against ground stations, jamming communications links, or attacking the satellites in space themselves.[25] Furthermore, as apparently occurred during the Kosovo air campaign, satellites can be used to relay transmissions that are part of a US information operation against a ground-based target.

Since the first satellite was launched by the Soviet Union in 1957, States have signed four major multilateral space treaties: (1) the 1967 Outer Space Treaty;[26] (2) the 1968 Rescue and Return Agreement;[27] (3) the 1972 Liability Convention;[28] and (4) the 1975 Registration Convention.[29] The Moon Agreement of 1979 was not signed by the United States and has in fact only been signed by eleven, and ratified by nine, countries.[30] Emerging from these four major space treaties are several principles concerning the use of space: (1) outer space is free for exploration and use by all States and cannot be subject to any claim of sovereignty; (2) activities in space must be done with due regard for the interest of other States; and (3) States that launch objects into space are liable for any damage they cause. As the DoD/GC Paper highlights, the rules on the use of force such as the law of war and the UN Charter are fully applicable in space. The paper also notes that, while space law contains the principle of non-interference with other States' space systems, this provision might be inapplicable during wartime if the treaties themselves do not remain in effect during hostilities.[31]

Although these treaties strictly limit the use of space for military purposes, they do not outlaw all military activities per se. Rather, the Outer Space Treaty mandates that parties shall not "place in orbit around the Earth any objects carrying *nuclear weapons* or any other kinds of weapons of *mass destruction*, install such weapons on celestial bodies, or station such weapons in outer space in any other manner" (emphasis added).[32] The Outer Space Treaty also prohibits the establishment of military bases and other types of military activities on the moon.[33] The 1972 Anti-Ballistic Missile (ABM) Treaty provides that no party may "develop, test or deploy" space-based ABM systems or components.[34] As the DoD/GC Paper summarizes, the web of international treaties concerning space prohibits the stationing, testing, or exploding of *nuclear* devices in outer space

and the deployment of a space-based anti-ballistic missile capability. However, despite the existence of certain limitations, the paper concludes that there is no legal prohibition on developing and using *non-nuclear* weapons in space, whether deployed in orbit or via flight from the earth's surface.[35] Seemingly, this conclusion appears to open space to information operations.

Still, the DoD/GC Paper does not explore one possible way in which the Outer Space Treaty might ban information operations utilizing satellites. While the Outer Space Treaty prohibits "objects carrying nuclear weapons or any other kinds of weapons of mass destruction . . . or stationing such weapons in outer space, in any other manner,"[36] it is unclear whether information operations fall into the category of weapons of mass destruction. For example, a computer attack against any national computer system of critical importance (e.g., key banking systems, key medical systems, computer systems controlling dams, oil refineries, and other critical infrastructure installations) could wreak "mass destruction" in the sense of widespread loss of life and property.[37] To the extent that a weapon is judged to be a weapon of mass destruction not because it falls within a certain category of what is already accepted as a weapon of mass destruction, namely, chemical, biological, radiological, and nuclear, but rather based on the weapon's effect, information operations could (if used skillfully) exact a fearful toll on both life and property.[38] Of course, even if certain information operations could constitute weapons of mass destruction, it is unclear what constitutes "carrying" or "station[ing]" such weapons on a satellite. If a satellite is used simply to relay data from a computer in the aggressor country to a computer in the victim country, it is unclear whether such a relay of information would be considered "carrying" or "stationing" as defined by the Outer Space Treaty. However, one could imagine a situation in which a particular program for information warfare is stored in a satellite's computer, waiting for the proper signal or timing for delivery to a ground-based target. In this case, the Outer Space Treaty could be interpreted as prohibiting the use of satellites for information warfare.

If the erratic development of US policy on anti-satellite weapons is any indication, policy regarding information operations in space may remain unsettled for many years. For example, in the early 1980s, the Air Force developed an anti-satellite missile designed to be fired from an F-15 fighter flying at a high altitude. After the system was tested in 1985, Congress prohibited the appropriation of funds for anti-satellite weapons to be tested against an object in orbit, leading to the termination of the program in 1987. Congressional critics of the anti-satellite weapons program argued that: (1) outer space should remain free from warfare; (2) tests in space of anti-satellite weapons created space debris; (3) testing of anti-satellite weapons might interfere with arms control negotiations;

and (4) the United States did not necessarily want to encourage other nations to develop an anti-satellite weapon system given its own heavy reliance on satellites. In contrast, supporters of anti-satellite programs argued that the United States should have the ability to attack opposing States' satellites and should invest in defending its own satellites.

By the early 1990s, anti-satellite technology had moved away from missiles and toward lasers. Congress first prohibited and then later allowed the use of appropriated funds for a test of a laser against an orbiting satellite. In October 1997, the US Army tested its MIRACL laser against an aging satellite. While the Army tried to construe the test as purely defensive in nature (namely to observe the effects of a laser on satellites in order to generate information for protecting satellites), a public uproar followed. President Clinton subsequently used his then-existing line-item veto authority to strike funds from the fiscal year (FY) 1998 DoD Authorization Act for projects related to an anti-satellite and space control program. Subsequently, following the Supreme Court's ruling that the line-item veto was unconstitutional, Congress approved funds for anti-satellite weapons in the FY 1999 DoD Authorization Act.[39] Accordingly, it is likely that the increased use of space-based systems as instruments in information warfare will engender criticism from opponents of anti-satellite weapons systems, who will argue that the United States should not further militarize space. However, the assumption in 1999 by US Space Command of responsibility for information operations signals that the military will likely integrate space-based systems into information operations.[40]

International Telecommunications Law and Information Operations

International telecommunications law is a web of bilateral and multilateral treaties.[41] The 1992 ITU Convention[42] is the preeminent treaty in this area, with over 130 signatories. This convention and others established the International Telecommunications Union (ITU), a specialized agency of the United Nations with the authority to formulate telegraph and telephone regulations which become binding legal obligations after formal acceptance by ITU members.

Article 45 of the ITU Convention states that all radio stations, "whatever their purpose, must be established and operated in such a manner as not to cause harmful interference to the radio services or communications of other Members or of other duly authorized operating agencies, which carry on a radio service, and which operate in accordance with the provisions of the Radio Regulations."[43] Annex 2 of the Convention defines harmful interference as "interference which

endangers the functioning of a radionavigation service or of other safety services or seriously degrades, obstructs or repeatedly interrupts a radiocommunication service operating in accordance with the Radio Regulations."[44] The DoD/GC Paper recognizes that jamming or spoofing a radio navigation service would violate this provision.[45] Therefore, the ITU Convention and the entire telecommunications multilateral treaty regime would seem to limit information operations that involve interference with radio broadcasting.

Still, as the paper notes, Article 48 of the ITU Convention provides an exemption for military operations: "Members retain their entire freedom with regard to military radio installations of the Army, Naval, and Air Forces."[46] Article 48 continues, "[n]evertheless, these installations must, so far as possible, observe . . . the measures to be taken to prevent harmful interference, and the provisions of the Administrative Regulations concerning the types of emission and the frequencies to be used, according to the nature of the service performed by such installations."[47] The DoD/GC Paper also notes that, in July 1994, the Department of Justice's Office of Legal Counsel relied on Article 48 in deciding that the United States could broadcast messages to the Haitian people from military aircraft and international air space urging them not to flee Haiti by sea in hazardous vessels.[48]

The ITC also allows signatory States to interfere with international telecommunications in certain circumstances. Article 34 allows members to "stop the transmission of any private telegram which may appear dangerous to the security of the State or contrary to its laws, to public order or to decency, provided that they immediately notify the office of origin of the stoppage of any such telegram or part thereof, except when such notification may appear dangerous to the security of the State."[49] In addition, States may "cut off any other private telecommunications which may appear dangerous to the security of the State or contrary to its laws, to public order or to decency."[50] And finally, Article 35 allows members "to suspend the international telecommunications service for an indefinite time, either generally or only for certain relations and/or for certain kinds of correspondence, outgoing, incoming or in transit, provided that it immediately notifies such action to each of the other Members through the medium of the Secretary-General."[51] The ITC provisions do not state whether the treaty applies during armed conflict. However, as the DoD/GC Paper notes, there is precedent that international communications treaties are suspended during armed conflict. During World War I, for example, the British Navy cut Germany's major submarine cables despite the existence of the 1884 Convention for Protection of Submarine Cables. It should be noted, however, that the United States may have entered into bilateral communications agreements with particular

countries that may be relevant depending on the circumstances of a particular information operation.

The DoD/GC Paper concludes by stating that "International Communications Law contains no direct and specific prohibition against the conduct of information operations by military forces, even in peace time."[52] However, US information operations may be carried out not only by military forces, but also by intelligence personnel engaged in covert action or other intelligence-related activities. Yet, the ITU Convention's Article 48 exemption for military operations does not appear to allow for such interference in telecommunications by non-military personnel such as intelligence operatives.[53] Also, the international telecommunications treaty regime contains certain notice provisions, and it is unlikely that the military would wish to publicize its information operations in that way.

A Checklist of Other US Treaty Obligations

In addition to international law governing the use of outer space and telecommunications, various other treaties and international obligations could impact upon, interfere with, and possibly even prohibit the conduct of US information operations. The following discussion is intended as a non-exhaustive checklist for decisionmakers faced with the question of whether to authorize a particular information operation.

The United Nations Convention on the Law of the Sea (LOSC)

This convention, which is currently under review by the Senate for advice and consent, codifies several provisions of customary international law and creates new requirements. One such provision of preexisting customary international law is Article 19, which states that a vessel exercising the right of innocent passage through another nation's territorial sea cannot engage in activities "prejudicial to the peace, good order, or security of the coastal State."[54] Article 19 defines "prejudicial activities" to include:

- Any threat or use of force against the sovereignty, territorial integrity or political independence of the coastal State, or in any other manner in violation of the principles of international law embodied in the Charter of the United Nations; . . .
- Any act aimed at collecting information to the prejudice of the defense or security of the coastal State;

- Any act of propaganda aimed at affecting the defense or security of the coastal State; . . .
- Any act aimed at interfering with any systems of communication or any other facilities or installations of the coastal State[.][55]

While the DoD/GC Paper observes that LOSC provisions "have the potential to affect only a narrow category of information operations,"[56] a literal reading of the LOSC seems to point to information operations falling under its purview. Ship-borne information weapons could be classified as "prejudicial to the peace, good order or security of the coastal State" because information operations are "aimed at interfering with particular systems of communication or other facilities or installations of the coastal State." The Convention establishes a nation's maximum territorial sea as twelve miles from the nation's coast, significantly smaller than the 200 miles that particular nations claim.[57] Thus, an obvious remedy for any legal problems with ship-borne information operations is for ships wielding information weapons "against" or otherwise "aimed at" a coastal nation to stay outside of the twelve-mile limit. It should be noted that the LOSC does not expressly address whether its obligations are enforced during an international armed conflict.

Treaties on Civil Aviation

Article 3(d) of the 1944 Chicago Convention, which established the International Civil Aviation Organization (ICAO), states, "The contracting States undertake, when issuing regulations for their state aircraft, that they will have due regard for the safety of navigation of civil aircraft."[58] The DoD/GC Paper observes that, as a result, military aircraft have an obligation of "due regard" for the safety of civil aircraft, meaning an obligation "not to interfere with the systems" of civilian aircraft, but does not elaborate on this obligation.

A question thus arises concerning the use of information warfare against particular navigational systems or other dual-use systems, i.e., used both by military and civilian aircraft. For example, a particular navigational satellite might be used both by military and civilian aircraft, or a particular civilian–military airport might use the same radar for both military and civilian flights. An information operation against such computer equipment with the aim of disrupting military operations could impact civilian aircraft as well, leading to a violation of civil aviation treaty obligations. The DoD/GC Paper notes that the Chicago Convention specifically provides that the treaty does not "affect the freedom of action of any of the contracting States affected,

whether as belligerents or as neutrals."[59] It also notes that many provisions of the convention are inconsistent with wartime circumstances and, therefore, the Chicago Convention would be unlikely to survive as a complete entity in the event of an armed conflict. However, Article 89 does not provide adequate guidance in ascertaining what provisions of the Chicago Convention are applicable during an armed conflict and thus what limitations exist on information operations in wartime.

Treaties on Diplomatic Relations

The 1961 Vienna Convention grants to diplomatic missions the right of inviolability of the premises and its documents and communications. The convention also requires that diplomatic personnel respect the laws and regulations of the State in which they are stationed and that "premises of the mission must not be used in any manner incompatible with the functions of the mission as laid down in the present Convention or by other rules of general international law or by any special agreements in force between the sending State and the receiving State."[60] As the DoD/GC Paper concludes, "Planning for any information operations activity that involves diplomatic premises, persons, archives, documents, or communications, either as an instrument or as a target of the operation, must take into account these international legal obligations."[61]

Treaties of Friendship, Commerce and Navigation (FCN)

These bilateral agreements between the United States and other nations establish arrangements for tourism, trade, transportation, and other routine and practical issues. According to the DoD/GC Paper, such treaties probably would be suspended in the event of armed conflict. However, to the extent that information operations are utilized in peace-time, decisionmakers must take into account obligations incurred in FCN treaties to the extent they will impact information operations. For example, one could imagine the scenario in which the targeted nation will attribute the information operation to criminal elements or to economic espionage and will request assistance from the United States under the FCN treaty (or under mutual legal assistance agreements and extradition agreements)in response to such information operations. US officials need to be prepared to respond to such a request even when the information operation is a military or intelligence operation.

Status of Forces Agreements and Foreign Domestic Law

Stationing agreements and defense cooperation agreements memorialize the consent of the host nation to the presence of US troops, set limits on troop numbers, and identify facilities. The United States also commonly enters into status of forces agreements (SOFAs) to address legal jurisdiction over its forces. The DoD/GC Paper notes that, by the end of 1998, the United States was a party to 103 SOFAs. Many require that the US notify the host nation of any significant change regarding the capabilities or status of the military forces stationed in the host country.

As the DoD/GC Paper states, if authorities intend to conduct information operations from US bases abroad, a determination must be made as to whether the relevant agreements require notifying the host nation and perhaps even requesting its consent.[62] The paper also notes that such agreements often require that US equipment not interfere with the host nation's communication system and that such equipment cannot violate the host nation's laws and regulations. Host nations may understandably be concerned about information weapons criss-crossing their telecommunications equipment for fear of possible, unintentional infection of the host nation's computers. They might also be wary of the counter-measures or acts of self-defense by the target nation of a US information operation. Yet, even if a host nation opposed the use of US forces stationed in its country to conduct information operations, the difficulty of attributing an information operation to its true source might give US forces sufficient cover regarding the origin of the attack, and thus might assuage the host nation's concern regarding its own possible vulnerability to counter-measures or reprisals.

It should be noted that foreign domestic laws impact the conduct of US defensive information operations because foreign law enforcement officials may not be authorized to conduct criminal investigations of possible computer crime or information warfare unless the conduct at issue constitutes a crime according to the laws of that particular country. As a result, officials may not receive the expected levels of cooperation from foreign law enforcement officials in the investigation of an apparently criminal information operation emanating from a particular country. Conversely, if a foreign government does outlaw activity that constitutes information warfare, US military officials may decide to refrain from offensively-oriented information operations conducted from their bases in that particular country in order not to subject US forces to liability or culpability for violating that foreign country's laws. Furthermore, even if US forces would not be liable or culpable legally, commanders may wish to avoid the appearance of violating foreign domestic law.[63] As the DoD/GC Paper notes, conduct by

military personnel that constitutes an offense under the host nation's law and not under US law could give the host nation exclusive jurisdiction to prosecute. This situation could occur if a host nation's computer law is more developed than US law or prohibits particular forms of information warfare.[64] Of course, the flexibility and interconnectedness of the Internet mean that the United States could conduct the information operations from a host country that allows such operations, thus avoiding the particular countries that criminalize such activity.[65]

Espionage

The DoD/GC Paper emphasizes the fact that, given the ambiguity surrounding the concept of information warfare, the division between espionage and the use of force is ambiguous. Thus, it may be unclear whether an information operation constitutes espionage or a military attack—or both. The paper also notes that the division of labor between the intelligence community and the military concerning covert action is likely to be blurred by information operations. As it concludes, "it remains to be seen how information operations activities will fall within this division of labor," especially when such information operations occur in the context of military operations other than war such as peacekeeping, peace-enforcement, and counter-narcotics missions.[66]

An Information Warfare Treaty?

In October 1998, Russia introduced a resolution in the United Nation's First Committee calling for States to report their views concerning the "advisability of elaborating international legal regimes to ban the development, production and use of particularly dangerous information weapons." The United States responded that it was premature to discuss negotiating an international treaty concerning information warfare. On the one hand, an international treaty serves the interest of less-technologically developed nations because the treaty would most likely restrict more advanced nations such as the United States from developing information warfare techniques. On the other hand, an international treaty need not necessarily set restrictions below the level at which advanced nations currently operate. Such restrictions would be equivalent to arms-control agreements setting a limit on number of weapons well-above the number of weapons actually possessed by signatory States. Furthermore, a treaty limiting information operations by nations does not address the problem of terrorists or hackers.[67]

A treaty could potentially ban information operations but allow research on information warfare or limit research to defensive capabilities. However, the

distinction between offensive and defensive information warfare might blur because an understanding of offensive operations is required for construction of effective defenses (and vice versa).[68] Alternatively, a treaty could conceivably require certain identifying marks on military information operations so that countries can identify the source of operations, although the lack of such attribution characteristics might be a violation of the current law of war concerning perfidy—meaning that a new treaty is not required for this specific purpose. It should also be noted that, as a nation advances technologically, it becomes more vulnerable to technological attack; in other words, the United States could actually benefit from an international treaty due to its economy's heavy reliance on computer infrastructure. This assumes, however, that the treaty is both widely adopted and enforceable. Also, the treaty should not leave the United States powerless to defend itself against attacks from terrorists or hackers as opposed to information operations launched by another State.

The DoD/GC Paper concludes that "[t]here seems to be no particularly good reason for the United States to support negotiations for new treaty obligations and most of the areas of international law that are directly relevant to information operations."[69] It nevertheless observes that one area in which international agreements would be beneficial is cooperation concerning criminal law, namely efforts to raise the level of foreign countries' criminal laws concerning computer crimes to that recognized by the United States. Although the DoD/GC Paper states that it is unclear how such a treaty could actually work in practice, it also speculates that a treaty concerning information terrorism might be useful.

Conclusion

The DoD/GC Paper states that there are no "show-stoppers" in international law prohibiting US information operations.[70] However, obligations concerning the use of outer space may present problems if a particular information operation qualifies as a "weapon of mass destruction." Furthermore, other obligations under international law present complications—and opportunities—for the conduct of US information operations. Decisionmakers must be sure to assess the impact of international law on each proposed information operation.

Notes

1. WILLIAM SHAKESPEARE, KING HENRY THE SIXTH, act II, scene i, *in* WILLIAM SHAKESPEARE: THE COMPLETE WORKS (Alfred Harbage ed., 1969).

2. Office of General Counsel, Department of Defense, An Assessment of International Legal Issues in Information Operations (Nov. 1999) [hereinafter DoD/GC Paper]. This paper is appended to this volume as the Appendix. All cites are to Appendix pagination.

3. The law of war includes such general principles as the distinction of combatants from noncombatants, military necessity, proportionality, and the outlawing of indiscriminate weapons and perfidy.

4. Article 2(4) of the UN Charter requires signatory States to "refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations." UN CHARTER art. 2, para. 4, 59 Stat. 1031, 1037. The Charter also permits the Security Council to authorize coercive measures, such as military force, in the event that there is a "threat to the peace, breach of the peace, or act of aggression." *Id.*, art. 39, 59 Stat. 1043. Article 51 provides that "nothing in the present Charter shall impair the inherent right of individual or collective self-defense, if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. *Id.*, art. 51, 59 Stat. 1044–45. The DoD/GC Paper concludes that "[a] close parsing of the language would tend to limit its effect to attacks and invasions using traditional weapons and forces." DoD/GC Paper, *supra* note 2. However, the paper does not explicate the opposing view, namely that an armed attack may not mean *only* an armed attack in a traditional sense, but also may include information warfare because information operations can lead to property destruction and the loss of life. Still, the paper goes on to state that there is "a well-established view that article 51 did not create the right of self-defense, but that it only recognized a pre-existing and inherent right that is in some respects broader than the language of article 51." *Id.* In other words, even if information operations might not constitute an armed attack under the language of Article 51, States might have a right of self–defense in response to information warfare attacks based on a more expansive right of self-defense that existed prior to the UN Charter.

5. *See also* Todd Morth, *Considering Our Position: Viewing Information Warfare as a Use of Force Prohibited by Article 2(4) of the U.N. Charter*, CASE WESTERN RESERVE JOURNAL OF INTERNATIONAL LAW 567–600 (Spring–Summer 1998); Richard W. Aldrich, The International Legal Implications of Information Warfare (US Air Force Academy, Institute for National Security Studies, 1995); Sean P. Kanuck, *Information Warfare: New Challenges for Public International Law*, 37 HARVARD INTERNATIONAL LAW JOURNAL 272 (1996).

6. *See generally*, LAWRENCE T. GREENBERG, SEYMOUR E. GOODMAN, & KEVIN J. SOO HOO, INFORMATION WARFARE AND INTERNATIONAL LAW (1997).

7. *See generally*, THE INFORMATION REVOLUTION AND INTERNATIONAL SECURITY (Stuart J.D. Schwartzstein ed., 1996). *See* THE INFORMATION REVOLUTION AND INTERNATIONAL SECURITY (Ryan Henry & C. Edward Peartree eds., 1998).

8. *See generally*, IN ATHENA'S CAMP: PREPARING FOR CONFLICT IN THE INFORMATION AGE, (John Arquilla & David Ronfeldt, eds., 1997); DAVID A. OCHMANEK, EDWARD R. HARSHBERGER, ET AL., TO FIND AND NOT TO YIELD: HOW ADVANTAGES IN INFORMATION AND FIREPOWER CAN TRANSFORM THEATER WARFARE (1998). *See also* BRIAN NICHIPORCK & CARL H. BUILDER, INFORMATION TECHNOLOGIES AND THE FUTURE OF LAND WARFARE (1995).

9. Prosenjit Bhattacharya, *The Next Wars in Space, Cyberspace*, FOREIGN ECONOMIC TIMES, Dec. 21, 1999. One advantage that western countries have in terms of facing information warfare attacks is that they have already been targeted themselves by their own children, namely teenage hackers who constantly probe governmental and other key computer systems for weaknesses. In essence, these teenage hackers keep governmental and industry leaders who are charged with defense against information warfare on their toes, resulting in hardened defenses that have as a

secondary benefit increased defensive capability against foreign attackers. *See* Interview with Jarod Lanier, CNN (Jan. 9, 2000).

10. Winn Schwartau, *An Introduction to Information Warfare*, *in* WAR IN THE INFORMATION AGE: NEW CHALLENGES FOR U.S. SECURITY 49 (Robert L. Pfaltzgraff, Jr. & Richard H. Shultz Jr. eds., 1997).

11. Chairman of the Joint Chiefs of Staff, Joint Publication 3-13, Joint Doctrine for Information Operations (1998).

12. *Id.* at I-11.

13. *Id.* at I-9.

14. *See Washington Outlook*, AVIATION WEEK AND SPACE TECHNOLOGY, Dec. 6, 1999, at 27.

15. Robert Burns, *Pentagon Cites Cyber Warfare Report*, *AP Online*, Nov. 9, 1999.

16. David A. Fulghum, *Telecom Links Provide Cyber-Attack Route*, AVIATION WEEK AND SPACE TECHNOLOGY, Nov. 8, 1999, at 81–83. While the Iraqi telecommunications network was severely attacked during the Gulf War by Coalition air forces, Yugoslav telephone and Internet links apparently went relatively unscathed. Some analysts have postulated that this was a deliberate move by NATO in order to maintain pathways for US military hackers to enter Yugoslav computers. An after-action survey of bombing damage done by William Arkin, an independent defense analyst, found that only 3 of about 30 Serbian telephone system nodes had been attacked by NATO aircraft and that none of the three network control stations for cell phone usage had been attacked, even though Yugoslav agents were reportedly phoning in with the times of NATO aircraft departures from NATO bases. Arkin speculated that NATO forces deliberately did not attack these communications nodes in order to maintain pathways for information operations. *Id.*

17. *See* Bradley Graham, *Military Grappling with Rules for Cyber Warfare*, THE WASHINGTON POST, Nov. 8, 1999, at A1.

18. *See* Michael Evans, *War Planners Warn of Digital Armageddon*, THE TIMES OF LONDON, Nov. 20, 1999, at 11.

19. *See* MND Calls for Establishment of High-level Defense Mechanism, Central News Agency of Taiwan, Nov. 2, 1999.

20. *Bringing the Internet into the Military System is of Equal Significance with Land, Sea, and Air Power*, LIBERATION ARMY DAILY, Nov. 1999.

21. Robert Karniol, *Briefing-Military Modernization in Asia*, JANE'S DEFENSE WEEKLY, Nov. 24, 1999.

22. *See* DoD/GC Paper, *supra* note 2.

23. *See id.*

24. *Id.* This is even more true with the growing use of commercial satellite imagery. *See* Ann M. Florini & Yahya Dehganzada, *Commercial Satellite Imagery Comes of Age*, ISSUES IN SCIENCE AND TECHNOLOGY, Fall 1999, at 45–52.

25. DoD/GC Paper, *supra* note 2.

26. The Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, Jan. 27, 1967, 18 U.S.T. 2410, 610 U.N.T.S. 205 [hereinafter Outer Space Treaty].

27. Agreement on the Rescue of Astronauts, Return of Astronauts, and the Return of Objects Launched into Outer Space, April 22, 1968, 19 U.S.T. 7570, 672 U.N.T.S. 119 [hereinafter Rescue and Return Agreement].

28. The Convention on International Liability for Damages Caused by Space Objects, March 29, 1972, 24 U.S.T. 2389, 961 U.N.T.S. 187 [hereinafter Liability Convention].

29. The Convention on the Registration of Objects Launched into Outer Space, Jan. 14, 1975, 28 U.S.T. 695, 1023 U.N.T.S. 15 [hereinafter Registration Convention].

30. Agreement Governing the Activities of States on the Moon and Other Celestial Bodies, *opened for signature* Dec. 18, 1979, 1363 U.N.T.S. 22. The Multilateral Prohibition of Military and

other Hostile Use of Environmental Modification Techniques, signed in 1977, contains some provisions applying to space activity, but these are not relevant to information operations. *See* DoD/GC Paper, *supra* note 2.

31. DoD/GC Paper, *supra* note 2. *See* MICHAEL J. MUOLO, SPACE HANDBOOK: A WAR FIGHTER'S GUIDE TO SPACE 53–57 (1993).

32. Outer Space Treaty, *supra* note 26, art. IV, 18 UST. 2413–14, 610 U.N.T.S. at 208.

33. *Id. See also* DoD/GC Paper, *supra* note 2. The 1963 Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space and Under Water (Limited Test Ban Treaty) prohibits nuclear explosions in outer space (Aug. 5, 1963, 14 U.S.T. 1313, 480 U.N.T.S. 43).

34. Limitation of Anti-Ballistic Missile Systems Treaty, May 26, 1972, art. V, US-USSR, 23 U.S.T. 3435, 3441.

35. *See* DoD/GC Paper, *supra* note 2.

36. Outer Space Treaty, *supra* note 26, art. IV.

37. *See* Byard Q. Clemmons, *Cyberwarfare: Ways, Warriors and Weapons of Mass Destruction*, MILITARY REVIEW, Sept.–Oct. 1999, at 35–45.

38. *See id.*

39. *See* DoD/GC Paper, *supra* note 2.

40. *See generally*, THE US AIR FORCE IN SPACE: 1945 TO THE TWENTY-FIRST CENTURY (R. Cargill Hall & Jacob Neufeld eds., 1998); AIR AND SPACE POWER IN THE NEW MILLENNIUM (Daniel Goure & Christopher M. Szarza eds., 1977); MUOLO, *supra* note 31, vol. I & II.

41. *See* Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUMBIA JOURNAL OF TRANSNATIONAL LAW 885–937 (1999).

42. Constitution and Convention of the International Telecommunication Union, Dec. 22, 1992, S. Treaty Doc. No. 104–34. (1996) [hereinafter ITU Convention].

43. *Id.*, art. 45.

44. *Id.*, Annex 2.

45. *See* DoD/GC Paper, *supra* note 2. The paper makes reference to the articles as numbered in the 1982 International Telecommunication Convention, the predecessor of the ITU Convention of 1992. The substantive content of the articles in both conventions is the same.

46. ITU Convention, *supra* note 42, art. 48.

47. *Id.*

48. *See* DoD/GC Paper, *supra* note 2.

49. ITU Convention, *supra* note 42, art. 34, S. Treaty Doc. No. 104-34.

50. *Id.*

51. *Id.*, art. 35.

52. DoD/GC Paper, *supra* note 2.

53. It is interesting to note that domestic US law concerning telecommunications, 47 US Code § 502, provides as follows:

> Any person who willfully and knowingly violates any rule, regulation, restriction, or condition . . . made or imposed by any international radio or wire communications treaty or convention, or regulations annexed thereto, to which the United States is or may hereafter become a party, shall, in addition to any other penalties provided by law, be punished, upon conviction thereof, by a fine of not more than $500 for each and every day during which such offense occurs.

The DoD/GC Paper notes that the Department of Justice's Office of Legal Counsel issued a written opinion stating that 47 US Code § 502 does not apply to US military personnel acting under instructions of the President as Commander in Chief, specifically referring to the October

1993 radio messages broadcast by the US armed forces to Haitians. DoD/GC Paper, *supra* note 2. This opinion does not cover, although it does not necessarily prohibit, such operations by non-military personnel.

54. United Nations Convention on the Law of the Sea, Dec. 10, 1982, art. 19, 1833 U.N.T.S. 397, 404 [hereinafter LOSC].

55. *Id.*, art. 19 (a), (c), (d), and (k).

56. DoD/GC Paper, *supra* note 2.

57. *See* LOSC, *supra* note 54, art. 3, 1833 U.N.T.S. 400.

58. Convention on International Civil Aviation, Dec. 7, 1944, art. 3(d), 61 Stat. 1180, 1181, 15 U.N.T.S. 295, 298 [hereinafter Chicago Convention].

59. *Id.*, art. 89, 61 Stat. 1205, 15 U.N.T.S. 356.

60. Vienna Convention on Diplomatic Relations, April 18, 1961, art. 41, 23 U.S.T. 3227, 3247, 500 U.N.T.S. 95, 120 [hereinafter Vienna Convention].

61. DoD/GC Paper, *supra* note 2.

62. *Id.* at 40.

63. *Id.* at 42.

64. *Id.* at 43.

65. *Id.*

66. *Id.* at 47. For an analysis of interagency problems associated with US defensive information operations, *see* Brian A. Persico, *Under Siege: The Jurisdictional and Interagency Problems of Protecting the National Information Infrastructure*, COMMUNICATION LAW CONSPECTUS, Winter 1999, at 153–172. For an analysis of information operations in military operations other than war, see THE CENTER FOR ADVANCED COMMAND CONCEPTS AND TECHNOLOGY, OPERATIONS OTHER THAN WAR (OOTW: THE TECHNOLOGICAL DIMENSION) (1995), at www.ndu.edu/inss/books/ootw/ootwhome. html.

67. *See* Bill Flynt, *Threat Convergence*, MILITARY REVIEW, Sept.–Oct. 1999, at Z-11 (listing the range of sources of threats, including terrorist and hackers).

68. *See generally*, DAVID S. ALBERTS, DEFENSIVE INFORMATION WARFARE (1996), www.ndu/edu/inss/books/diw/index.html. *See also* ROBERT H. ANDERSON, PHILLIP M. FELDMAN, ET AL., SECURING THE US DEFENSE INFORMATION POSTURE: A PROPOSED APPROACH (1999).

69. *See* DoD/GC Paper, *supra* note 2.

70. *Id.*

XIX

International Law of Armed Conflict and Computer Network Attack: Developing the Rules of Engagement

Brian T. O'Donnell and James C. Kraska

This chapter offers a framework for military commanders and policy makers to begin constructing rules of engagement (ROE) for computer network attack (CNA) during armed conflict, military operations other than war, and other overt and covert national security activities. Focused on the operational commander rather than the academic, it introduces the legal and policy considerations surrounding the drafting of ROE for CNA, and discusses the unique legal issues that arise from CNA within the law of armed conflict. Such considerations are important for military commanders, their operators, planners, and lawyers in designing and employing CNA because they serve to facilitate and provide guidance that operationalizes the concept of computer network attack—removing it from the realm of speculation and placing it as a tool in the hands of military commanders. Moreover, since legal and ROE decisions impact the development of tactics and doctrine, and the acquisition and force structure processes, the discussion is relevant to force providers and trainers, as well as fleet commanders.

Emerging Technologies and War

Over the last decade, information technologies, including computer and communications systems, have brought about a sea change in the global economy. Technology has grown from just 6% of the US economy at the beginning of the 1990s, to over 20% today.[1] What was once a narrow "technology" sector within the whole economy has emerged as the "New Economy," comprised of that third or fourth of the economy that serves as the source of rapid innovation and engine of economic growth.[2] Entire subsectors of the New Economy have emerged, and whole new industries have grown virtually overnight: photonics, micro-electrical mechanical (MEMs) devices, wireless systems and specialty communications semiconductors, and, of course, the Internet, which has become omnipresent throughout the economy. The New Economy has transformed industry data management and storage, manufacturing, accounting, and inventory management. Many of the same technologies have even more dramatically recast military communications, command and control, targeting, logistics and weapons.[3] These technological changes are transforming thinking about military force structure and doctrine, and have opened up computer network attack as a viable instrument of military power.

Military technology displayed by coalition forces during the Gulf War in 1991, particularly those technologies that were used by the United States military, ignited broad interest among strategists and policymakers worldwide in how to best develop or channel the emerging "revolution in military affairs" (RMA).[4] RMA, which encompasses technologies that "gather, process and fuse information on a large geographical area in real time, all the time,"[5] has driven the creation of new military capabilities and doctrine based on advanced concepts and emerging technologies. It grew from Cold War planning in the West that sought to apply technology as a force multiplier to counter numerically superior Soviet forces in Europe.[6] After the Cold War, RMA began to be seen as a way to ensure Western superiority, or at least preserve military advantage, in a broad variety of post-Cold War conflicts that might be encountered within the context of a resource-constrained defense budget environment. Computer network attack is one of the latest and most advanced manifestations of RMA. With the growth of computer networks and integrated systems, computers have assumed a central role in enabling both offensive and defensive military operations. Despite widespread recognition that the technologies that enable computer network attack are already a reality, the specific legal and policy considerations that will control their employment have received scant attention. This is not surprising, since the

development of concrete legal analysis tends to lag the advancement in technology, particularly in the application of international law to new methods of warfare.[7] It is equally important to recall that history is replete with examples in which superior military technology was squandered, and advantage was surrendered, because the army employing the new weapon had an inattentive or feckless approach to developing corresponding doctrine and tactics for its employment.[8] In the modern era, the development of appropriate ROE for CNA, along with operational doctrine, tactics, and force structure, will determine whether CNA is an effective weapon.

In the mid-1990s, the initial US focus on computers and military conflict resided almost exclusively in defending perceived weaknesses and vulnerabilities in critical national information infrastructure—especially electronic banking, communications, and industrial energy grids. This focus, which emerged within the Department of Defense (DoD) as "Information Warfare—Defense" (IWD) was replicated by other governmental agencies, who also became concerned after 1995 about the vulnerability of their networks, coinciding with the widespread use of the Internet.[9] All of these efforts migrated under the umbrella term, "Computer Network Defense" (CND), which has served to concentrate interagency resources and attention toward protecting and defending critical computer and information networks from sabotage by individual hackers, terrorist groups, and unfriendly governments.[10] Planning for CND was accelerated with the advent of Presidential Decision Directive 63 (PDD-63) in May 1998, which ordered federal agencies, in concert with the private sector and state and local authorities, to create defenses against attacks on critical infrastructures from network assaults from all State and non-State actors that potentially threaten American "national and economic security."[11] The DoD responded by standing up the Joint Task Force Computer Network Defense (JTF-CND), which was renamed Joint Task Force Computer Network Operations (JTF-CNO).[12] The JTF is assigned to Commander-in-Chief, United States Space Command, but has representatives from each military service and many government agencies.[13] The CND movement has made great progress in identifying information infrastructure vulnerabilities, and organizing and resourcing defensive interagency plans to address them. Initial panic at perceived gaping holes in critical information infrastructure has recently given way to a more measured and sober, and more confident, vulnerability assessment. Now that the concern over CND has stabilized, US planners, particularly in the military, have begun to more seriously consider the potential advantages to be gained in military operations by offensive attack against an adversary's information infrastructure.

Computer Network Attack

Computer network attack has emerged as one of the more promising tools available to a military commander for mission accomplishment and self-defense. It encompasses activities designed to ". . . disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."[14] While the legality of information warfare generally, or CNA in particular, is very fact-dependent and open to considerable debate, it has received at least some attention among international law scholars. Some scholars maintain that a CNA constitutes a use of force, whereas other scholars maintain that CNA is much more akin to adverse nonforceable influence.[15] This debate is healthy and serves to shape the international law in the area.

Despite the importance of CNA, military and civilian commanders have been unable to adequately explain it, or to achieve a consensus in designing CNA ROE. Moreover, military staff judge advocates, civilian lawyers within the national security and intelligence establishment, and academics are grappling with how to best articulate the legal and policy underpinnings for computer network attack decisions.

While theories and approaches that emerge from academia are useful to national decision-makers contending with these issues, they may be of limited value to operational commanders, including those at the Navy fleet and battle group levels. For the operational commanders, the legal and policy research surrounding CNA often raises more questions than it answers. This results in leaving those commanders who might integrate CNA into real-world operations confused and frustrated. Rather than offering a theoretical legal model for CNA, this chapter accepts the premise that CNA is quickly becoming a reality. There is a broad range of capabilities to attack computer networks that are in various stages of development, testing, and training, both in the United States and abroad. There is evidence that they are already being employed in actual operations by a growing number of nations. Furthermore, as these capabilities become better understood and easier to use, it is likely that the approval authority to employ them will gravitate downward in the chain of command to task force commanders. Eventually, proven methods of CNA could be authorized to individual units and platforms. This chapter presents a question of first impression by examining the development of operational CNA ROE for military operations, and it offers a practical approach to drafting CNA ROE. This pressing issue of exactly how a commander begins to approach the legal aspects of developing and applying CNA in the real world is on the cusp of wide discussions. There is a tremendous legal and policy gap—between rapidly advancing CNA

technical capabilities emerging from the laboratories—and the legal architecture to support them. The advancement of ROE for computer network attack, which has not kept pace with these developments, should begin to fill this gap. Determining the ROE process, considerations for creating the parameters of CNA engagement, and some guidelines for inclusion in operational orders are especially important for operational commanders executing real world missions. The commander should be able to understand which computer network and related military instruments may be used, under what conditions they may be employed, and to which missions they may be applied. This prevents a commander from either employing means or methods that lie beyond the scope of his or her authority, and ensures that the he or she does not unnecessarily limit the application of CNA because of confusion over the rules governing its use. There is a need to discipline and govern the process of development of ROE for CNA. The National Command Authorities (NCA) have a central stake in overseeing the process to ensure that the emerging CNA rules of engagement comply with international law and domestic legislation, as well as remain in concert with national military policy and national diplomatic and political goals.

For this chapter, we assume that some level of CNA is lawful within the context of international law, but the more practical question—indeed for commanders, the greater question—is how best to develop rules of engagement for an actual operation. The objective is to begin to fill in the vacuum pertaining to the control, application, and employment of CNA at the warfighting level.[16] Does the existing process for developing ROE adequately accommodate CNA? What can guide commanders, their warfighters, and operational judge advocates in developing rules for computer network attack? Is this an area best left to policymakers inside the beltway or is there a role for crafting rules for CNA at the operational level—forward deployed, at sea, or in the field? This chapter considers the historical basis for ROE, identifies the factors that fold into ROE development for computer network attack, explores the considerations that might limit or empower a commander, and suggests an architecture for designing computer network attack ROE that may be employed throughout the conflict spectrum. By providing a "navigational chart" to many of these issues, the goal is to begin to demystify the process for commanders and decisionmakers alike.

Historical ROE Development[17]

Modern ROE have their roots in the naval and maritime tradition. With the advent of oar and sail, effective central control of a military asset by the

sending government was lost once a ship got underway from port. It was incumbent upon the commanding officer to conduct the mission pursuant to the general guidance of the government. Virtually alone until the ship reached the next friendly port, or until the ship encountered another friendly vessel that could deliver news or orders, the commanding officer operated within broad parameters or rules issued by the leadership. The Continental Navy's first exposure to rules governing operations occurred on January 5, 1776, when Commodore Esek Hopkins received written orders to engage British raiders that included a broad discretionary clause of authority:

> Notwithstanding these particular Orders, which 'tis hoped you will be able to execute, if bad Winds or Stormy Weather, or any other unforeseen accident or disaster disable you so to do You are then to follow such Courses as your best Judgment shall Suggest to you as most useful to the American Cause and to distress the Enemy by all means in your power.[18]

Although modern technology has tremendously improved communication to underway vessels, naval vessels now routinely travel far from port, and transit much faster—sometimes even underwater—without access to detailed and real time guidance from a fleet commander or government leader. Prior to World War II, there was little need for a policy on use of force aside from occasional ships on diplomatic missions.[19] Following World War II regulations governing the use of force, now known as rules of engagement, were promulgated in the 1948 United States Navy Regulations with Article 0614, "Use of Force Against a Friendly State."[20] In 1962 the first in a series of ROE were issued that applied Navy-wide. Written to address the unique challenges and special concerns arising from surface, undersea, and aviation operations throughout the maritime environment, these ROE were subsequently updated in 1970 and 1981.[21] Even in the updated version, however, they still only applied to US naval forces.

In 1986, the United States issued generalized JCS Peacetime ROE that, for the first time, included guidance for air and land forces.[22] Two years later, following the experiences of the USS STARK (FFG-31) and USS VINCENNES (CG-49) in May 1987 and July 1988 respectively, the Peacetime ROE were again updated and revised. In 1994, a major revision was accomplished, and the ROE that applied to all US forces were promulgated by the Chairman of the Joint Chiefs of Staff as the Standing Rules of Engagement for US Forces (SROE)[23] Aside from the obvious title change that removed the "peacetime" reference, the 1994 document not only streamlined the ROE drafting and approval process, but also contained significant revisions, including a more

uniform approach. Separate ROE issued by the combatant Commanders-in-Chief (CINCs)[24] augment the SROE, and are referenced as "theater-specific" ROE.[25] This marked a break from past practice, in which each CINC had a theater-wide top-to-bottom set of rules. Also, the 1994 SROE clarified a commander's inherent right and obligation of self-defense, and articulated a bright-line distinction between self-defense and the use of force for mission accomplishment. For self-defense, the SROE are firmly grounded in responding to a hostile act or responding to a demonstration of hostile intent. One of the more significant changes was the declassification of the basic self-defense SROE provisions. This enhanced training and application throughout US forces and enabled better coordination between allies and coalition partners.

The most recent iteration of the SROE was released on January 15, 2000.[26] This latest version further refines and clarifies the concepts contained in earlier editions. It is comprised mainly of thirteen enclosures, including a separate enclosure for Information Operations. Unlike the 2000 revision, the 1994 edition contained little substantive mention of CNA, sticking mostly to definitional terms and basic concept statements. Under the SROE, use of CNA may be authorized to a commander under the umbrella of the mission ROE provisions and the international law of armed conflict (LOAC), subject to any additional supplemental authorizations or restrictions received from higher authority.[27]

Even though commanders of forces tasked to accomplish an operation or mission might be authorized CNA as a means of warfare, that does not mean they will decide to use it. Historically, personnel in the fleet or field did not question the ROE they were provided. Often, ROE were not well-understood within theater, or at the tactical level. Moreover, there was a sense that the ROE dictated from above could not be changed and were to be applied without question.[28] This was demonstrated during the 1981 Gulf of Sidra freedom of navigation operation off the coast of Libya. Prior to the operation, orders issued to the Navy F-14s restrained those forces from responding to indications of hostile intent even though the ROE in effect at the time authorized self-defense in response to hostile intent.[29] Another instance occurred during the bombing of the Marine Battalion Landing Team (BLT) Headquarters building in Beirut, Lebanon, in 1983, when a local commander's interpretation of the ROE led to orders for "sentries to keep their magazines in their ammunition pouches as a precaution against an accidental or over-eager discharge of a weapon that might kill or wound one of the thousands of Lebanese civilians who visited the airport daily."[30]

Innovation, Military Doctrine, and ROE

Limitations on the use of CNA may also fall victim to unnecessary restraint due to several factors. First, the complex and typically highly classified nature of CNA tools may not inspire confidence in commanders. They may be hesitant to rely upon bare promises that certain CNA tools can accomplish a mission, such as taking down an air defense site, when proven alternatives, such as air strikes or cruise missiles, are available. Commanders likely will have had training and experience with kinetic methods, but may not understand or appreciate CNA. During the 2000 Global War Game at the Naval War College, this dynamic was repeated by commanders who tended to move away from more speculative instruments toward those which were more familiar. This tendency toward traditional and proven methods of warfare has been demonstrated in war games of other services as well. Nevertheless, the war games also showed that US commanders were becoming more willing to adopt innovative methods to accomplish the mission, even when the methods lack historical record.

The military services are beginning to realize that to gain acceptance as a viable weapon system, the secretive nature of the tools must be reduced to a more accessible classified level so that commanders and their staffs and subordinate commands can familiarize themselves with the systems. Consider the development of the machine gun more than one hundred years ago. An American, Richard J. Gatling, patented and demonstrated a reliable, multi-barreled repeating gun in 1862, but the Belgian-invented and French-developed mitrailleuse was the first combat-tested machine gun.[31] On the eve of the Franco-Prussian war, the 11 mm mitrailleuse, recognized by the French army as a technical breakthrough in firepower, was kept in such tight secrecy in peacetime that very few French officers could discuss or develop doctrine or tactics for its use on the battlefield.[32] The weapon, which came as a complete surprise to the Germans, had the potential to swing victory to the French. Instead, advantage was lost because the French were caught up in marveling at the technical aspects of development without devising correspondingly effective doctrine and tactics for the weapon.[33] Similarly, although the Germans, British, and French were developing and fielding battle tanks during 1915-1916, they were ineffectively and wastefully employed on the battlefield. It was not until a coherent doctrine for their employment was developed—most notably by the innovative British strategist Major J.F.C. Fuller—that the tank was accepted as a viable weapon rather than a curiosity. On November 20, 1917, a spearhead of 476 British tanks penetrated German lines during the Battle of Cambrai, demonstrating that the armored vehicles could achieve rapid and complete command

of dug-in defenses.[34] Inertia prevents change, and we cannot assume that military commanders in the present day are immune from this phenomenon. Just as in the examples cited above, bringing ROE for computer network attack from the general and theoretical to the specific and concrete will help commanders migrate to computer warfare.

The method by which CNA will accomplish its end result likewise needs to be explained to commanders, and commanders need to be able to engage in professional debate on the subject. The ROE relate to the underpinning international and domestic authority for using CNA, the scope of the commander's authority within the context of the national and theater commander's mission, and the conditions, if any, in which CNA is considered a lawful attack. One especially important consideration is the potential for collateral effects of CNA in view of the law of armed conflict. How might CNA affect third countries or neutral forces beyond the scope of the conflict? What might be the effect on civil societies, civilian populations, businesses, and related public and private infrastructure? What impact might CNA have on protected persons or locations, such as sick and wounded personnel near the battle area or sites representing religious or cultural heritage? What about the effect on prisoners of war (POWs) and other protected classes of personnel, such as medical or religious personnel? Any anticipated or probable primary or secondary civilian injury or damage must be reviewed to determine whether it is excessive or disproportionate to the military advantage to be gained. Commanders are coming to view these issues personally and with growing interest since they bear the ultimate responsibility for the consequences of an attack. The trend toward creating universal multilateral "war crimes" jurisdiction only serves to exacerbate many commanders' uneasiness toward command and personal liability.

The first step is for a commander to be able to understand the foreseeable consequences of a CNA attack, including damage or disruption to non-military systems. A review of the potential consequences within the ROE and LOAC framework is essential to forming a decision on the use of CNA. In particular, commanders must estimate the expected military benefit of CNA, and weigh that calculation against the collateral costs of attack. Ideally, the commander should be supported by an ROE cell that can present a menu of options. The cell should include representatives from the operations, intelligence and plans directorate, as well as a judge advocate. The cell should analyze ROE, targeting and politico-military issues associated with CNA, and deliver recommendations to the commander.

Commanders are rightly hesitant to employ unproven systems as one critical component of a coordinated attack because if the CNA component fails, then

the entire effort is imperiled. Inherent risk is already attendant to real world missions without the injection of an unproven, and possibly speculative system. Doubt as to legality and ROE would only serve to magnify these concerns. Compounding this problem may be the short life span of the attack due to rapid advance in technology and creative enemy adaptation. Even more so than conventional weapons systems, once the impact of a particular CNA has been experienced, adversaries can be expected to devise a tailored defense, thereby limiting future effectiveness.[35] Moreover, the comparatively low cost and global availability of computer systems and trained programmers enables terrorist groups or developing nations to enter the realm of information and computer warfare. All of these factors serve to keep CNA tools underutilized, thereby foregoing potential military benefit. Doing so deprives a commander of the opportunity to observe its effectiveness in training or on lesser targets prior to applying it to a major target. A successful laboratory demonstration is not likely to do much to dissuade this opinion. As legal analysis continues to lag technological breakthrough, we can expect that without great attention, the development of mission-specific ROE for ever newer computer network attack systems will be a challenge.

Understanding this background, proponents of the new technology are beginning to realize that not only must they be able to adequately explain and demonstrate CNA, but they must also ensure that the commander understands how it functions. Computer network warfare and information operations are upsetting the existing Westphalian paradigm of warfare upon which traditional ROE and law of war are based. The very nature of CNA is rapidly changing. For instance, some suggest that the architecture of CNA is migrating from the traditional model of "waves" of attack to a model based on a simultaneous "swarming" or overtaking of an opponent's system. "Swarming occurs when the dispersed nodes of a network of small . . . forces converge on a target from multiple directions. The overall aim is sustainable pulsing of a force or fire."[36] Once in motion, swarm networks must be able to coalesce rapidly and stealthily on a target, dissever and redisperse, and then immediately recombine for a new pulse. In other words, information-age attacks may come in swarms rather than the more traditional waves.[37] Such a paradigm shift could completely transform the way many elements of ROE are applied in computer network attack. The concepts of "hostile act" and "hostile intent," for example, best fit a linear "wave" model, in which State action is directed toward another State in waves along a timeline—often becoming more permissive or aggressive as time lapses. Crisis war games bear this out; often, military exercises begin with a "Road to War" prelude of rising political tensions that gradually escalate into military confrontation. Then, conflict

slowly accelerates from peacekeeping to peace enforcement. The multilateral US-Thailand-Singaporean series of unclassified COBRA GOLD 00 and 01 exercises were built from this model. Crafting suitable ROE for those scenarios exposed the lack of flexibility inherent in a linear focus.

Swarming attacks would pose, simultaneously, a confusing mixture of actions by a State or non-State actor against a State, with some actions perhaps tantamount to a "hostile act" or demonstration of "hostile intent." At the same time, other actions would fall below that threshold, confounding the development of ROE.

> The blurring of offense and defense reflects another feature of net-war: it tends to defy and cut across standard boundaries, jurisdictions, and distinctions between state and society, public and private, war and peace, war and crime, civilian and military, police and military, and legal and illegal. A government has difficulty assigning responsibility to a single agency—military, police, or intelligence—to respond.[38]

Of course, this generates confusion over developing a common understanding of rules of engagement as the DoD vies with international and multilateral organizations, international coalition partners, a host of other federal agencies, state and local law enforcement, and private business to develop ROE. Lines of authority will crisscross, and the "operational paradigms of politicians, officials, soldiers, police officers, and related actors get fuzzy and clash."[39] In particular, the military's ROE, which are developed for military operations, may conflict with other agencies' approaches, which are often based on law enforcement. These fundamental questions must be addressed before mission-specific legal analysis can be thoroughly conducted. The essential law of armed conflict and generalized military rules of engagement for CNA, however, can be developed as a point of departure for policy and planning. This will enable commanders to begin a dialogue within the defense establishment and with their counterparts outside the military, facilitating interagency cooperation and action.

The ROE Process

The SROE has added granularity to what many commanders had realized all along—that they are ultimately responsible for developing and applying ROE. This responsibility cannot be abrogated to the Staff Judge Advocate or other directorate. During crisis action planning, the Director of Operations (J3) is key to generating options and ranking the choices available to the commander. When

engaged in deliberate planning, the Director of Strategic Plans and Policy (J5) is the central player. These directorates are closely assisted by the judge advocate, who serves as a facilitator to ensure that the principles of international and domestic law are honored.[40] Toward this end, subject matter experts are critical to forming meaningful ROE. Generally, the Director of Intelligence (J2) and the Director of Command, Control, Communications and Computers (J6) are key advisors regarding CNA capabilities and limitations.

Toward a Results-Based Model

During the drafting process, a "results-based" approach to ROE should be given preference over broad grants of authority to engage in CNA. Results-based ROE tie CNA into a specific mission type, along with the expected, as well as the desired, political or military effect. Using an air defense unit as an example, CNA ROE might be written to authorize CNA to disable an air defense site for a specific period of time in order to accomplish one part of an overall mission. This could prove extremely useful when the alternative of kinetic attack might release dangerous forces, physical destruction of the site is not required, or physical destruction might cause excessive collateral damage or adverse political consequences. CNA, by contrast relies upon a data stream to execute an attack, such as sending an attacking code to an air defense system computer, causing the power supply to short out. This is in contrast to using the electromagnetic spectrum, such as an electromagnetic pulse, that relies upon kinetic energy to obtain a similar result.[41]

Many commanders are concerned about the delay required to obtain supplemental ROE approval, especially if the requested rules require NCA approval.[42] During joint and combined exercises in the Western Pacific, scenario events typically overtook requests for supplemental ROE, as superseding events made the supplemental request irrelevant by unfolding scenario events. The same dynamic occurs in the real world, and the introduction of computer network attack ROE can only decelerate the process. One method that might speed this process along has been to request supplemental rules early in a scenario, delegating authorization to approve the ROE to a level closer to the commander ultimately charged with its use. For example, a combatant regional CINC might be delegated authority in advance for actions that would normally require NCA approval. Additionally, the supplemental ROE might be authorized pending occurrence of a certain set of events or tripwires. This type of thinking was evident in discussions with Australian operators and attorneys during Exercise TANDEM THRUST 99.[43] In the Australian Defence Forces, this concept is called "dormant ROE," and it may

prove to be adaptable to CNA ROE. In "dormant ROE," a set of pre-authorized supplemental or mission-specific rules becomes effective upon some triggering event or receipt of a specialized code word. This method has the advantage of commanders being able to see in advance the level at which authorizations will be given depending upon how a particular mission develops, rather than waiting for change to occur during the mission. This avoids the commander having to address ROE that are suddenly inadequate, and ameliorates the need for additional rules in the midst of a crisis. It would also let the military personnel involved in the mission train for a change in ROE with the actual rules that would apply. Personnel familiar with US and Australian ROE will quickly point out that while the American ROE are permissive in nature and US commanders feel comfortable with broad grants of authority without the need to have specific grants of authority, the Australian rules are more restrictive. However, in dealing with CNA, US commanders should expect more restrictions. When a commander is granted authority to employ CNA, a limited authorization will most likely be the norm. This will be the case until such time as decision makers become more comfortable with this new method of warfare, and the ROE mature. One way to accomplish this, without actual use in a conflict, is to better integrate CNA into war games and exercises. In the last two years in particular, ROE addressing computer network attack and defense have begun to enter the exercise lexicon. Unfortunately, war games and exercises still rarely contain an ROE development phase where supplemental rules are discussed and developed. The concepts should be gravitating more quickly from the national or theater levels to the operational and battle group levels. It is even rarer for the CNA procedures and effects to be explained, or the rules for their employment to be debated in the fleet. The highly classified nature of CNA serves to exacerbate this problem.

Training and Gaming ROE

Over the last two decades, the rules of engagement have matured considerably. Captain J. Ashley Roach, USN (ret.) recognized the need for greater understanding of ROE and practice prior to conflict when he wrote nearly twenty years ago:

> There is a very real need for greater knowledge of rules of engagement on the part of strategy and policy personnel, tacticians and operators, and even by our civilian leaders. At present these rules are rarely, if ever, exercised and too few planners and commanders seek contingent approval for additional or relaxed rules.[44]

Since that time, judge advocates and commanders have made great progress in integrating ROE with operations. Due to the rapid advance in capabilities and the explosion of computer networks in civil and military infrastructures throughout the globe, computer network attack has emerged as one of the few areas that require more immediate attention. Typically, when any type of CNA is included in a war game or exercise, a judge advocate is given the task of crafting ROE for their use, usually without operator input or a full understanding of the mission it is supporting. The problem of lawyer-operator decoupling during the drafting of ROE is certainly not unique to computer network attack issues. Nonetheless, the process of an attorney crafting ROE without the input of other staff representatives—the intelligence and operations directorates in particular—may yield rules that do not serve the commander's complete package of political and military goals. In exercises, CNA events often are handled "notionally." That is to say the "Blue" or "Red" team will state its intention to use CNA for an event, applying pre-authorized ROE developed prior to the game, and they will be informed by the exercise control group that the effort either succeeded or failed. Even when a supplemental ROE request is sent up the chain-of-command to the NCA, there is usually no discussion of the actual method to be employed, making the event much more of a showcase assumption than an actual exercise. Moreover, neither the Blue or Red force, or even the control group, has an understanding of the mechanics of the CNA and how it will operate, particularly the potential collateral effects—expected or unexpected. Ideally, there will be a military attorney advising the exercise control group that can work with the control staff to determine legal effects of CNA. One part of this analysis that might benefit from more attention is whether CNA affects persons with protected or special status under international law.

"Train As We Type"

No matter what shape the ROE begin to take, if we do not train like we actually anticipate utilizing a CNA tool, commanders may not have confidence in its use. Moreover, decision makers will lack confidence in their authorization. Incrementally, progress on increased use of CNA in war games and experiments is unfolding, much like early use of the concept of responding in self-defense based upon a demonstration of hostile intent. Many might assume this concept has been around forever—but although it was adopted into early US ROE and expressed as an inherent right under individual and unit self-defense, this did not guarantee acceptance or use.[45] Discussing the August 19, 1981, shoot-down of two Libyan Su-22 fighters by US Navy F-14s, Captain Roach observed:

> It is a common misperception that under the peacetime ROE a commander must "take the first hit" and cannot act in self-defense until the opposing force has missiles away. That is not the law and is not required by our general peacetime ROE.[46]

Interestingly, the tools and technologies for initiating computer network attack are expanding at a rapid pace, unsettling the associated ROE and complicating the ability of attorneys and commanders alike to fashion widely accepted principles. On the other hand, through the process of incorporating CNA into realistic war games and experiments, the familiarity of future decision makers and commanders is increasing. Once CNA is an option available in time of crisis, deliberate planning during an armed conflict or other military operation will expand the panoply of available tools for use by the commander. This offers flexibility, asymmetric action, and potentially reduced casualties among both friendly forces and opponents alike. In turn, it promises to favorably mold the political outcome.

Disciplining CNA

The surest way to control the use of CNA is to keep its authorization at the NCA level. Doing so simplifies the decision making process for the commander in the field, but it does so at the expense of removing a flexible instrument from his or her inventory. This approach tends to move away from the traditional American position on ROE construction that empowers military commanders with all necessary authority to accomplish an assigned mission, so long as the ROE are not limited by higher authority.[47] The goal should be to exercise and prepare task force and group commanders to engage opposing forces with computer network attack, but to do so according to accepted criteria or rules. Thus, we need to migrate from an ad hoc approach to ROE for CNA to a more routine crisis action checklist appropriate for its employment. Any such checklist would have to be frequently updated to reflect advances in computer technology. Only by standardizing rules for initiating ROE will commanders become comfortable with exercising independent judgment on how, when, where, and against whom to employ CNA. This requires judge advocates to convince commanders, and perhaps innovative technical developers, that computer network attack is properly analyzed within the traditional ROE and LOAC paradigm with which our leadership has grown accustomed. Of course, questions remain—and the dispositive issue of whether a computer network attack constitutes a "use of force" (and if so, what kind of force)—looms large in the

background.[48] Still, it would be shortsighted to await the resolution of this and other politico-legal debates before the military begins to think about a legal model for computer network attack. With that in mind, the existing approach of rules of engagement, embedded within the law of armed conflict, has several advantages. The construct is familiar within the United States and abroad, and it is accepted as a global standard for ameliorating the effects of military operations. It is also flexible and adaptable, and reflects hundreds of years of developmental thinking, so it is a solid foundation on which to build. Most importantly, to the extent that the law of armed conflict has been respected and observed in times of conflict, it has alleviated suffering, limited destruction and spared civilian casualties.

Law of Armed Conflict

The basic framework for all discussions of the laws of armed conflict center around the four principles that evolved from customary international law and subsequently codified in the Hague and Geneva Conventions. These principles are: military necessity, distinction, proportionality, and chivalry. They frame all military activities in armed conflict, and thus must be understood by policy makers and war fighters alike. Military necessity is a cornerstone principle of military action. A commander may employ only that degree and kind of force, not otherwise prohibited by the law of armed conflict, required for the partial or complete submission of the enemy. A minimum expenditure of time, life, and physical resources may be applied.[49]

As reflected in Article 49 of Additional Protocol I to the 1949 Geneva Conventions, distinction ensures "respect for and protection of the civilian population and civilian objects . . . ."[50] Article 51 protects civilian populations, and 51(4) defines unlawfully indiscriminate attacks as: (a) those which are not directed at a specific military objective; (b) those which employ a method or means of combat which cannot be directed at a specific military objective; or (c) those which employ a method or means of combat the effects of which cannot be limited as required by Protocol I. Consequently, military strikes must distinguish between lawful combatants and civilians.[51] It would be a violation of LOAC to use civilians or a protected place or property to shield combatants or a valid military objective. The presence of civilians within or near a legitimate military target does not make an attack unlawful.

In the fog of modern war, in which a State's entire society becomes vested in warfare, it is especially difficult to distinguish between lawful and unlawful targets:

> One related issue is the extent that commanders could order preemptive or responsive attacks against non-state targets. It's not just the military. The Chinese, for example, put a lot of emphasis on people's information warfare—encouraging individuals to use their own technology to annoy and attack others.[52]

As we enter the computer warfare age, nations will attempt to further exploit this difficulty.

Loss of life and damage to property incidental to attack must not be excessive in relation to the concrete and direct military advantage expected to be gained. This concept of proportionality defines "concrete and direct" military advantage as "the advantage anticipated from the specific military operation of which the attack is a part taken as a whole and not from isolated or particular parts of the operation."[53] Collateral damage and incidental injury have historically been the product of three factors: (1) a lack of full knowledge as to what is being hit; (2) the inability to surgically craft the amount of force being applied to the target; and (3) the inability to ensure that the weapon strikes precisely the right point.[54] On the digital battlefield, collateral damage could affect entire sectors of the economy and society.

Finally, the main tenets of chivalry center around the principles of treachery and perfidy. The 1977 Additional Protocol I bans ". . . acts inviting the confidence of an adversary to lead him to believe that he is entitled to, or is obliged to accord, protection under the rules of international law applicable in armed conflict, with intent to betray that confidence. . . ."[55]

Perfidy includes: 1) feigning of intent to negotiate or surrender, 2) feigning incapacitation, 3) feigning civilian, noncombatant status, and 4) feigning protected status by use of signs or uniforms of the UN or neutral states. Ruses, however, are not prohibited in an armed conflict.[56] Legitimate ruses include camouflage, deceptive lighting, decoys, mock operations, simulated forces and use of enemy codes and passwords.[57] These long-standing principles of international law have direct bearing on possible future CNAs that might rely upon e-mail delivery. One author has advanced the premise that:

> While chivalry may seem archaic today, it retains some normative value. . . [by] analogy [it] strongly weighs against sending a logic bomb disguised as e-mail from the International Committee of the Red Cross (ICRC) or even from "Microsoft Software Support". . . . [S]uch a message might be permissible without perfidious labels. Using ICRC and Microsoft tags would constitute an illegitimate act of perfidy, much as would disguising any dangerous military intruder in the form of an innocuous invitee.[58]

With the principles of LOAC in mind, a commander must also possess additional information prior to requesting permission for, or directing, a CNA. As a practical matter, the commander must know the target—is it a network, link, facility or person? He or she must also understand the effect—both military and cascading or collateral—the CNA will cause.

What is the Target?

Determining the target, and evaluating its lawfulness, will continue to be a focus of rules of engagement, and attacks against information systems are no exception. Whether the target is purely military or civilian, or nominally civilian but intertwined with military purposes or uses (dual-use) is central to this analysis. In the computer network attack realm, achieving "Supervisory Control and Data Acquisition" (SCADA) over a target is often the objective. SCADA is the computer control of a power system, railroad or sewer system, or fresh water system. Over the last twenty years, the US military has relied more on targeting dual-use infrastructure systems. As this infrastructure becomes modernized and networked in most nations throughout the world, reaching system SCADA on a variety of lucrative targets is quickly becoming a milestone in any military operation.[59] At least one proponent has argued that the targeting of electric power distribution and civilian bridges is a violation of Additional Protocol I.[60] The Basic Rule of Article 48 states, "In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives." Article 51 (4) states, "Indiscriminate attacks are prohibited."[61] Article 51 (2) states: "The civilian population as such as well as individual civilians shall not be the object of attacks. Acts or threats of violence, the primary purpose of which is to spread terror among the civilian population, are prohibited."[62]

Cascading Effects

Other than the desired military impact, what other probable and possible effects—cascading effects—can the CNA cause? Once such effects are assessed, the principle of proportionality must be examined. This would require an analysis of whether civilian systems will be affected. Is any damage excessive in light of the definite military advantage anticipated? What is the threshold of allowable civilian damage? Are there alternative means available to accomplish the mission?

Getting these answers is the toughest part of the process. Intelligence might be lacking, collateral effects may not be clearly understood, and the infrastructure being attacked may not be fully comprehended. Uncertainty is the order. In some ways, a CNA could be considered like a kinetic, indirect fire weapon. Firing a weapon into an area, even during combat, without proper intelligence, observation, and identification of valid targets is generally unlawful.[63] In much the same way, launching a CNA without sufficient understanding of the system being attacked would be improper. Add to that the fact that the weapon itself, in this case a CNA tool, and its effects on a given target system and other linked collateral systems may be poorly understood. That is not to say that the CNA tool will not have been reviewed prior to being placed in inventory—for the United States and many other nations, it is a prerequisite that a weapons review be accomplished prior to it being authorized for use.[64] However, unlike a hand grenade, CNA might have different effects depending upon the system it is launched against. Additionally, as technology changes, CNA might not have the same effect originally anticipated. Also of concern, due to the complex nature of computer programming and principles, is how the commander in the field will ever hope to reach the same level of understanding as computer and policy experts. Can he rely upon another's judgment when he is the one "pulling the trigger" by pressing the keyboard? Will this satisfy his requirements under international law? What is the minimum level of knowledge the commander must possess? Must the commander—

- understand what the targeted system does and how it operates?
- understand how and what CNA will do to the targeted system?
- be in a position, either through intelligence or direct observation, to judge the effects of the attack?
- determine what other systems share or are linked to the target system and how those other systems operate and what they control?
- determine what impact the CNA tool will have on the non-targeted shared or linked system?

Blurring Lines: CNA ROE for Self-Defense

Up to this point we have concentrated mainly on CNA ROE for mission accomplishment. However, a brief discussion of the use of CNA in self-defense is worthy of examination.

The 2000 SROE position on actions for self-defense seems to be clear: "These rules do not limit a commander's inherent authority and obligation to use all necessary means available and to take all appropriate actions in self-defense of the commander's unit and other US forces in the vicinity."[65]

It follows, then, that if CNA has been placed into the available inventory of weapons, it would be available for actions in self-defense, subject only to authorization by higher authority. Does the novelty of the weapon or the periodic comparison of CNA to a weapon of mass destruction (WMD)[66] alter the conditions precedent for the exercise of self-defense, namely necessity and proportionality?[67] If the CNA use conforms to the four LOAC principles, then characterizing CNA as a WMD is a dubious analogy. Although CNA is, at least for the present, a novelty, it does not require creation of an entirely new ROE. The unfamiliarity with CNA, the secrecy with which it is treated, and, perhaps most importantly, the misperceptions it may cause, could increase provocation and escalation. The SROE already stretches to accommodate these considerations.[68] However, taking CNA off the table for self-defense may be restricting an otherwise valid option for self-defense. If specifically tailored, CNA has the potential to remove or counter a hostile act or hostile intent threat in a "human-friendly" fashion. Unlike a kinetic weapon, CNA can disable systems without injuring civilians.

Concluding Comment

This chapter focuses on the process of developing rules of engagement for CNA within the greater context of the international law of armed conflict. It does not address the general lawfulness of CNA in international law, except as it bears on use of force, targeting, and the ROE process. That question is largely academic, often lying outside the immediate needs of the operational commander and forward-deployed judge advocate. Moreover, much of the analysis to date, tends toward the theoretical and thus is of greater interest and utility to scholars than operational commanders.

By offering some practical principles for developing ROE, we hope to begin closing the gulf between theoretical discussions of CNA and its operational application by theater and task force commanders. The ROE process includes developing the rules within the context of the law, doctrine, and force structure, as well as the boundaries of the mission. During the developmental process, and throughout the application of CNA across the conflict spectrum, the commander should be personally involved. ROE drive CNA and have a dispositive effect on the political and military landscape.

Notes

1. As measured by the technology sector of the Wilshire 5000, often referred to as the Total Stock Market Index, which is the largest index market in the world and provides a broad measure of trends in stock prices across the whole of the market. The Wilshire 5000 consists of approximately 7,000 US-based stocks traded on the New York Stock Exchange, American Stock Exchange and NASDAQ. *See* www.wilshire.com.

2. *See generally*, GEORGE GILDER, MICROCOSM: THE QUANTUM REVOLUTION IN ECONOMICS AND TECHNOLOGY (1990).

3. *See* John Arquilla and David Ronfeldt, *Cyberwar is Coming!*, 12 Comparative Strategy No. 2, 141–165 (1993).

4. Nicholas Lemann, *Dreaming About War: Someone in the Pentagon is Staging a Defense Revolution—and It's Not the Generals*, NEW YORKER, July 16, 2001, at 32. For recent debates on the revolution in military affairs, see Project on Defense Alternatives, RMA Debate, www.comw.org/pda/.

5. William A. Owens, *The American Revolution in Military Affairs*, JOINT FORCE QUARTERLY, Winter 1995–96, at 37.

6. For example, the deep strike concept of "Follow-on Forces Attack" (FOFA) was intended to design forces that would interdict Soviet mechanized and armored forces along the entire path of their attack into Western Europe—beginning at their starting point positioned at barracks and depots in Eastern Europe and the Soviet Union, throughout the entire course of their transit westward to the front in Western Europe. *See* F.W. VON MELLENTHIN ET AL., NATO UNDER ATTACK 12 (1984). The technologies and doctrine that grew from FOFA were applied with stunning results during the Gulf War, and are best illustrated by the tremendous devastation of Iraqi forces fleeing northward from Kuwait along the "highway of death."

7. Sean P. Kanuck, *Information Warfare: New Challenges for Public International Law*, 37 HARVARD INTERNATIONAL LAW JOURNAL 272 (Winter 1996).

8. *See* GEORGE M. CHINN, THE MACHINE GUN: HISTORY, EVOLUTION AND DEVELOPMENT OF MANUAL, AUTOMATIC, AND AIRBORNE REPEATING 65–68 (1951).

9. GARY F. WHEATLEY AND RICHARD E. HAYES, INFORMATION WARFARE AND DETERRENCE, 17–22 and 29–30, December 1996. *See also* Office of the Undersecretary of Defense for Acquisition & Technology, Report of the Defense Science Board Task Force on Information Warfare—Defense (IW-D), November 1996.

10. Report of the President's Commission on Critical Infrastructure Protection: Critical Foundations Protecting America's Infrastructures (Oct. 1997).

11. Alan D. Campen, Intelligence is The Long Pole in the Information Operations Tent, Mar. 30, 2000, www.infowar.com.

12. MG James D. Bryan, USA, Commander JTF-CNO, USCINCSPACE, Statement Before the House Armed Services Committee May 17, 2001, www.house.gov/hasc/openingstatementsandpressreleases/107thcongress/01-05-17bryan.html. *See also* Hon. Linton Wells II, Assistant Secretary of Defense for Command, Control, Communications and Intelligence (Acting) and DoD Chief Information Officer, Hearing on Information Assurance, Statement Before the House Armed Services Committee May 17, 2001, www.house.gov/hasc/openingstatementsandpressreleases/107thcongress/01-05-17wells.html.

13. *Id.*

14. Chairman of the Joint Chiefs of Staff, Joint Pub. 3-13, Joint Doctrine for Information Operations, GL-5 (1998), www.dtic.mil/doctrine/jel/operations.htm.

15. *See* Richard W. Aldrich, *The International Legal Implications of Information Warfare*, Institute for National Security Analysis Occasional Paper 9, US Air Force Academy, April 1996, at ix and 6–7; M.E. Bowman, *Is International Law Ready for the Information Age?* 19 FORDHAM

INTERNATIONAL LAW JOURNAL 1935 (1996); Kanuck *supra* note 8, which were among the first to address the issue. *See also* LAWRENCE T. GREENBERG ET AL., OLD LAW FOR A NEW WORLD? THE APPLICABILITY OF INTERNATIONAL LAW TO INFORMATION WARFARE (1997), which was republished by the Institute for International Studies, Stanford University, and revised in 1998 by the Institute for National Strategic Studies, National Defense University under the title INFORMATION WARFARE AND INTERNATIONAL LAW. Analysis from current or former judge advocates include Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUMBIA JOURNAL OF INTERNATIONAL LAW 885 (1999); Roger D. Scott, *Legal Aspects of Information Warfare: Military Disruption of Telecommunications*, 45 NAVAL LAW REVIEW 57 (1998); and W. GARY SHARP, SR., CYBERSPACE AND THE USE OF FORCE (1999). Within the Pentagon, the most authoritative address of the issue is a White Paper from Office of General Counsel, Department of Defense, An Assessment of International Legal Issues in Information Operations (Nov. 1999). The paper is appended to this volume as the Appendix.

16. The warfighting or operational level is defined as that intermediate level of military operations between the national or strategic and the individual or small unit tactical level, and includes, in the US Navy, the numbered fleet, carrier battle groups, amphibious groups and squadrons, and in the USMC, the malleable Marine Air-Ground Task Force (MAGTF). *See* Edward N. Luttwak, *The Operational Level of War*, INTERNATIONAL SECURITY, Winter 1980–1981, at 61–79.

17. Discussions with Jack Grunawalt, Professor (Emeritus), Naval War College, in Newport, RI (May 2001); Brian O'Donnell, Rules of Engagement (Oct. 1999–Jun. 2001) (unpublished Naval War College course material on file with authors).

18. JOSEPH BOUCHARD, THE USE OF NAVAL FORCES IN CRISIS 638 (1990).

19. *Id.* at 250.

20. US Navy Regulations, 1948, art. 0614:

> The use of force by United States naval personnel against a friendly foreign state, or against anyone within the territories thereof, is illegal. The right of self-preservation, however, is a right which belongs to states as well as to individuals, and in the case of states it includes the protection of the state, its honor, and its possessions and the lives and property of its citizens against violence, actual or impending, whereby the state or its citizens may suffer irreparable injury. In no case shall force be exercised in time of peace otherwise than as an application of the right of self-preservation as above defined. It must only be used as a last resort, and then only to the extent which is absolutely necessary to accomplish the end required. It can never be exercised with a view to inflict punishment for acts already committed.

21. Peacetime Rules of Engagement for US Seaborne Forces (1981).

22. Peacetime Rules of Engagement for US Forces (1986).

23. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3121.01, Standing Rules of Engagement for US Forces (1994).

24. Joint Chiefs of Staff, Joint Pub. 0-2, Unified Action Armed Forces (1995), www.dtic.mil/doctrine/jel/capstone.htm.

25. USCINCPAC, USCINCEUR, and USCINCCENT have all supplemented CJCS SROE with theater-specific ROE.

26. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3121.01A, Standing Rules of Engagement for US Forces (2000) [hereinafter SROE]. The basic instruction is unclassified, but contains substantive topical classified enclosures.

27. For a discussion of SROE, see R. J. Grunawalt, *The JCS Standing Rules of Engagement: A Judge Advocate's Primer*, 42 AIR FORCE LAW REVIEW 245 (1997).

28. *Supra* note 17.

29. *Id. See also* A.R.Thomas, Joint Tactical Command and Control Course on Rules of Engagement (Feb. 25, 2000)(unpublished, on file with authors). The Task Group Commander is attributed as telling the pilots not to worry about the definition of hostile intent since that was the Admiral's job. The pilots were directed to just relay all Libyan aircraft information, such as armaments, maneuvering, speed, etc., back to the Admiral who would decide if the aircraft were hostile. Interestingly, Professor Grunawalt discussed this with commander years after the operation and he indicated that it was not his intent to limit the pilots' right of self-defense. The authority to respond to hostile intent is founded upon the theory of anticipatory self-defense under international law. For a historical discussion of anticipatory self-defense see G. K. Walker, *Anticipatory Collective Self-Defense in the Charter Era: What the Treaties Have Said*, 31 CORNELL INTERNATIONAL LAW JOURNAL 321 (1998). See also YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENCE (3d ed. 2001) for a discerning distinction between "anticipatory" self-defense, which he indicates is not permitted, and "interceptive" self-defense which is permissible under Article 51 of the UN Charter.

30. Bradd C. Hayes, Naval Rules of Engagement: Management Tools for Crisis (RAND, CA), July 1989, at 14 *citing* DAVID C. MARTINE AND JOHN WALCOTT, BEST LAID PLANS: THE INSIDE STORY OF AMERICA'S WAR AGAINST TERRORISM 121 (1988).

31. JOHN ELLIS, SOCIAL HISTORY OF THE MACHINE GUN 16–20 (1975).

32. F.W. VON MELLENTHIN ET AL., NATO UNDER ATTACK 12–13 (1984).

33. *Id.*

34. ERIC MORRIS ET AL., WEAPONS & WARFARE OF THE TWENTIETH CENTURY, 131–132 (1975).

35. *See* MARTIN VAN CREVELD, TECHNOLOGY AND WAR: FROM 2000 B.C. TO THE PRESENT (1991); JOHN KEEGAN, THE FACE OF BATTLE (1976).

36. John Arquilla et al., *Networks, Netwar, and Information-Age Terrorism*, *reprinted in* IAN O. LESSER ET AL., COUNTERING THE NEW TERRORISM 54 (1999).

37. *Id.*

38. *Id.*

39. *Id.* at 55.

40. SROE, *supra* note 26, at L-1.

41. Joint Chiefs of Staff, Joint Pub. 1-02, DoD Dictionary of Military and Associated Terms, 88 (2001), www.dtic.mil/doctrine/jel/ref.htm.

42. During the authors' experiences with several USCINCPAC bi-lateral exercises with US Pacific Command Partner Nations in the Western Pacific from 1999-2001, communications difficulties and the rapid pace of the exercises made it more difficult to obtain rapid approval of supplemental ROE requests.

43. Exercise TANDEM THRUST is a biennial Australian-US exercise held in the Pacific and uses a common set of classified ROE called the Combined Rules of Engagement (CROE) for Australian and US forces (on file with authors).

44. J. Ashley Roach, *Rules of Engagement*, NAVAL WAR COLLEGE REVIEW 46, Jan.–Feb. 1983. *See also* F. M. Lorenz, *Rules of Engagement in Somalia: Were They Effective?*, 42 NAVAL LAW REVIEW 62 (1995).

45. Roach, *supra* note 44, at 49. The central question by US Navy commanders was, "Do I have to take the first hit?" This question was definitively answered in the negative by Captain Roach in his article, nonetheless, it took more than a decade for commanders to fully internalize this rule.

46. *Id., citing to* T. Wood Parker, *Thinking Offensively*, US NAVAL INSTITUTE PROCEEDINGS, Apr. 1981, at 29 (footnote omitted). *See also* George Bunn, *International Law and the Use of Force in Peacetime: Do U.S. Ships Have to Take the Fist Hit?*, NAVAL WAR COLLEGE REVIEW 69–80, May–Jun. 1986. Also of note is that some eight years earlier authority to respond to a threat of force

was articulated in US Navy Regulations, art. 0915 (1973) which reads: "The right of self-defense may arise in order to counter either the use of force or an immediate threat of the use of force."

47. SROE, *supra* note 26, at J-1.

48. *See generally*, Schmitt, *supra* note 15.

49. The Hague Convention of 1907, Article 22, protects human life by stating "The right of belligerents to adopt means of injuring the enemy is not unlimited." Convention (IV) Respecting the Laws and Customs of War on Land, Hague, Oct. 18, 1907 *reprinted in* THE LAWS OF ARMED CONFLICTS: A COLLECTION OF CONVENTIONS, RESOLUTIONS AND OTHER DOCUMENTS 84 (Dietrich Schindler & Jiri Toman eds., 3d ed. 1988)[hereinafter Hague IV]. Article 23(g) does the same for property by stating "[it is especially forbidden] to destroy or seize the enemy's property, unless such destruction or seizure be imperatively demanded by the necessities of war."

50. Protocol I Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, opened for signature Dec. 12, 1977, art. 48., 1125 U.N.T.S. 3 (1979) [hereinafter Protocol I]. "Although the U.S. military takes the position that an attacker should accept some responsibility to minimize collateral civilian casualties," the United States has not ratified Protocol I because it shifts the burden to segregate civilians from military objectives to the attacker from its traditional situation where the defender carried this obligation. Danielle L. Infeld, *Note, Precision-guided Munitions Demonstrated Their Pinpoint Accuracy in Desert Storm; but Is a Country Obligated to Use Precision Technology to Minimize Collateral Civilian Injury and Damage?*, 26 GEORGE WASHINGTON JOURNAL OF INTERNATIONAL LAW AND ECONOMICS 109, 123 (1992).

51. Protocol (I), *supra* note 50, art. 51.

52. Charles Bickers, *Combat on the Web*, Far Eastern Economic Review, 16 August 2001, www.feer.com/2001/0108_16/p030innov.html.

53. MICHAEL BOTHE *ET AL.*, NEW RULES FOR VICTIMS OF ARMED CONFLICTS: COMMENTARY ON THE TWO 1977 PROTOCOLS ADDITIONAL TO THE GENEVA CONVENTIONS OF 1949, 311 (1982).

54. Michael N. Schmitt, *Bellum Americanum: The U.S. View of Twenty-first Century War and its Possible Implications for the Law of Armed Conflict*, 19 MICHIGAN JOURNAL OF INTERNATIONAL LAW 1051 (1998).

55. Protocol I, *supra* note 50, art. 37. *See also* US Navy, The Commander's Handbook on the Law of Naval Operations, Naval Warfare Publication (NWP 1-14M/MCWP 5-2.1/COMDTPUB 5800.7) chap. 12 (1995) [hereinafter Commander's Handbook].

56. Protocol I, *supra* note 50, art. 37; Hague IV, *supra* note 49, art. 24.

57. *See* Commander's Handbook, *supra* note 53. See also ANNOTATED SUPPLEMENT TO THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS 507–13 (A.R. Thomas and James C. Duncan eds. 1999) (Vol. 73, US Naval War College International Law Studies) [hereinafter ANNOTATED SUPPLEMENT] for a discussion of customary international law allowing naval forces to fly false colors to deceive an enemy into believing a vessel is a neutral or friendly prior to combat.

58. Mark R. Shulman, *NOTE: Discrimination In the Laws of Information Warfare*, 37 COLUMBIA JOURNAL OF TRANSNATIONAL LAW 939, 959 (1999). But see THOMAS C. WINGFIELD, THE LAW OF INFORMATION CONFLICT: NATIONAL SECURITY LAW IN CYBERSPACE 169 (2000) contending that a false message from Microsoft would be lawful in that Microsoft Corporation enjoys no protected status under international law.

59. Major General Bruce A. Wright, USA, Deputy Director for Information Operations, Joint Chiefs of Staff, speaking before the Defense Colloquium on Information Operations (Mar. 24, 1999), quoted in William Church, Information Operations Violates Protocol I, www.infowar.com.

60. *Id.* at 2. 159 States have ratified Protocol I, including a majority of the NATO countries, Yugoslavia, Russia, and China, but not the United States.

61. Protocol I, *supra* note 50, art. 51. Indiscriminate attacks are defined as those which are not directed at a specific military objective.

62. Wright, *supra* note 59, at 1, footnote 1.

63. *See generally*, ANNOTATED SUPPLEMENT *supra* note 57, at chapter 8, for a discussion of the law of targeting.

64. DoD Dir 5000.1, Defense Acquisition (2000). *See also* ANNOTATED SUPPLEMENT, *supra* note 55, at 437. The weapons review is a two-step process, the first review is prior to acquisition, the second review occurs prior to use.

65. SROE, *supra* note 26, at A-2.

66. Russian officials have announced that a CNA would be considered a WMD. *See* Byard Q. Clemmons and Gary D. Brown, *Cyberwarfare: Ways, Warriors and Weapons of Mass Destruction,* 79 MILITARY REVIEW, Sept.–Oct. 1999, at 35–45, *citing* V.I. Tsymbal, "Kontseptsiya 'Informatsionnoy voyny'" (Concept of Information Warfare), Speech given at the *Russian-US Conference on Evolving Post-Cold War National Security Issues* Moscow (Sept. 12–14, 1995).

67. SROE, *supra* note 26, at A-4. See also DINSTEIN, *supra* note 29, at 202, discussing the conditions precedent to the exercise of self-defense and noting the addition of immediacy as a third condition.

68. SROE, *supra* note 26, at A-6.

XX

Responding to Attacks on Critical Computer Infrastructure

What Targets? What Rules of Engagement?

James P. Terry

Introduction

In 1997, in an exercise emphasizing infrastructure security, the National Security Agency exposed the United States' vulnerability to the disruption of computer operations at our major military commands at the hands of a hostile State or an organization with hostile intent.[1] A year earlier, US authorities had detected the introduction of a program, called a "sniffer," into computers at NASA's Goddard Space Flight Center, that permitted the perpetrator to download a large volume of complex telemetry information transmitted from satellites. The Deputy Attorney General reported that the "sniffer" had remained in place for a significant period of time.[2] Of equal concern, an FBI report in 1999 detailed Chinese efforts to attack US Government information systems, including the White House network.[3] These actual and projected interstate intrusions into Government computer networks once thought secure raise important questions concerning what, if any, rights in self-defense are triggered by such attacks. More importantly, they pose the issue of how the right of self-defense, if

an attack impacts a vital national security interest, would be translated into effective rules of engagement, specifically, legally defensible targeting decisions.

Understanding the Threat

The world of information operations represents an environment created by the confluence of cooperative networks of computers, information systems, and telecommunication infrastructures. The concern addressed here relates to the threat posed to these systems when operations are unlawfully disrupted, denied, or degraded, or when secure information that is stored in computers or computer networks is destroyed, compromised, or altered in such a way that it has a destructive effect on the national security interests of a nation. Computer espionage and computer network attacks, as well as the subversion of political, economic, and/or non-military information bearing on a nation's capabilities and vulnerabilities, may well constitute an unlawful use of force warranting a military response under traditional international law principles.

The threshold issues which emerge are: (1) which peacetime interstate activities within the telecommunications highway constitute a threat or use of force; (2) when does such a threat constitute an attack under the international law such that a right to use force in self-defense exists; and (3) what is an appropriate response. To respond to these issues, we must understand the military applications of information technology. This requires an understanding of the Internet. The Internet was originally a network of computers linked by telecommunications infrastructure and managed by the Department of Defense (DoD) in the 1970s. The internal computer networks of universities and private research facilities were merged through the development of hypertext, created in 1989 as the primary platform of the Internet. It (hypertext) translates diverse computer protocols into standard format.

This hypertext process, while extremely beneficial to both the military and civilian sectors, has created vulnerabilities. The World Wide Web, the full implementation of the Internet, which is at once the heart of the Defense Reform Initiative and key to the reengineering and streamlining of our business practices, can provide adversaries with a potent instrument to obtain, correlate, evaluate, and *adversely affect* an unprecedented volume of aggregated information critical to proper management of DoD and US infrastructure capabilities.

This chapter responds to these attacks on US infrastructure. Even though international law could not have anticipated specific information warfare concerns when the Hague Conventions of 1899, addressing means and methods of

warfare, were negotiated, the drafters thereof did anticipate technological change. The "Martens Clause," included within both Hague Convention II 1899, and Hague Convention IV 1907, provides that even in cases not explicitly covered by specific agreements, civilians and combatants remain under the protection and authority of principles of international law derived from established custom, principles of humanity, and the dictates of public conscience, and therefore are not left to the arbitrary judgment of military commanders.[4] This provision was considered necessary to prevent future unnecessary and/or disproportionate destruction from weapons systems not yet developed. The drafters had just witnessed unimaginable carnage in the Crimean War and the American Civil War resulting from advanced rifling techniques and other innovations, and were cognizant that warfare was rapidly changing. As Greenberg, *et al.*, so accurately state, as a result of the Martens Clause, "attacks will be judged largely by their effects, rather than by their methods."[5]

The Legal Parameters for Response

UN Charter System

The existing legal regime available to deter destructive actions through computer technology includes the United Nations Charter system and customary international law. The basic provision restricting the threat or use of force in international relations is Article 2, paragraph 4, of the Charter. That provision states: "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any manner inconsistent with the Purposes of the United Nations."[6]

The underlying purpose of Article 2(4), to regulate aggressive behavior between States, is identical to that of its precursor, the Covenant of the League of Nations. Article 12 of the Covenant stated that League members were obliged not to "resort to war."[7] This terminology, however, left unmentioned actions which, although clearly hostile, could not be considered to constitute acts of war. The drafters of the UN Charter wished to ensure that the legal niceties of a conflict's status did not preclude cognizance by the international body. Thus, in drafting Article 2(4), the term "war" was replaced by the phrase "threat or use of force." The wording was interpreted as prohibiting a broad range of hostile activities including not only "war" and other equally destructive conflicts, but also applications of force of a lesser intensity or magnitude.[8]

UN General Assembly Resolution 2625

The United Nations General Assembly has clarified the scope of Article 2 in two important resolutions, both adopted unanimously.[9] Resolution 2625, the Declaration on Friendly Relations, describes behavior which constitutes the "unlawful threat or use of force" and enumerates standards of conduct by which States must abide.[10] Contravention of any of these standards of conduct is declared to be in violation of Article 2(4).[11]

UN General Assembly Resolution 3314

Resolution 3314, The Definition of Aggression, provides a detailed statement on the meaning of "aggression" and defines it as "the use of armed force by a State against the sovereignty, territorial integrity or political integrity or political independence of another State, or in any manner inconsistent with the Charter of the United Nations."[12] This resolution contains a list of acts which qualify as acts of aggression. Included in the list is "the use of any weapon by a State against the territory of another State."[13] The resolution provides that the State which commits an act of aggression violates international law as embodied in the Charter.[14]

The actions of States or their surrogates in supporting or taking part in acts of aggression through information technology that threaten vital national interests of a State or States, whether through disruption of military information downlinks in satellites, sabotage of vital computer networks, or infiltration of electronic commercial transmission systems, clearly fall within the scope of Article 2(4).[15]

The Relationship Between Customary International Law and the Charter

When the UN Charter was drafted in 1945, the right of self-defense was the only included exception to the prohibition of the use of force. Customary international law had previously accepted reprisal, retaliation, and retribution as legitimate responses as well. Reprisal allows a State to commit an act that is otherwise illegal to counter the illegal act of another State. Retaliation is the infliction on the delinquent State of the same injury that it has caused the victim. Retribution is a criminal law concept, implying vengeance, that is sometimes used loosely in the international law context as a synonym for retaliation. While debate continues as to the present status of these responses, the US position has always been that actions protective of US interests, rather than being punitive in

nature, offer the greatest hope of securing a lasting, peaceful resolution of international conflict.[16]

The right of self-defense was codified in Article 51 of the Charter. That article provides: "Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations. . . . "[17] The use of the word "inherent" in the text of Article 51 suggests that self-defense is broader than the immediate Charter parameters. During the drafting of the Kellogg-Briand Treaty, for example, the United States expressed its views as follows:

> There is nothing in the American draft of an anti-war treaty which restricts or impairs in any way the right of self-defense. That right is inherent in every sovereign state and is implicit in every treaty. Every nation is free at all times and regardless of treaty provisions to defend its territory from attack or invasion and it alone is competent to decide whether circumstances require recourse to war in self-defense.[18]

Because self-defense is an inherent right, its contours have been shaped by custom and are subject to customary interpretation. Although the drafters of Article 51 may not have anticipated its use in protecting States from destructive actions perpetrated through technological means, international law has long recognized the need for flexible application. Former Secretary of State George Shultz emphasized this point when he stated that: "The UN Charter is not a suicide pact. The law is a weapon on our side and it is up to us to use it to its maximum extent."[19] The final clause of Article 2(4) supports this interpretation and forbids the threat or use of force "in any manner inconsistent with the Purposes of the United Nations."[20]

The late Professor Myres McDougal, of Yale Law School, has placed the relationship between Articles 2(4) and 51 in clearer perspective:

> Article 2(4) refers to both *the threat* and use of force and commits the Members to refrain from the "threat or use of force against the territorial integrity or political independence of any state, or in any manner inconsistent with the Purposes of the United Nations;" the customary right of self-defense, as limited by the requirements of necessity and proportionality, can scarcely be regarded as inconsistent with the purpose of the United Nations, and a decent respect for balance and effectiveness would suggest that a conception of impermissible coercion, which includes threats of force, should be countered with an equally comprehensive and adequate conception of permissible or defensive coercion . . . .[21]

Significant from Professor McDougal's interpretation is our correlative recognition of the right to counter the imminent threat of techno-violence as well as actual destructive acts of information warfare. This comprehensive conception of permissible or defensive actions, honoring appropriate response to threats of an imminent nature, is merely reflective of the customary international law. It is precisely this anticipatory element that is critical to an effective policy to counter destructive acts against critical information systems. This does not suggest the lack of international law restraints upon the determination of necessity for preemptive action. Rather, it suggests that legitimate considerations for effective response to evidence of imminent destructive acts against critical communications infrastructure must be appraised in the total context in which they occur. One aspect of this contextual appraisal of necessity, especially as it relates to responding after the fact to destructive acts against our critical information systems, concerns the issue of whether force can be considered necessary if peaceful measures are available to lessen the threat. To require a State to tolerate attacks on infrastructure critical to its security and/or economic well-being without resistance, on the grounds that peaceful means have not been exhausted, is absurd. Once an attack on critical infrastructure has occurred, the failure to consider a military response would play into the hands of those governments or groups who deny the relevance of law in their actions. The legal criteria for the proportionate use of force is established once a State or identifiable group-supported attack on technical infrastructure critical to the security of the nation has taken place. No State is obliged to ignore an attack as irrelevant, and the imminent threat to the national security requires consideration of a response.

A related, but more difficult, issue concerns the elapsed time between the attack on critical infrastructure and the identification of the State or group responsible. Admittedly, there must be some temporal relationship between a destructive act and the lawful defensive response. Nevertheless, it would be unreasonable to preclude the victim of techno-violence from redress, based upon a doctrinaire determination that the threat of further destructive intrusions into a critical system is no longer imminent, when the perpetrator's own actions have precluded immediate identification.

The requirement of proportionality is linked to necessity. Professor McDougal and Dr. Feliciano define the rule as follows:

> Proportionality in coercion constitutes a requirement that responding coercion be limited in intensity and magnitude to what is reasonably necessary promptly to secure the permissible objectives of self-defense. For present purposes, these objectives may be most comprehensively generalized as the conserving of

important values by compelling the opposing participant to terminate the condition which necessitates responsive coercion.[22]

This definition simply requires a rational relationship between the nature of the attack and the nature of the response. Although the relationship need not approach precision, a nation subjected to an isolated intrusion and disruption of an important computer system may not be entitled to launch a strike on the offender nation. Other canons of military practice, such as conservation of resources, support the principle of restraint in defense. The United Nations has condemned as reprisals those defensive actions that greatly exceeded the provocation.[23] Where there is evidence that a continuation of destructive electronic sabotage will occur, beyond the triggering event, that could threaten the very fiber of a nation's ability to defend itself, however, a response beyond that related to the initial intrusion would be legally appropriate to counter the continuing threat.

Because the real-time relationship between threat and threat recognition is often compressed in the techno-violence arena, strategy development is severely limited with respect to the non-military initiatives that may be considered in response to cyber-attack, although they are always the options of choice where available. Traditional means of conflict resolution, authorized by law and customary practice, are often precluded because attacks on computer systems are, by nature, covert in execution, unacknowledged by the State or group sponsor, and practiced with silent effectiveness.

It must be noted, however, that non-coercive efforts to avoid attacks on computer systems and telecommunication networks are also important. Diplomatic action, alone or in concert with allies or international organizations with conceivable successful impact upon a State or group considering such a cyber initiative, should be considered and employed whenever possible. In 1998, for example, the UN General Assembly passed Resolution 53/70,[24] an initiative of the Russian Federation, that called upon Member States "to promote at multilateral levels the consideration of existing and potential threats in the field of information security."[25] The United States supported this resolution with the following pertinent comments:

> The General Assembly's adoption of the resolution in plenary will launch the international community on a complex enterprise encompassing many interrelated factors which delegates . . . do not ordinarily address. For example, the topic includes technical aspects that relate to global communications—as well as non-technical issues associated with economic cooperation and trade, intellectual property rights, law enforcement, anti-terrorist cooperation, and

other issues that are considered in the Second and Sixth Committees. Further, the actions and programs of governments are by no means the only appropriate focus, for the initiative also involves important concerns of individuals, associations, enterprises, and other organizations that are active in the private sector.[26]

Despite such international initiatives focusing upon multilateral cooperation, the opportunity to look to outside assistance in protecting secure transmissions and critical systems in circumstances where our national security is threatened, is likely illusory. That responsibility will most certainly remain exclusively within the National Command Authorities.

Operational-Legal Considerations in Addressing Techno-Violence

Operational Law Context Provided in Rules of Engagement

The rules of necessity and proportionality in the information warfare scenario are given operational significance through rules of engagement (ROE). ROE are directives that a government may establish to define the circumstances and limitations under which its forces will initiate and continue responsive actions to eliminate the threat posed by an attack through technical or other means on critical communications/information infrastructure. In the US context, this ensures that the National Command Authorities' guidance for handling crisis responses to techno-violence and other threats is provided, through the Joint Chiefs of Staff (JCS), to subordinate headquarters and deployed US forces both during armed conflict and in periods of crisis short of war.

ROE reflect domestic law requirements and US commitments to international law. They are impacted by political, as well as operational considerations. For the commander concerned with responding to a threat to his communications/command and control infrastructure, ROE represent limitations or upper bounds on how to utilize defensive and/or responsive systems and forces, without diminishing the authority to effectively protect his own critical infrastructure from attack.

Evolution of JCS Rules of Engagement

Techno-violence against a critical US computer system, whether information, communications, or command and control-related, represents hostile activity which may trigger the applicable ROE. Until June 1986, the only US peacetime ROE applicable worldwide were the JCS Peacetime ROE for US

Seaborne Forces. These ROE, which until 1986 served as the basis for all commands' peacetime ROE, were designed exclusively for the maritime environment. In June 1986, Secretary of Defense Weinberger promulgated more comprehensive ROE for sea, air, and land operations worldwide.[27] The 1986 Peacetime ROE provided the on-scene commander with the flexibility to respond to hostile intent, as well as hostile acts, and unconventional threats with minimum necessary force, and to limit the scope and intensity of the threat. The strategy underlying the 1986 ROE sought to terminate violence quickly and decisively on terms favorable to the United States. In October 1994, Secretary of Defense Aspin approved the Standing Rules of Engagement for US Forces (SROE), which significantly broadened the scope of US national ROE.[28] As established in the SROE, US policy, should deterrence fail, provides flexibility to respond to crises with options that are both proportional to the provocation and designed to limit the scope and intensity of the conflict, discourage escalation, and achieve political and military objectives. The inherent right of self-defense establishes the policy framework for the SROE. These SROE are intended to provide general guidelines on self-defense and are applicable worldwide to all echelons of command. Providing guidance governing the use of force consistent with mission accomplishment, they are to be used, absent superseding guidance, in operations other than war, during transition from peacetime to armed conflict or war, and during armed conflict.

The expanded national guidance represented in the 1994 SROE, as further refined in the 2000 SROE, has greatly assisted in providing both clarity and flexibility of action for our theater commanders. The approval by the Secretary of Defense has ensured consistency in the way all military commanders, wherever assigned, address unconventional threats such as those posed to our advanced command and control infrastructure systems when these systems or computer networks are destroyed, compromised, or altered so as to have a destructive effect on the national security interests of the nation.

Targeting Considerations

The SROE, as they relate to information warfare, are implemented through the law of targeting, a subset of the law of armed conflict. The law of targeting is based upon three fundamental principles. These are:

- The right of States to adopt means of injuring the enemy is not unlimited.
- The launching of attacks against the civilian population as such is prohibited.

- Distinctions must be made between combatants and noncombatants, to the effect that noncombatants are spared to the extent possible.[29]

Because the law of armed conflict is an eminently practical law which takes into account military efficiency, these basic principles are also consistent with the response authorized for non-violent but equally destructive forms of coercive activity, such as sabotage of critical defense computer systems. Moreover, targeting theory is premised upon practical considerations that serve the purpose of defining the objects of legitimate and proportional response to each variant of aggression, whether it be an armed attack on US facilities or an equally debilitating computer-assisted attack, and of providing functional targeting criterion to the responsible official, whether civilian or military.

Executive Order 13010

The key, then, to an effective response to the threat posed by States or groups engaging in attacks against US critical infrastructure must be the commitment to address the attacks they sponsor within the scope of the law of armed conflict. We must think of cyber aggression as a variant of terrorist activity. This is precisely the approach taken by the Clinton Administration. When President Clinton signed Executive Order (EO) 13010 on July 15, 1996, thereby establishing the President's Commission on Critical Infrastructure Protection (CCIP), he declared that certain designated "national infrastructures are so vital that their incapacity or destruction . . . would have a debilitating impact on the defense or economic security of the United States." The eight categories of critical infrastructure designated in the EO as requiring the development of a national strategy for protection include: continuity of government; telecommunications; transportation; electric power systems; banking and finance; water supply systems; gas and oil storage and transportation; and emergency services (medical, police, fire and rescue). Chaired by Robert T. Marsh, a retired Air Force General, the CCIP was tasked with developing a comprehensive national strategy for protecting critical infrastructures from electronic and physical threats. On October 13, 1997, the CCIP issued the unclassified version of its report, entitled "Critical Foundations: Protecting America's Infrastructure." In addition to determining the challenge of adapting to a changing culture, the report found the existing legal framework inadequate to deal with threats to critical infrastructure. The centerpiece of the CCIP's national strategy, then, is the domestic and international legal regime required to protect against threats to critical infrastructure. Although the report itself provides few specifics, on May 22, 1998, the Administration issued Presidential Decision Directives (PDD) 62 and 63 in implementation of its policy framework.

Presidential Decision Directive 62

PDD 62, Combatting Terrorism, is the successor to National Security Decision Directive (NSDD) 138, signed by President Reagan on April 3, 1984, which determined that the threat of terrorism constitutes a form of aggression and justifies acts in self-defense.[30] PDD 62 is more expansive in its coverage than NSDD 138 and addresses a broad range of unconventional threats, to include attacks on critical infrastructure, terrorist acts, and the threat of the use of weapons of mass destruction. The aim of the PDD is to establish a more pragmatic and systems-based approach to protection of critical infrastructure and counter-terrorism, with preparedness the key to effective consequence management. PDD 62 creates the new position of National Coordinator for Security, Infrastructure Protection and Counter-Terrorism, which will coordinate program management through the Office of the National Security Advisor.[31]

Presidential Decision Directive 63

PDD 63, Critical Infrastructure Protection, mandates that the National Coordinator, established in PDD 62, initiate immediate action between the public and private sectors to assure the continuity and viability of critical infrastructures. The goal established within PDD 63 is to establish a reliable interconnected and secure information system infrastructure by the year 2003. A National Plan Coordination Staff is tasked with integrating the plans developed by the various departments of government serving as lead agencies within their respective areas of responsibility into a comprehensive National Infrastructure Assurance Plan, overseen by the National Infrastructure Assurance Council. The Council includes representation from both the public and private sectors. Under the PDD, the Federal Bureau of Investigation's National Infrastructure Protection Center, established in February 1998, will continue to provide a control and crisis management point for gathering information on threats to critical infrastructure and for coordinating the federal government's response.[32]

Targeting in the Context of PDD 62 and PDD 63

The issue remains, however, should the Critical Infrastructure Plan fail, what legal remedy can be applied under the law of armed conflict. If a response is justified, what targets in a perpetrator country are proportional to the threat posed by destruction or compromise of critical infrastructure. Again, our experience in addressing terrorism must be reviewed. The reason this is necessary is that the flexibility of the law of armed conflict in addressing unconventional threats provides far more salient options than domestic law or intelligence law in cases

where the very fiber of our national security is placed at risk. For example, as W. Gary Sharp correctly points out, an unlawful entry into and/or compromise of a critical national security system by an individual or individuals can be viewed as criminal activity under the jurisdiction of the federal and state law enforcement officials. The same intrusion by the same individual or individuals representing a State or international entity could be viewed as lawful espionage or intelligence gathering practiced by all States. If, however, that intrusion and the debilitating effect it has on national security can appropriately be characterized as an attack on vital US national interests, the range of options is greatly enhanced.[33]

This is important because the State or group attempting to compromise US national security through the calculated sabotage of critical infrastructure *is attacking the nation*, not with bombs or bullets, but with the intent of destroying equally critical elements of national well-being and sovereignty. The loss of a power grid or of a US telecommunications network through computer generated viruses for an extended period of time would have the capacity of placing more Americans at risk than a significant military threat.

The United States was jolted into an awareness of the changing character of aggression when its embassy in Tehran was seized on November 4, 1979, by Iranian militants who enjoyed the support of Ayatollah Khomeini's revolutionary government.[34] In August 1998, US Embassies in Nairobi and Dar-es-Salaam were the subjects of unconventional warfare attacks, resulting in the significant loss of life in Nairobi. In the attacks, a US response was only possible because of the linkage established between Osama bin Laden's organization and the assaults on American interests. The thrust of the new US strategy, outlined in PDD 62, must be to reclaim the initiative lost while the United States pursued a reactive policy toward unconventional threats, especially those to its critical infrastructure.

An examination of authorized responses (and the selection of appropriate targets) to techno-violence requires an understanding that cyberterrorism is a strategy that does not follow any of the traditional military patterns. In fact, a fundamental characteristic of attacks on critical infrastructure is its violation of the established norm of information security. The only norm for cyberterrorism is effectiveness. While traditional international law requires discrimination among those affected by an attack and proportion in its intensity, the nature of information warfare and cyberterrorism is such that success is measured by the extent and duration of destructiveness to the systems targeted, with no concern for those affected. In the contemporary language of defense economics, they wage countervalue rather than counterforce warfare.

Why is this important? It is important because the only credible response to attacks on critical infrastructure is deterrence. There must be an assured,

effective reaction that imposes unacceptable costs on the perpetrators and those who make possible their activities. For domestic intruders, the criminal law may suffice. For those operating outside the United States, the US reaction must counter the cyber-terrorist's strategy within the parameters of international law and PDD 62. Those who suggest otherwise neither understand the inherent flexibility of international law nor the cost of violating that law.

In this regard, a case for a response in self-defense is not persuasive either on the political or legal level unless a reasonable basis of necessity is perceived. Those to whom a justification is addressed (that is, other governments or the public) will consider whether it is well founded; they will not regard the use of force as a purely discretionary act. An important dimension of this question concerns the separate issue of when does action become necessary; that is, when is the use of force necessary to enforce adherence to the norm of information security. As Professor Lauterpacht has pointed out, every State judges "for itself, in the first instance, whether a case of necessity in self-defense has arisen," but that "it is obvious that the question of the legality of action taken in self-preservation is suitable for determination and must ultimately be determined by a judicial authority or political body . . . ."[35] The United States has long taken the position that each nation is free to defend itself and is the "judge of what constitutes the right of self-defense and the necessity . . . of same."[36] Similarly, more than a half-century ago, Secretary of State Frank Kellogg noted that when a State has resorted to the use of force, "if it has a good case, the world will applaud and not condemn its actions."[37]

A Pro-Active Response to Threats to Critical Infrastructure is Authorized under International Law

The decision to respond with force against techno-violence must be as closely tied to a clear objective as in the case where planning is conducted at the higher end of the coercion spectrum. Because the relationship between objective and threat is often unclear in the low intensity conflict arena, a strategy to fight cyberterrorism must always focus on the underlying political purpose of the State or group attempting to degrade or destroy an element of critical US infrastructure, whether that element be commercial, communications, intelligence, or defense-related. That purpose is unquestionably the degradation of our critical systems such that we are unable to defend ourselves militarily or protect ourselves from serious political or financial overreaching on the part of our adversaries. How do we counter this purpose, this objective? Former Secretary of State Shultz was correct when he stated that US policy

"must be unambiguous. It must be clearly and unequivocally the policy of the United States to fight back—to resist challenges, to defend our interests . . ."[38] Implementation of this pro-active policy requires that we make the fullest use of all the weapons in our arsenal. These should include not only those defensive and protective measures which reduce US systems-vulnerability, but also new legal tools and agreements on international sanctions, as well as the collaboration of other concerned governments. While we should use our military power only as a last resort and where lesser means are not available, there will be instances where the use of force is the only alternative available to eliminate the threat to critical civil or military infrastructure.

Closely related to the legal question is the political question of linkage. When clear linkage to a supporting State exists, we must publicize that relationship and respond with discrimination in a manner calculated both to eliminate the current threat while deterring the offending State from further destabilizing actions. The "center of gravity" in the offending State must always be that target or capability which most significantly undermines that State's will to continue to destabilize our critical infrastructure. Since cyberterrorism is a lesser form of international conflict and is bound by its rules, lawful response is properly limited to those targets which do not enjoy civilian immunity. Military targets may be preferable for two other reasons. First, the selection of military targets, while our adversaries are attacking our civil infrastructure in violation of international law, should not raise concerns on the part of other States. Additionally, selection of military targets would refocus attention on the fact that cyberterrorism and techno-violence are, in fact, forms of armed conflict.

The thrust of this new strategy, outlined in PDDs 62 and 63, must be to reclaim the initiative lost while the United States pursued a reactive policy to incidents of information warfare which neither deterred cyber-terrorists nor encouraged successful response. The key to an effective, coordinated policy to address the threat posed by those willing to target our critical infrastructure is the commitment to hold those accountable responsible under the law of armed conflict. Full implementation of the two PDDs should lead to increased planning for protective and defensive measures to address this challenge to US national security, and, where deterrence fails, to respond in a manner which eliminates the threat, rather than treating each incident after the fact as a singular crisis provoked by international criminals. By treating cyber-terrorists as participants in international coercion where clear linkage can be tied to a State actor, the right of self-defense against their sponsor is triggered, and responding coercion (political, economic, or military) may be the only proportional response to the threat.

This pro-active strategy to the threat posed by attacks on our critical infrastructure embraces the use of protective, defensive, non-military, and military measures. It attempts, for the first time, to define acts designed to destabilize our eight most important infrastructure systems in terms of "aggression," with the concomitant right of self-defense available as a lawful and effective response. The use of international law and, more specifically, the law of armed conflict, will not only complement the current criminal law approaches, but give pause to those who would target vital US interests.

NOTES

1. *See* Bradley Graham, *US Studies New Threat: Cyber Attack*, WASHINGTON POST, May 24, 1998, at A-1. The author describes Operation Eligible Receiver, conducted by the NSA and other government agencies.

2. Speech of the Hon. Jamie Gorelick before the Corps of Cadets, US Air Force Academy, February 29, 1996.

3. See William Gertz, *Chinese Hackers Raid US Computers*, WASHINGTON TIMES, May 16, 1999 at C1, C8, for a troubling review of Chinese efforts to attack White House, State Department and other government computer systems.

4. Convention (II) with Respect to the Laws and Customs of War on Land, July 29, 1899, 1 AMERICAN JOURNAL OF INTERNATIONAL LAW (Supp.) 129 (1907); Convention (IV) Respecting the Laws and Customs of War on Land, Oct. 18, 1907, 2 AMERICAN JOURNAL OF INTERNATIONAL LAW (Supp.) 90 (1908), ADAM ROBERTS AND RICHARD GUELFF, DOCUMENTS ON THE LAWS OF WAR 59 (3rd ed. 2000); Protocol I Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, June 8, 1977, 16 INTERNATIONAL LEGAL MATERIALS 1391 (1977), ROBERTS AND GUELFF, *supra*, at 420. Most treaties relevant to the law of armed conflict are available on the International Committee of the Red Cross website at www.icrc.org/ihl/.

5. LAWRENCE T. GREENBERG, SEYMOUR E. GOODMAN, AND KEVIN J. SOO HOO, INFORMATION WARFARE AND INTERNATIONAL LAW 32 (1997).

6. UN CHARTER, art. 2, para. 4.

7. *See* LEAGUE OF NATIONS COVENANT, art. 12.

8. MYRES MCDOUGAL AND FLORENTINO FELICIANO, LAW AND MINIMUM WORLD PUBLIC ORDER 142–143 (1961).

9. *See* Definition of Aggression, G.A. Res. 3314, 29 UN GAOR Supp. (No. 31) at 142, UN Doc. A/9631 (1974) [hereinafter Definition of Aggression]; Declaration on Principles of International Law Concerning Friendly Relations and Cooperation Among States in Accordance with the Charter of the United Nations, G.A. Res. 2625, 25 UN GAOR Supp. (No. 28) at 121, UN Doc. A/8028 (1970) [hereinafter Declaration on Friendly Relations].

10. The Declaration on Friendly Relations includes the following provisions:

- Every State has the duty to refrain from organizing, instigating, assisting or participating in acts of civil strife or terrorist acts in another State.
- No State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State.
- No State shall organize, assist, foment, finance, incite, or tolerate subversive, terrorist, or armed activities directed towards . . . the regime of another State.

Declaration on Friendly Relations, *supra* note 9, at 122–23.

11. "By accepting the respective texts [of the Declaration on Friendly Relations], States have acknowledged that the principles represent their interpretations of the obligations of the Charter." Robert Rosenstock, *The Declaration of Principles of International Law Concerning Friendly Nations: A Survey*, 65 AMERICAN JOURNAL OF INTERNATIONAL LAW 713, 715 (1971).

12. Definition of Aggression, *supra* note 9, at 142.

13. *Id.* at 143.

14. A fundamental purpose of the UN Charter is to "maintain international peace and security." UN CHARTER art. 1, para. 1. Article 5, paragraph 2, of the Definition of Aggression provides: "A war of aggression is a crime against international peace. Aggression gives rise to international responsibility." Definition of Aggression, *supra* note 9, at 144.

15. One potential act of destructive information warfare that would certainly trigger the definition of aggression would be the use of information technology to disrupt some vital element of the US economic apparatus (banking system, Stock Exchange, etc.) such that a juggernaut was placed on US commercial activity.

16. 68 AMERICAN JOURNAL OF INTERNATIONAL LAW 720, 736 (1974) (Statement of Acting Secretary of State Dean Rusk).

17. UN CHARTER, art. 51.

18. 5 MARJORIE WHITEMAN, DIGEST OF INTERNATIONAL LAW § 25, at 971–72 (1965).

19. George Shultz, Low Intensity Warfare: The Challenge of Ambiguity, US Department of State Current Policy No. 783, at 3 (Jan. 1986).

20. UN CHARTER, art. 2, para. 4.

21. Myres McDougal, *The Soviet-Cuban Quarantine and Self-Defense*, 57 AMERICAN JOURNAL OF INTERNATIONAL LAW 597, 600 (1963).

22. MCDOUGAL AND FELICIANO, *supra* note 8, at 242.

23. See the Security Council's discussion in 36 UN SCOR.(2285–2288 mtgs.), UN Docs. S/PV 2285–88 (1981).

24. G.A. Res. 53/70, UN GAOR, 53rd Sess., UN Doc. A/RES/53/70 (1998).

25. *Id.*

26. United States Explanation of Vote After the Vote, re: G.A. Res. 53/70 (1998), *reprinted in* W. GARY SHARP, SR., CYBERSPACE AND THE USE OF FORCE 189 (1999).

27. Joint Chiefs of Staff Peacetime Rules of Engagement for U.S. Forces (June 1986).

28. Chairman of the Joint Chiefs of Staff Instruction 3121.01, Standing Rules of Engagement for US Forces, Oct. 1, 1994, as amended Dec. 22, 1994. (The current version of the SROE was promulgated on Jan. 15, 2000, as CJCS Instruction 3121.01A.)

29. US NAVY, The Commander's Handbook on the Law of Naval Operations (NWP 9), para. 8.1., (1987).

30. Classified document described by Robert C. McFarlane in "Terrorism and the Future of a Free Society," (Speech delivered at the National Strategic Information Center, Defense Strategy Forum, Washington, D.C.: 25 March 1985). See discussion in James Terry, *An Appraisal of Lawful Military Response to State-Sponsored Terrorism*, NAVAL WAR COLLEGE REVIEW, May–June 1986, at 58.

31. Presidential Decision Directive 62, Combatting Terrorism, May 22, 1998. Richard C. Clarke, longtime senior National Security Council staff-member, was appointed as the first National Security Coordinator.

32. Presidential Decision Directive 63, Critical Infrastructure Protection, May 22, 1998. *See* SHARP, *supra* note 26, at 201–204, for a comprehensive review of the major elements of PDD 63 and the requirements imposed upon the various departments of government and the private sector under this directive.

33. *Id.* at 205–206.

34. *See* James Terry, *The Iranian Hostage Crisis: International Law and US Policy*, JAG JOURNAL 31-79 (Summer 1982).

35. ROBERT OPPENHEIM, INTERNATIONAL LAW 299 (8th ed. 1955).

36. Ian Brownlie, *The Use of Force in Self-Defense*, BRITISH YEARBOOK OF INTERNATIONAL LAW 183, 207 (1961).

37. Address by Secretary of State Kellogg before the American Society of International Law, April 28,1928, PROCEEDINGS OF THE AMERICAN SOCIETY OF INTERNATIONAL LAW 141, 143 (1928).

38. George Shultz, Address before the Low Intensity Warfare Conference, National Defense University, Washington, D.C., Jan. 15, 1986.

XXI

Is It Time for a Treaty on Information Warfare?

Phillip A. Johnson

Introduction

Several participants in the conference on computer network attack held at the Naval War College in Newport, Rhode Island, in June 1999 addressed the issue of whether serious consideration should be given in the near future to negotiating international agreements to regulate information warfare. The consensus appeared to be that it would be useful to expand current efforts to improve international cooperation in investigating and prosecuting computer crimes and "cyber-terrorism," but that it would be premature anytime in the near future to attempt any further prohibition or regulation of State action in the broad area of information warfare. I generally share those views. This chapter will discuss a number of possibilities for international agreements on information warfare, indicate the extent of declared support for negotiations intended to produce such agreements, and venture an opinion on their potential utility.

Some observers have said that the few calls already heard for a treaty banning information warfare come primarily from "have-not" nations that fervently desire to keep the "haves" from reaping any advantage from the information warfare capabilities they have developed by their effort and investment. Others say that new agreements are necessary to enhance the international cooperation that

is essential to effective suppression of malicious interference with information systems that are essential to development, prosperity, international peace and security, and human health and safety. Still others say that new information technologies raise novel international legal issues that would be better resolved by negotiating a definitive international agreement than through the slow and uncertain process by which customary international law develops. Others reply that we are not yet smart enough to sit down and create international law on these new issues, and that the gradual accumulation of practice and precedent offers the best process for applying existing international law to these new issues in cyberspace. I boldly take the position that each of these views is correct—in part and on some subjects.

For the purposes of this chapter, I intend to set aside discussion of a number of military missions that are often considered to be elements of information warfare. These are the physical destruction of information systems by traditional military means, electronic warfare (e.g., "jamming" of radio and radar signals), military deception, and operations security. These traditional military missions have been conducted for a long time over a wide spectrum of military operations from peace to war, and the application of international law to them is reasonably well settled. I also intend to set aside discussion of directed energy weapons such as high-energy radio, microwave, and electro-magnetic pulse devices. The technology of these devices is relatively new, but their employment and effects are likely to be so similar to those of traditional weapons that established principles of international law concerning the use of force and the law of armed conflict can be applied to them with great confidence.

Psychological operations have also been a traditional military mission, but new technologies such as the broadcasting of radio and television signals from aircraft and satellites, worldwide access to the Internet, and greatly improved capabilities to create false images and messages give "psyops" unprecedented reach and power. As we shall see, there already have been a few isolated calls for new international controls over these new capabilities for spreading "propaganda."

The newest element of information warfare, and the one currently drawing the most attention, is computer network attack, or CNA. CNA is conducted by sending electronic messages from one computer to another through some connecting medium or network, such as radio or the Internet, or by direct input by a user of the target computer system. The most common forms of CNA are: (1) overloading an adversary's web pages or e-mail systems with so much input that they cannot function properly; (2) tricking an authorized user into inputting malicious logic, as by sending an e-mail message with a virus or a worm in an attached file; and (3) obtaining unauthorized access to an adversary's computer

system. Unauthorized access may be obtained by exploiting a security weakness in the target's operating system, by unauthorized use of a genuine user identification and password, or by other means. Even if an intruder does no apparent harm, the mere fact that an intruder has gained unauthorized access renders the system and its contents suspect, since an intruder could have altered stored data, changed the operating system, or introduced malicious logic such as a virus, worm, or logic bomb. An intruder may even damage the system to the point where it becomes unusable. The remainder of this chapter will focus primarily on the question of whether it would be desirable to negotiate international agreements to prohibit or regulate CNA.

At this point in history, there are a number of "revealed truths" concerning CNA that make it different from prior methods and means of conducting hostilities. I list them here as common points of departure; the reader can find a fuller discussion of them in the other contributions to this volume:

- The more a nation relies on sophisticated information systems, the more vulnerable it is to interference with them;
- Geography has ceased to be relevant to the security of information systems that are connected to the Internet or that are accessible by radio;
- The worldwide use of comparable equipment, operating systems, and software greatly facilitates CNA;
- Information technologies change rapidly;
- Most advances in information technology are developed by individuals or companies for commercial purposes;
- Developing at least some capability to interfere with other nations' information systems is relatively cheap and easy, compared to other modern weapons systems, and the necessary expertise and equipment are widely available;
- CNA "offense" currently seems to be dominant over CNA "defense," but the balance between them might change quickly and dramatically;
- In most cases it is difficult to locate and identify computer intruders, to discover their motive and intent, and to determine whether their acts are attributable to State sponsors; and
- Because many "dual-use" information infrastructures whose support to military operations makes them legitimate military targets are also used for noncombatant purposes, interference with them may endanger the safety of persons and property protected by the law of war from deliberate attack and from disproportionate collateral damage.

Calls For International Agreements

Public calls by governments for new international agreements on information warfare consist primarily of: (1) initiatives by the United States and by certain European and other American nations to promote better international cooperation in investigating and prosecuting computer crimes and terrorism; and (2) a campaign by Russia in United Nations channels for multilateral arms control negotiations to protect international "information security."

International cooperation in investigating and prosecuting computer crimes has sometimes proven to be quite effective even in the absence of new agreements and working arrangements specifically tailored to this new category of offenses. For example, in 1987 West German authorities relied on the authority provided by existing German law to trace the origin of over 200 intrusions into US government computers to four German nationals who turned out to be working for the KGB.[1] In far too many cases, however, effective international cooperation in investigating computer offenses has been frustrated by the unwillingness of the requested State to cooperate, its lack of domestic legal authority to investigate and punish computer offenses, the absence of established procedures and points of contact, and problems arising from extradition treaties.

In an effort to address such problems, in December 1997 the United States Attorney General hosted a meeting of the Group of Eight (G-8) Justice and Interior Ministers to discuss international cooperation in the investigation and prosecution of computer intrusions and other high-tech crimes.[2] Since this meeting, a number of international working groups have devoted considerable effort to modernizing the G-8 nations' domestic criminal laws and to improving international agreements and arrangements providing for mutual legal assistance and extradition in cases involving computer offenses. This work has also generated a project in the Council of Europe, which the United States has assisted, to draft an international convention on "cyber-crime." The United States has also undertaken similar initiatives in the Organization of American States and at the United Nations. Significant progress has been made, but there is still an enormous amount of work to be done in this area. For example, while several European nations have made significant reforms in their domestic computer crime laws and the state of procedures for international assistance in investigating computer offenses has greatly improved between various nations, Russia has essentially stonewalled all requests for cooperation in investigating several thousand intrusions into US military computer systems in early 1999 that apparently originated in Russian territory.[3]

In addition, these efforts have focused on computer offenses committed by individuals that can be characterized as crimes or terrorism. They are not directly

relevant to State action. Somewhat ironically, the only nation that has made a prominent effort to address the use of computer network attack by States against other States has been Russia. In October 1998, Russian Federation Ambassador Vasily Sidorov made a statement before the UN General Assembly's Committee on Disarmament and International Security to the effect that Russia is alarmed by the serious threats to international peace and security raised by developments in information technology, and that it is urgent to take preventive measures by establishing international principles on the use of information technology and possibly an international monitoring and control regime.[4] Russia also tabled a resolution that called for Member States to express their views on the creation of "international legal regimes to prohibit the development, production or use of particularly dangerous forms of information weapons" and the establishment of "an international system (centre) for monitoring threats pertaining to the security of global information and telecommunications systems."[5]

No significant support was expressed by other nations for the Russian proposal. Instead, on December 4, 1998, the General Assembly adopted without a vote a greatly watered-down resolution that called on Member States to "promote at multilateral levels the consideration of existing and potential threats in the field of information security," invited all Member States to inform the Secretary General of their views on the subject, requested the Secretary-General to submit a report to the General Assembly in its 1999 session, and included in the provisional agenda for its next session the topic, "Developments in the field of information and telecommunications in the context of international security."[6]

Undeterred, Russia has continued to pursue its proposal for an "international legal regime" on "information weapons." In its submission of views to the Secretary General as invited by the General Assembly resolution, Russia declared that "information weapons" can have "devastating consequences comparable to the effect of weapons of mass destruction," called for the General Assembly to pass "resolutions on the question of information security with a view to reducing the threat of the use of information for terrorist, criminal or military purposes," and proposed the development of a code of conduct for States concerning international information security that would ultimately be incorporated into a multilateral international legal instrument.[7]

The United States also submitted its views, which generally were that the international community should give priority to developing measures to deal with criminal or terrorist misuse of information technology, and that "it would be premature to try to formulate overarching principles pertaining to information security in all its aspects."[8]

Only eight other nations—Australia, Belarus, Brunei, Cuba, Oman, Qatar, Saudi Arabia, and the United Kingdom—submitted written views to the Secretary General. Of these, only Belarus and Cuba expressed support for negotiations to restrict information warfare. The Secretary General offered no opinion.

In August 1999, the United Nations Department of Disarmament Affairs and the United Nations Institute for Disarmament Research (UNIDIR) hosted a conference in Geneva, Switzerland on the topic: "Developments in the Field of Information and Telecommunications and Their Impact on International Security." Russia used the forum to promote its proposals for international legal restrictions on information warfare, but it was unable to garner significant support for doing more than continuing to study the problem.[9]

Nevertheless, the current paucity of enthusiasm for negotiating an international agreement restricting information warfare may not last forever. In the past twenty years, the international community has negotiated multilateral treaties restricting such weapons as chemical weapons, blinding lasers, incendiaries, weapons designed to wound with undetectable fragments, and antipersonnel landmines.[10] It might take only a few spectacular incidents involving CNA to provoke serious interest in placing international legal restrictions upon "information weapons."

Subjects For Possible Agreements

Treaties to suppress private misconduct.

1. *Suppression of "cyber-crime."* As indicated above, efforts are already under way in the G-8, the Council of Europe, the Organization of American States, and the United Nations to improve domestic criminal legislation, international cooperation in investigations and prosecutions, and extradition treaties in order to more effectively investigate and punish cross-border computer crimes. The US and British submissions of views mentioned above recommended that the United Nations give this area top priority in its activities concerning information security.

ASSESSMENT: This topic is a logical candidate for priority consideration, since both the nature of the problem of cross-border computer crime and the required remedial steps are reasonably well understood, and since national security issues are not directly implicated. (It should be noted, however, that effective international cooperation in tracing computer network attacks to their origin would also greatly expedite attribution of State-sponsored CNA.) That is not to say that the negotiation of the necessary international agreements will be easy,

given the major differences that exist among domestic legal systems and the encroachment on traditional sovereignty principles that will be inescapable in creating legally binding obligations to assist with criminal investigations and prosecutions, not to mention the proposals that are under consideration for reciprocal authorization of cross-border electronic tracing and monitoring.

2. *Suppression of "cyber-terrorism."* A "cyber-terrorism" agreement might well adopt the common features of the existing multilateral treaties intended to combat such terrorist acts as the hijacking and sabotage of aircraft, hostage taking, attacks on diplomats, terrorist bombing, and the seizure of ships on the high seas.[11] These common features are a recognition of universal or quasi-universal jurisdiction over individuals committing specified acts, an obligation upon each Party to put into place severe domestic criminal penalties for such acts, and an obligation to prosecute or extradite any person suspected of such acts who is found in the territory of a Party.

ASSESSMENT: It may prove to be difficult to generate much interest in negotiating such an agreement until the international community experiences incidents in which "cyber-terrorism" causes death and destruction on the scale experienced as the result of more traditional forms of terrorism. To date, the most common form of cross-border CNA motivated by political reasons has consisted of individuals defacing the target nation's websites, which is likely to strike most people more as vandalism than as terrorism. Even the theft of large amounts of money or the crippling of expensive information systems is unlikely to provoke the same kind of fear and loathing created by more traditional terrorist acts that directly threaten innocent human lives. It would probably take an incident in which planes crash, trains collide, floods cause death and devastation, or a nuclear accident spreads radiation over the countryside before CNA would be taken seriously as "cyber-terrorism." Another major problem would be reaching agreement on definitions of the acts to be suppressed. It is certainly worth exploring the possibilities here, but rapid progress—or even moving the international community at large to devote serious effort to negotiation of a "cyber-terrorism" treaty—seems unlikely in the near future. It may turn out that the most effective legal mechanism for suppression of "cyber-terrorists" will be "cyber-crime" agreements, as discussed above, that would put into effect domestic computer crime laws and facilitate cross-border investigations and prosecutions.

Treaties to restrict state action.

1. *Declarations of general legal principles.* Perhaps the simplest approach to advancing the development of international law on information security would be

to negotiate a multilateral treaty that declares broad relevant principles of international law. An example of such a document is the 1967 Outer Space Treaty,[12] which declares, *inter alia,* that space is not subject to national appropriation or territorial claims, that nations are obligated not to interfere with the space activities of other nations, that space objects remain under the jurisdiction and control of their nation of registry, that nations bear international responsibility for their space activities, and that established principles of international law, including the UN Charter, apply to space activities. Some candidate principles for a similar declaration of principles on information activities might be that nations must not damage/disrupt/interfere with the information systems of other nations; that such acts violate the sovereignty of the victim nation and threaten international peace and security; and perhaps even that interference with information systems causing death, injury, widespread property damage, or serious damage to communications, public utilities, economic institutions, emergency services, or national security systems will be considered to be equivalent to an armed attack, thereby authorizing the victim nation to employ the remedies provided under international law to the victims of traditional armed attacks, including the use of force in individual or collective self-defense.

ASSESSMENT: It will take some time for most nations to determine what international legal principles concerning information warfare are likely to best serve their long-term national interests. Even nations that already possess sophisticated information systems have little confidence at this point that they can reliably forecast near-term technical developments that may drastically affect the balance of information warfare capabilities and vulnerabilities. Those nations that have even a minimum of capabilities to engage in information operations must make a judgment as to whether their interests would be best served by keeping open their options to interfere with other nation's information systems, especially when they are engaged in an international armed conflict, or whether their national interests would be best served by creating an international legal regime that broadly prohibits such interference.

The current domestic and international debate over "space control" may present a useful analogy. As indicated above, the Outer Space Treaty declares the general principle that nations will not interfere with the space activities of other nations. However, its provisions recognizing that nations must conduct their space activities in compliance with international law, including the UN Charter, bring to bear the international law principles that force can be used in self-defense and to execute mandates of the Security Council. Accordingly, these widely-recognized legal authorizations for the use of force apply to space activities in the same manner as they do in the air, at sea, and on land.

Furthermore, since the Outer Space Treaty is silent as to its application during an international armed conflict, we are left to rely on the general principles of international law to determine the extent to which its obligations may apply in wartime.[13] In these circumstances, there has been considerable activity in the UN General Assembly and in the Conference on Disarmament devoted to drafting a multilateral agreement to prevent an "arms race in space." To date, however, this activity has produced virtually nothing in the way of concrete results.[14]

The continuing impasse over attempts to develop international legal measures to prevent an "arms race in space" might be seen as a confrontation of the "haves" versus the "have-nots," which might also be seen as the dynamic at work in the impasse over proposals for complete nuclear disarmament. On the other hand, the impasse might also be seen as reflecting the reluctance of at least some of the thirty or so space-capable nations to participate in formulating international legal principles concerning space control when they have yet to reach their own judgments concerning where their own long-term national interests lie.

The analogy between space control and information warfare is less than exact, for several reasons. One is the fact that it is many orders of magnitude easier for a nation to develop a significant information warfare capability than it is to develop space control capabilities. This is clearly demonstrated by the computer network attacks that have already been reported in connection with such conflicts as Kosovo and Chechnya, and in the continuing tensions between Taiwan and mainland China.[15] The converse is also true—virtually every nation employs at least some automated information systems, making them vulnerable to CNA, while only about thirty nations conduct space activities. In these circumstances, it seems unlikely that very many nations will regard themselves as "non-players" in information warfare. It seems equally unlikely that many of them will come to firm conclusions anytime soon about how their own long-term national interests might be affected by restricting CNA or other information warfare activities. Accordingly, even a declaration of general legal principles concerning information warfare is likely to be beyond the grasp of the international community for the foreseeable future.

2. *Arms Control Agreements.* Another approach would be to negotiate agreements under which the parties would commit themselves not to develop, possess, or transfer certain information warfare capabilities, or to use them in a manner that is destabilizing to other arms control regimes or to crisis management systems.

ASSESSMENT: This approach is subject to the same caveat stated above, which is that not many nations—if any—have figured out where their long-term national interest lies in relation to information warfare. It also suffers from the great difficulty of defining exactly what capabilities the parties would

agree not to develop, possess, or transfer; from the apparent impossibility of verification; from the fact that governments have no monopoly over the development or use of CNA capabilities; and from the fact that CNA capabilities and vulnerabilities change rapidly. The development of "hacking" tools is a worldwide cottage industry, unlike nuclear weapons, tanks, artillery, submarines, ballistic missiles, or warplanes. Powerful hacker tools are posted on the Internet for use by all comers.[16] Furthermore, many highly capable computer network attack capabilities spring directly from techniques and programs developed for legitimate purposes.[17] For these reasons, it is difficult to envisage how an arms control-style agreement could be negotiated anytime in the near future. In addition, any proposal for a nonproliferation agreement might well raise suspicions among the developing nations that the "have" nations are engaged in a conspiracy to deny the developing nations the benefits of highly capable information systems.

Strategic arms control agreements often contain provisions to preserve or expand transparency, such as obligations not to interfere with other parties' national technical means of verification. It may not be necessary to negotiate separate agreements in order to extend the reach of such agreements to ban electronic means of interference with national technical means of verification. At most, an agreed interpretation by the parties should suffice. Another similar extension of arms control principles that might prove to be both useful and attainable would be an agreement that the parties will not employ information warfare techniques in a manner that would interfere with each others' command and control of strategic weapons or disrupt missile attack warning systems.

Another theme of arms control agreements has been to create new confidence-building procedures, as in the Open Skies Agreement.[18] However, it is difficult to imagine how a confidence-building agreement could be devised for computer network attack capabilities, since such an agreement would entail widespread access by each party to the national computer systems of other parties that would be exceptionally intrusive without holding out much promise of effectiveness.

In 1989, the United States and the Soviet Union agreed not to conduct dangerous military activities in peacetime in proximity to the military forces of the other party.[19] One of the activities in which the parties agreed not to engage is interference with command and control networks in a manner which could cause harm to personnel or damage to equipment of the other party. Since electronic interference was already the primary mechanism causing interference with command and control networks, it would appear that this agreement can be applied to CNA without change. Whether circumstances will make it appropriate to enter into similar agreements with other nations remains to be seen.

3. *Law of War Agreements.* Existing law of war treaties ban the use in international armed conflicts of weapons such as expanding bullets, barbed weapons, and projectiles filled with glass on the basis that, used as intended, they are likely to cause unnecessary suffering.[20] The methods and means of information warfare do not generally raise such considerations, since few information warfare techniques cause any direct personal injury or impairment to health. An odd and isolated exception is a report by Russian authorities that they have discovered a computer virus called "666" that displays certain light patterns on a computer screen that cause the operator to lapse into a coma. Fifty computer operators are reported to have died as a result of exposure to the "666" virus.[21] With this bizarre exception, information warfare "weapons" are not generally understood to cause unnecessary suffering in the same way as do weapons that have been banned for this reason.

The law of war also bans the use in international armed conflict of weapons that are indiscriminate, i.e., they cannot be controlled and directed only against authorized military targets. Poison gas and non-self-destructing/non-self-disabling antipersonnel landmines are examples of weapons that have been banned for this reason.[22] We have already seen self-propagating computer "viruses" and "worms" that clearly foreshadow the issue of malicious logic that runs amok through military and civilian computer systems. Again, however, malicious computer logic is unlikely to directly cause injury and death. Furthermore, any attempt at drafting an international agreement that would ban indiscriminate information warfare "weapons" is likely to founder on the difficulty of defining them. It seems unlikely that any resulting agreement would advance international law beyond the principle that "information weapons," like all weapons, must be discriminate.

Law of war agreements have also taken the tack of banning or restricting attacks on certain targets, such as medical facilities, prisoner of war camps, and cultural property.[23] These existing agreements already protect these facilities from attack by any means, including information warfare techniques. It might be argued that infrastructures that are heavily relied upon for the health and safety of the civilian populations and that are particularly vulnerable to CNA should be specifically protected from such attack by international agreement. Examples might be public utilities, transportation, communications, financial networks, emergency services, and universities. The problem is that such systems may in certain circumstances be legitimate targets of attack. This may be the case when the system is being used to provide direct support to military operations, as when a single electric power net is used both for military and civilian purposes. It may also be the case, in a long and protracted conflict,

that a belligerent's transportation, utilities, financial system, and research and development systems become valid military targets because disrupting them would significantly undermine its military strength. Accordingly, it seems unlikely that the nations would agree to bestow blanket immunity on such systems, or that an international agreement could be negotiated that would advance law of war principles on the targeting of dual-use infrastructures beyond their current state. Furthermore, it would be highly counterproductive to ban CNA against such infrastructures while leaving them open to attack by traditional military weapons, which would in most cases create a much greater danger of collateral damage.

Finally, one theme of the Russian initiative for a ban on "especially dangerous information weapons" has been a push for limitations on psychological warfare. The Russian statement submitted to the Secretary General in June 1999 referred to the threat of "(u)se of information with a view to undermining a State's political and social system; psychological manipulation of a population for the purpose of destabilizing society."[24] The Cuban submission also addressed this issue: "The misuse of information and telecommunications systems and information resources, especially when such systems and resources are used by some States to carry out their policies of interference in the affairs of other States, is an infringement of the sovereignty and independence of the affected States and creates centres of tension that may pose a serious threat to international security."[25] From past experience, it seems highly unlikely that the international community will be eager to create broad restrictions on propaganda, even as it has been empowered by new and more powerful information technologies. Russia, Cuba, and other States stung in the past by the Voice of America, Radio Marti, and other "voices of freedom" will no doubt continue to beat this drum. It seems particularly unlikely that any of the Western democracies will support such calls to impose international legal restraints on the criticism of other societies or governments. As the authors of a recent article in *Foreign Affairs* concluded, "Their societies are familiar with the free exchange of information, and their institutions of governance are not threatened by it."[26]

Forms Of Possible Agreements

A. Multilateral Conventions. Multilateral conventions, especially those to which substantially all nations become parties, carry the greatest weight of authority in establishing new international law. It seems extremely unlikely, however, that a multilateral convention restricting State action relating to information warfare will be adopted anytime soon. As stated above, few nations

have expressed any interest in negotiating such an agreement, chiefly because few nations understand information warfare capabilities and vulnerabilities well enough to determine what principles of international law would best serve their long-term national interests.

In addition, the fundamental unhappiness felt by many nations as the result of recent experiences in diplomatic conferences is likely to generate significant procedural controversies that would have to be settled before negotiating new multilateral conventions. There are essentially two procedural approaches to the negotiation of a multilateral convention, whether through UN channels or in a special diplomatic conference. The first is a consensus procedure, which is used in such fora as the Conference on Disarmament. This procedure requires achieving general acceptance of a negotiating text, usually by a process of tough bargaining and compromise.

A recent alternative approach to negotiating multilateral conventions has been the use of majority-rule procedures, which were in essence the procedures used in the negotiations in Oslo that produced the Ottawa Convention banning antipersonnel landmines and in the Rome Conference that produced the draft Statute of the International Criminal Court. The great practical advantage and also the worst defect of such procedures is that they allow the majority of participating nations to approve a treaty text to which minority nations have fundamental objections. Such a result affords the organizers of the negotiations and the members of the majority immediate gratification, but it produces a treaty that will probably not be accepted by the dissenting States. In the case of the Ottawa Convention, this process generated a treaty which is almost meaningless because it apparently will not be ratified by a number of countries whose military forces and operations are most important to world affairs, including the United States, Russia, and China. The same is true to a somewhat lesser extent for the draft Statute of the International Criminal Court. Ironically, there were opportunities in the negotiations that produced both of these conventions to arrive at compromises that would have made them more widely acceptable. In both cases, however, the "like-minded" groups were not required to agree to these compromises to produce an agreement, and in both they chose ideological purity over wider acceptance. With these recent debacles in mind, it seems unlikely that there will be much enthusiasm in the near future for convening any major new international law-making diplomatic conferences on any subject.

B. Bilateral Agreements. Bilateral agreements, or agreements among a small number of nations, are most useful when only a few governments are directly

involved in the issues to be addressed. This may be because the issues are limited to one geographic area, or because only a few nations are capable of engaging in the activities in question. Good examples of the latter group are strategic nuclear arms control agreements and agreements to limit anti-ballistic and theater missile defense systems. Agreements to promote better suppression of cybercrime and cyberterrorism could be negotiated either multilaterally or bilaterally. The results of the current efforts described above in the G-8, the Council of Europe, and the Organization of American States are likely to be a combination of both, with regional agreements arrived at on some issues, and bilateral approaches taken to others. Negotiation of a global multilateral convention on these issues is unlikely until the problems of cybercrime and cyberterrorism are more broadly experienced and more broadly understood.

C. General Assembly Resolutions. The United Nations General Assembly has displayed great enthusiasm for passing resolutions on a broad range of subjects calling on Member States to adhere to certain principles. When such resolutions enjoy broad support they may persuasively influence the policies of member governments and international institutions, but such resolutions do not generally have the force of international law. On the other hand, there are occasional General Assembly resolutions that are expressly intended to declare certain principles of customary international law. When such resolutions are supported by all or substantially all Members, they may be given great weight as evidence of customary international law. An example of such a resolution recognized as "law-declarative" by the United States is the 1970 Declaration on Principles of International Law Concerning Friendly Relations and Cooperation among States in Accordance with the Charter of the United Nations.[27] Judging from the lack of interest generated by the Russian initiatives on "information security" in the General Assembly, it seems unlikely that there will be enough support to pass any kind of resolution calling on Member States to observe any set of principles concerning information warfare. Given the novelty of the international legal issues involved, it seems even more unlikely that the General Assembly will pass a "law-declarative" resolution on information warfare in the next several decades.

D. "Codification" of Existing Customary International Law. Several participants in the Newport conference recalled the work of the round-tables of governmental and academic experts that met periodically from 1988 to 1994, hosted by the International Institute of Humanitarian Law, which ultimately produced the *San Remo Manual on International Law Applicable to Armed Conflicts at*

Sea. The San Remo Manual is widely recognized as an authoritative restatement of the consensus understanding among the world's leading governmental and academic experts in this branch of international law, and it will no doubt be accorded great weight as evidence of the interpretation of applicable treaties and the state of customary international law. However, there would appear to be little potential in the foreseeable future for successfully employing an "experts conference" to authoritatively record the customary international law governing information warfare. At present there is no such law, which can only accumulate from State practice in reaction to events as they unfold over time. Accordingly, there are no "experts" either, since there is no accumulation of State practice that learned commentators could analyze and restate.

Conclusions

The next few years are likely to produce a number of regional and bilateral agreements designed to improve international cooperation in battling cybercrime and cyberterrorism. If dramatic events occur involving cyberterrorism, or if the international community feels the necessity to do *something* in the area of computer network attacks, a multilateral convention on suppression of cyberterrorism may result. The parties to strategic arms control treaties may find it useful to state their common understanding concerning how their provisions apply to CNA directed against national technical means of verification, command and control systems, and attack warning systems.

However, there seems to be little or no prospect of negotiating international agreements that would broadly prohibit or regulate state action involving information warfare techniques because: (1) the issues involved are not yet well understood; (2) traditional arms control and law of war mechanisms are not well suited for application to CNA; and (3) the nations—including the United States—do not yet have a clear understanding of what kind of international legal regime relating to information warfare would best serve their long-term national interests. For the foreseeable future, the development of international law concerning information warfare is most likely to consist of the incremental accumulation of customary international law resulting from the actions and statements of nations in response to events as they unfold. Considering the circumstances, that is probably the best available process. During this formative period, statesmen and their advisers will have a heavy responsibility to bear in mind that their acts and statements will play a major role in the development of international law concerning information warfare.

Notes

1. CLIFF STOLL, THE COOKOO'S EGG (1989).

2. U.S. Dep't Justice Press Release, Statement by Attorney General Janet Reno on the Meeting of Justice and Interior Ministers of the Group of Eight, Dec. 10, 1997. The members of the G-8 are Canada, France, Germany, Italy, Japan, Russia, the United Kingdom, and the United States.

3. Jim Wolf, *Moscow Said to Withhold Full Help on Cyber-Blitz*, REUTERS, Nov. 5, 1999.

4. Daniel Verton, *DoD Faces Infowar Controls*, FEDERAL COMPUTER WEEK, Jan. 11, 1999.

5. Russian Federation, draft resolution, Developments in the field of information and telecommunications in the context of international security, U.N. Doc. A/C.1/53/L.17 (1999).

6. G.A. Res. 53/70, U.N. GAOR, 53rd Sess., U.N. Doc. A/53/70 (1999).

7. Report of the Secretary General on developments in the field of information and telecommunications in the context of international security, U.N. Doc. A/54/213 (1999), at 8.

8. *Id.* at 11.

9. Discussion Summary, Developments in the Field of Information and Telecommunications in the Context of International Security (Private Discussion Meeting Hosted by the Department of Disarmament Affairs and the UN Institute for Disarmament Research, Geneva, Aug. 25–26, 1999).

10. Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may be Deemed to be Excessively Injurious or to have Indiscriminate Effects, Oct. 10, 1980, S. TREATY DOC. NO. 103-25 (1993) [hereinafter Conventional Weapons Convention]; Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction, Jan. 13, 1993, S. TREATY DOC. NO. 103-21 (1993) [hereinafter Chemical Weapons Convention]; Convention on the Prohibition of the Use, Stockpiling, Production, and Transfer of Anti-Personnel Mines and on their Destruction, Sept. 18, 1997, 36 I.L.M. 1507 (1997) [This agreement has not been signed by the United States].

11. Convention on Offenses and Certain Other Acts Committed on Board Aircraft, Sept. 14, 1963, 20 U.S.T. 2941, 704 U.N.T.S. 219; Convention for the Suppression of Unlawful Seizure of Aircraft, Dec. 16, 1970, 22 U.S.T. 1641, 860 U.N.T.S. 105; Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, Sept. 23, 1971, 24 U.S.T. 564; Convention to Prevent and Punish the Acts of Terrorism Taking the Form of Crimes against Persons and Related Extortion that are of International Significance, Oct. 16, 1973, 27 U.S.T. 3949; Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons, Including Diplomatic Agents, Dec. 14, 1973, 28 U.S.T. 1974, 1035 U.N.T.S. 167; Convention on the Physical Protection of Nuclear Materials, Oct. 26, 1979, T.I.A.S. 11080; International Convention Against the Taking of Hostages, Dec. 17, 1979, T.I.A.S. 11081; Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, Feb. 24, 1988, S. TREATY DOC. NO. 100-19 (1988); Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, Mar. 10, 1988, 27 I.L.M. 668 (1988); Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf, Mar. 10, 1988, 27 I.L.M. 685 (1988); International Convention for the Suppression of Terrorist Bombing, Nov. 25, 1997, 37 I.L.M. 249 (1998).

12. Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and other Celestial Bodies, Jan. 27, 1967, 18 U.S.T. 2410, 610 U.N.T.S. 205.

13. *See* Office Of General Counsel, Department of Defense, An Assessment Of International Legal Issues In Information Operations, sect. I.B (Nov. 1999) [hereinafter DoD/GC Paper]. This paper is appended to this volume as the appendix.

14. *Id.*

15. *See,* e.g., *Nerd World War,* ECONOMIST, Oct. 30, 1999 (LEXIS); Robyn Dixon, *Chechyns Use Net in Publicity War with Russia,* LOS ANGELES TIMES, Oct. 8, 1999, at A-4; David A. Fulghum, *Telecom Links Provide Cyber-Attack Route,* AVIATION WEEK & SPACE TECHNOLOGY, Nov. 8, 1999, at 81; Bob Brewin, *Kosovo Ushered in Cyberwar,* FEDERAL COMPUTER WEEK, Sept. 27, 1999.

16. Michael E. Ruane, *New Computer Technology Makes Hacking a Snap,* WASHINGTON POST, Mar. 10, 1999, at 1.

17. Donn Parker, *Automated Security,* INFORMATION SECURITY, Oct. 1999, at 32.

18. Treaty on Open Skies, Mar. 24, 1992, S. TREATY DOC NO. 102-37 (1992). The United States has ratified this agreement but it has not come into force.

19. Agreement on the Prevention of Dangerous Military Activities, June 12, 1989, 28 I.L.M. 877 (1989).

20. Hague Convention IV, Respecting the Laws and Customs of War on Land, Oct. 18, 1907, 36 Stat. 2277; Conventional Weapons Convention, *supra* note 10.

21. Timothy L. Thomas, *Dialectical Versus Empirical Thinking: Ten Key Elements of the Russian Understanding of Information Operations,* JOURNAL OF SLAVIC MILITARY STUDIES, Mar. 1998, at 51.

22. Geneva Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous, or Other Gases, and of Bacteriological Methods of Warfare, June 17, 1925, 26 U.S.T. 571, 94 U.N.T.S. 65; Chemical Weapons Convention, *supra* note 10, Conventional Weapons Convention, *supra* note 10.

23. Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31; Convention for the Protection of Cultural Property in the Event of Armed Conflict, May 14, 1954, 249 U.N.T.S. 240. The United States has signed but has not ratified this agreement.

24. Secretary General's Report, *supra* note 7, at 9.

25. *Id.* at 5.

26. Robert O. Keohane and Joseph S. Nye, Jr., *Power and Interdependence in the Information Age,* FOREIGN AFFAIRS, Sept.–Oct. 1998, at 93.

27. G.A. Res. 2625, U.N. GAOR, 25th Sess., U.N. Doc. A/8082 (1970). *See* DoD/GC Paper, sect. III. A, *supra* note 13.

Appendix

AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS

SECOND EDITION
NOVEMBER 1999

Department of Defense
Office of General Counsel

PREFACE

This assessment of international legal issues in information operations reflects the combined efforts of a superb team of Department of Defense lawyers. It could not have been produced without the contributions of representatives of the General Counsels of the Army, Navy, Air Force, the National Security Agency and the Defense Information Systems Agency, as well as the Judge Advocates General of the military services and the Legal Counsel to the Chairman of the Joint Chiefs of Staff. Their insight, wisdom and persistence have not only been of great value but have reflected exceeding well on themselves and their offices. The principal draftsman, Phillip A. Johnson (Colonel USAF, Retired), is owed a note of special appreciation; his scholarship and dedication were truly extraordinary.

This second edition contains a number of editorial changes, refers to several events that have occurred since publication of the first edition, including a brief discussion in Section II of EUTELSAT's actions during the 1999 NATO bombing campaign in Yugoslavia, adds a paragraph in Section VI concerning the U.S.-Soviet Dangerous Military Activities Agreement, and—by popular demand—adds Section XI, Notes for Further Research.

TABLE OF CONTENTS

I. INTRODUCTION

A. Sources and Application of International Law.

International law consists of binding legal obligations among sovereign states. Two of the basic principles of the international legal system are that sovereign states are legally equal and independent actors in the world community, and that they generally assume legal obligations only by affirmatively agreeing to do so. The most effective instruments in creating international law are international agreements, which may be either bilateral or multilateral. Some of these agreements, such as the United Nations Charter, establish international institutions that the parties agree to invest with certain authority. It is also generally accepted that there is a body of customary international law, which consists of practices that have been so widely followed by the community of nations, with the understanding that compliance is mandatory, that they are considered to be legally obligatory.

International institutions have legislative authority to create legal obligations for nations only when their member nations have agreed to give them that authority. The most prominent example is the power of the UN Security Council to pass resolutions requiring individual nations to perform or refrain from certain actions in order to protect or restore international peace and security in the context of a particular situation. The decisions of the International Court of Justice are binding upon nations that have accepted the jurisdiction of the Court and are parties to litigation before it. Other international institutions can also be given the power to impose binding obligations upon nations that agree to submit to their authority. In addition, certain actions of some international institutions, such as the International Court of Justice and the UN General Assembly, are considered to be persuasive evidence of the existence of principles of customary international law.

As with domestic law, the primary mechanism that makes international law effective is voluntary compliance. Also as with domestic law, the threat of sanctions is often required as well. The international legal system provides institutional enforcement mechanisms such as international litigation before the International Court of Justice and other judicial and arbitral tribunals, as well as the right to petition the United Nations Security Council to authorize coercive measures to protect or restore international peace and security. The international legal system also provides self-help enforcement mechanisms such as the right to use force in individual and collective self-defense and the right in some circumstances to repudiate treaty obligations which have been violated by

another party. An aggrieved nation may always withdraw from voluntary relationships involving diplomatic representation and most kinds of commerce. Even the right to publicly complain about another nation's illegal behavior may provide an effective enforcement mechanism if such complaints generate diplomatic costs for the offending nation.

Chief Justice Oliver Wendell Holmes once wrote, "The life of the law has not been logic; it has been experience." It seldom happens that a legislature foresees a problem before it arises and puts into place a legislative solution before it is needed. More typically, legislators react to a problem that has already manifested itself. The international legal system operates in the same manner. The international community ordinarily does not negotiate treaties to deal with problems until their consequences have begun to be felt. This is not all bad, since the solution can be tailored to the actual problems that have occurred, rather than to a range of hypothetical possibilities. One consequence, however, is that the resulting law, whether domestic or international, may be sharply influenced by the nature of the events that precipitate legal developments, together with all their attendant policy and political considerations.

The development of international law concerning artificial earth satellites provides a good example. If the nations had sat down with perfect foresight and asked themselves, "Should we permit those nations among us that have access to advanced technology to launch satellites into orbits that will pass over the territories of the rest of us and take high-resolution imagery, eavesdrop on our telecommunications, record weather information, and broadcast information directly to telephones and computers within our borders?", a very restrictive regime of space law might have resulted. Instead, what happened was that the first satellites launched by the Soviet Union and the United States were seen as entirely benign devices engaged in scientific research, and it was also perfectly clear that no nation had the capability to interfere with them as they passed over its territory. In these circumstances, it quickly became accepted customary international law, soon enshrined in the Outer Space Treaty, that objects in orbit were beyond the territorial claims of any nation, and that outer space is available for exploitation by all.

The history of space law contrasts sharply with that of air law. Much of the early development of heavier-than-air aviation coincided with the First World War, during which the military power of aircraft for collecting intelligence, attacking ground forces, and bombing enemy cities was clearly demonstrated. The result was a highly restricted regime of air law in which any entry into a nation's airspace without its permission was to be regarded as a violation of its sovereignty and territorial integrity.

Similarly, we can make some educated guesses as to how the international legal system will respond to information operations, but the direction that response actually ends up taking may depend a great deal on the nature of the events that draw the nations' attention to the issue. If information operations techniques are seen as just another new technology that does not greatly threaten the nations' interests, no dramatic legal developments may occur. If they are seen as a revolutionary threat to the security of nations and the welfare of their citizens, it will be much more likely that efforts will be made to restrict or prohibit information operations by legal means. These are considerations that national leaders should understand in making decisions on using information operations techniques in the current formative period, but it should also be understood that the course of future events is often beyond the control of statesmen.

The actors in the international legal system are sovereign states. International legal obligations and international enforcement mechanisms generally do not apply to individual persons except where a nation enforces certain principles of international law through its domestic criminal law, or in a very limited class of serious offenses (war crimes, genocide, crimes against humanity, and crimes against peace) that the nations have agreed may be tried and punished by international criminal tribunals.

B. Essentials of Treaty Law.

In domestic U.S. law there are important distinctions between treaties and executive agreements. This distinction primarily involves issues of Constitutional authority within the U.S. government, but it is of little importance internationally. Treaties and executive agreements are equally binding between the United States and the other party or parties to an international agreement. We will use the term "treaty" in this paper as a shorthand way of referring to all forms of legally binding state-to-state international agreements.

Treaty obligations are binding on their parties, but international law recognizes certain circumstances in which a nation can regard a treaty obligation as being suspended, modified, or terminated. The parties can always modify or terminate a treaty by mutual consent. Some international agreements expire by their own terms after a fixed period of time. Generally, unless the terms of the agreement establish a right of unilateral withdrawal, a nation may not unilaterally repudiate or withdraw from a treaty unless it has a basis for doing so that is recognized under international law. Treaty obligations are reciprocal in nature. If one of the parties commits a material breach of its obligations under the treaty, the other may be entitled to suspend its own compliance, or to withdraw from

the agreement entirely. Also, a fundamental change in circumstances may justify a decision by one of the parties to regard its treaty obligations as suspended or terminated.

One of these fundamental changes of circumstance is the initiation of armed hostilities between the parties. Some international agreements specifically provide that they will remain in effect during armed conflict between the parties, such as law of war treaties and the United Nations Charter. Most treaties, however, are silent on whether or not they will continue to apply during hostilities between the parties. Many peacetime agreements facilitate tourism, transportation, commerce, and other relationships the continuation of which would be fundamentally inconsistent with a state of armed conflict between the parties. Agreements on other subjects, such as boundary settlements and reciprocal rights of inheritance of private property, may be unrelated to the existence of hostilities and may ultimately be determined to remain in full force. The issues involved may be particularly complicated when the treaty concerned is multilateral, rather than bilateral. When two parties to a multilateral treaty are engaged in armed conflict, the result may well be that the effect of the treaty is suspended between the belligerents, but remains in effect among each belligerent and the other parties. We will see later in this paper that the United States is a party to a variety of bilateral and multilateral agreements containing obligations that may affect information operations. One of our tasks will be to determine as best we can which of these agreements are likely to remain in effect during hostilities. The tests we will apply are (1) whether there is specific language in the treaty addressing its effect during hostilities between the parties, and (2) if there is no such language, whether the object and purpose of the treaty is or is not compatible with a state of armed hostilities between the parties.

C. New Legal Challenges Presented by Information Operations.

Many traditional military activities are included in current concepts of "information operations" and "information warfare," including physical attacks on information systems by traditional military means, psychological operations, military deception, and "electronic warfare" operations such as jamming radar and radio signals. The application of international law to these traditional kinds of operations is reasonably well settled. Similarly, electro-magnetic pulse (EMP) weapons and directed-energy weapons such as lasers, micro-wave devices, and high energy radio frequency (HERF) guns will probably operate in a manner similar enough to that of traditional weapons that one could apply existing legal principles to them without much difficulty. It will not be as easy to apply existing

international law principles to information attack, a term used to describe the use of electronic means to gain access to or change information in a targeted information system without necessarily damaging its physical components. One of the principal forms of information attack is likely to be computer network attack, or in today's vernacular, the "hacking" of another nation's computer systems.

The proliferation of global electronic communications systems and the increased interoperability of computer equipment and operating systems have greatly improved the utility of all kinds of information systems. At the same time, these developments have made information systems that are connected to any kind of network, whether it be the Internet or some other radio or hard-wired communications system, vulnerable to computer network attacks. Moreover, global communications are almost seamlessly interconnected and virtually instantaneous, as a result of which distance and geographical boundaries have become essentially irrelevant to the conduct of computer network attacks. The result is that many information systems are subject to computer network attack anywhere and anytime. The attacker may be a foreign state, an agent of a foreign state, an agent of a non-governmental entity or group, or an individual acting for purely private purposes. The equipment necessary to launch a computer network attack is readily available and inexpensive, and access to many computer systems can be obtained through the Internet or through another network to which access is obtained.

One major implication is that it may be very difficult to attribute a particular computer network attack to a foreign state, and to characterize its intent and motive. For the purposes of analysis we will initially assume away issues of attribution and characterization, returning to them near the end of the analysis. Another major implication is that an attacker may not be physically present at the place where the effects of the attack are felt. The means of attack may not be tangibly present either, except in the form of anonymous and invisible radio waves or electrons. This will complicate the application of traditional rules of international law that developed in response to territorial invasions and attacks by troops, aircraft, vehicles, vessels, and kinetic weapons that the victim could see and touch, and whose sponsor was usually readily apparent.

II. THE LAW OF WAR

A. Essentials of the Law of War.

The terms "law of war" and "law of armed conflict" are synonymous. The latter term has the virtue that it more clearly applies to all international armed conflicts, whether or not they are formally declared wars. "Law of war" is shorter and more familiar, and we will use it in this paper. The application of the law of war does not generally depend on which of the parties was at fault in starting the conflict. The law of war applies whenever there is a state of international armed conflict, and it applies in the same manner to all the parties to the conflict. There is a small subset of the law of war that applies to noninternational armed conflicts such as civil wars, but those sorts of conflict are not immediately relevant to this paper and will not be discussed. As with other branches of international law, the law of war is composed of treaties and customary international law. The United States is a party to eighteen law of war treaties, along with their various annexes and protocols, and several more law of war agreements are pending before the Senate. The United States also recognizes the existence of a considerable body of customary law of war.

The general principles of the law of war have been expressed in various ways, but their essence can be said to be as follows:

• Distinction of combatants from noncombatants: With very limited exceptions, only members of a nation's regular armed forces are entitled to use force against the enemy. They must distinguish themselves from noncombatants, and they must not use noncombatants or civilian property to shield themselves from attack. If lawful combatants are captured by the enemy they may not be punished for their combatant acts, so long as they complied with the law of war. They are required to be treated humanely in accordance with agreed standards for the treatment of prisoners of war, and they must be released promptly at the cessation of hostilities. Persons who commit combatant acts without authorization are subject to criminal prosecution.

• Military necessity: Enemy military forces are declared hostile. They may be attacked at will, along with their equipment and stores. Civilians and civilian property that make a direct contribution to the war effort may also be attacked, along with objects whose damage or destruction would produce a military advantage because of their nature, location, purpose, or use. A corollary of this principle is that noncombatants and civilian objects making no direct

contribution to the war effort, and whose destruction would provide no significant military advantage to the attacker, are immune from deliberate attack.

• Proportionality: When an attack is made against a lawful military target, collateral injury and damage to noncombatants and civilian property may be unavoidable. Attacks may be carried out against lawful military targets even if some amount of collateral damage is foreseeable, unless the foreseeable collateral damage is disproportionate to the military advantage likely to be attained. The military advantage to be gained from an attack refers to an attack considered as a whole rather than only from isolated or particular parts of an attack. Generally, "military advantage" is not restricted to tactical gains, but is linked to the full context of war strategy. The commander ordering the attack is responsible for making the proportionality judgment. The calculus may be affected somewhat if the enemy has failed to carry out his duty to separate his troops and equipment from noncombatants and civilian property, since in such circumstances the defender must shoulder much of the blame for any collateral damage that results. A corollary of the principle of proportionality is that the attacker has a responsibility to take reasonable steps to find out what collateral damage a contemplated attack may cause.

• Superfluous injury: The nations have agreed to ban certain weapons because they cause superfluous injury. Among these are "dum-dum" bullets, projectiles filled with glass or other nondetectable fragments, poisoned weapons, and laser weapons specifically designed to cause permanent blindness to unenhanced vision.

• Indiscriminate weapons: The nations have agreed to ban certain other weapons because they cannot be directed with any precision against combatants. Among these are bacteriological weapons and poison gas.

• Perfidy: The law of war provides certain visual and electronic symbols to identify persons and property that are protected from attack. Among these are prisoners of war and prisoner of war camps, the wounded and sick, and medical personnel, vehicles, aircraft, and vessels. Any misuse of these protected symbols to immunize a lawful military target from attack constitutes the war crime of perfidy. Suppression of such acts is necessary to preserve the effectiveness of such symbols, since known misuse may lead the combatants to disregard them. For similar reasons, it is unlawful to feign surrender, illness, or death to gain an

advantage in combat, as well as to broadcast a false report of a cease-fire or armistice.

• Neutrality: Nations not engaged in a conflict may declare themselves to be neutral. A neutral nation is entitled to immunity from attack by the belligerents, so long as the neutral nation satisfies its obligation not to assist either side. If a neutral nation is unable or unwilling to halt the use of its territory by one of the belligerents in a manner that gives it a military advantage, the other belligerent may have a right to attack its enemy in the neutral's territory. There is considerable support for the argument that the concept of neutrality has no application during a conflict in which one of the belligerents is a nation or coalition of nations authorized by the UN Security Council to use armed force to protect or restore international peace and security. This conclusion is based upon Article 49 of the Charter, which provides, "The Members of the United Nations shall join in affording mutual assistance in carrying out the measures decided upon by the Security Council." In other situations, however, as when a nation uses armed force in individual or collective self-defense without the benefit of a Security Council mandate, it would appear that nations not involved in the conflict retain the option of declaring themselves to be neutral.

B. Application to Information Operations.

It is by no means clear what information operations techniques will end up being considered to be "weapons," or what kinds of information operations will be considered to constitute armed conflict. On the other hand, those issues may not end up being particularly important to the analysis of law of war issues. If the deliberate actions of one belligerent cause injury, death, damage, and destruction to the military forces, citizens, and property of the other belligerent, those actions are likely to be judged by applying traditional law of war principles.

• Distinction of combatants from noncombatants: This rule grew up when combatants could see each other and make a judgment of whether or not to open fire based in part on whether or not the individual in the sights wore an enemy uniform. When the unit of combat came to be a vessel, tank, truck, or aircraft, it became more important that such vehicles be properly marked than that their occupants wear a distinctive uniform. If a computer network attack is launched from a location far from its target, it may be of no practical significance whether the "combatant" is wearing a uniform. Nevertheless, the law of war requires that lawful combatants be trained in the law of war, that they serve under

effective discipline, and that they be under the command of officers responsible for their conduct. This consideration argues for retaining the requirement that combatant information operations during international armed conflicts be conducted only by members of the armed forces. If combatant acts are conducted by unauthorized persons, their government may be in violation of the law of war, depending on the circumstances, and the individuals concerned are at least theoretically subject to criminal prosecution either by the enemy or by an international war crimes tribunal. The long-distance and anonymous nature of computer network attacks may make detection and prosecution unlikely, but it is the firmly established policy of the United States that U.S. forces will fight in full compliance with the law of war.

• Military necessity: In developed nations both military and civilian infrastructures are vulnerable to computer network attacks. During an armed conflict virtually all military infrastructures will be lawful targets, but purely civilian infrastructures must not be attacked unless the attacking force can demonstrate that a definite military advantage is expected from the attack. Stock exchanges, banking systems, universities, and similar civilian infrastructures may not be attacked simply because a belligerent has the ability to do so. In a long and protracted conflict, damaging the enemy's economy and research and development capabilities may well inhibit its war effort, providing a lawful basis on which to target such capabilities. In a short and limited conflict, however, it would be hard to articulate any expected military advantage from attacking purely economic targets. Targeting analysis must be conducted for computer network attacks just as it traditionally has been conducted for attacks using traditional weapons.

• Proportionality: During Desert Storm, one of the earliest targets of the coalition bombing campaign was the electrical power system in Baghdad. Considering the important military uses being made of electricity from that system, it was clearly a lawful military target. The Iraqi government then made a public pronouncement that the coalition's attack on the city's electrical power system constituted an act of attempted genocide. The logic of this position was that the city's sewage system depended on electric pumping stations, so when the electricity went out the sewage system backed up and created a threat of epidemic disease. No one took this claim very seriously, but this incident highlights the fact that when an attack is made on an infrastructure that is being used for both military and civilian purposes the commander will not be in a proper position to weigh the proportionality of the expected military advantage against the

foreseeable collateral damage unless the commander has made a reasonable effort to discover whether the system is being used for civilian purposes that are essential to public health and safety. This principle operates in exactly the same way whether the attack is carried out using traditional weapons or in the form of a computer network attack.

As stated above, the law of war places much of the responsibility for collateral damage on a defending force that has failed to properly separate military targets from noncombatants and civilian property. When military officials decide to use civilian infrastructure for military purposes (or vice-versa), they ought to consider the fact that such action may make that infrastructure a lawful military target. There may be no choice, as when military traffic has to move on civilian highways and railroads. There may be little alternative to military use of civilian communications systems, since it is impractical to put into place dedicated military communications systems that have sufficient capacity to carry all military communications. Where there is a choice, however, military systems should be kept separate from infrastructures used for essential civilian purposes.

Military command and control systems have long been recognized as lawful military targets. Civilian media generally are not considered to be lawful military targets, but circumstances may make them so. In both Rwanda and Somalia, for example, civilian radio broadcasts urged the civilian population to commit acts of violence against members of other tribes, in the case of Rwanda, or against UN-authorized forces providing humanitarian assistance, in the case of Somalia. When it is determined that civilian media broadcasts are directly interfering with the accomplishment of a military force's mission, there is no law of war objection to using the minimum necessary force to shut them down. The extent to which force can be used for purely psychological operations purposes, such as shutting down a civilian radio station for the sole purpose of undermining the morale of the civilian population, is an issue that has yet to be addressed authoritatively by the international community.

• Superfluous injury: We are not aware that any weapon or device yet conceived specifically for use in information operations has any potential for causing superfluous injury, but new systems should always be reviewed with an eye to their potential for causing catastrophic and untreatable injuries to human beings to an extent not required by military necessity.

• Indiscriminate weapons: The prohibition on indiscriminate weapons may apply to information operations techniques such as malicious logic, as when

malicious logic launched against a military information system spreads to other information systems being used to provide essential services to noncombatants. It might also apply if malicious logic spreads to information systems belonging to neutral or friendly nations. Finally, it might be applied indirectly if the consequence of a computer network attack is to release dangerous forces, such as opening the floodgates of a dam, causing an oil refinery in a populated area to explode in flames, or causing the release of radioactivity.

• Perfidy: It may seem attractive for a combatant vessel or aircraft to avoid being attacked by broadcasting the agreed identification signals for a medical vessel or aircraft, but such actions would be a war crime. Similarly, it might be possible to use computer "morphing" techniques to create an image of the enemy's chief of state informing his troops that an armistice or cease-fire agreement had been signed. If false, this would also be a war crime.

• Neutrality: If a neutral nation permits its information systems to be used by the military forces of one of the belligerents, the other belligerent generally has a right to demand that it stop doing so. If the neutral refuses, or if for some reason it is unable to prevent such use by a belligerent, the other belligerent may have a limited right of self-defense to prevent such use by its enemy. It is quite foreseeable, for example, that a belligerent might demand that a neutral nation not provide satellite imagery of the belligerent's forces to its enemy, or that the neutral cease providing real-time weather information or precision navigation services.

There appears, however, to be a limited exception to this principle for communications relay systems. The primary international agreement concerning neutrality, the 1907 *Hague Convention Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land*, to which the United States is a party, provides in Articles 8 and 9 that "A neutral Power is not called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraph apparatus belonging to it or to Companies or private individuals," so long as such facilities are provided impartially to both belligerents. The plain language of this agreement would appear to apply to communication satellites as well as to ground-based facilities.

There is nothing in this agreement, however, that would suggest that it applies to systems that generate information, rather than merely relay communications. These would include the satellite imagery, weather, and navigation systems mentioned above, as well as other kinds of intelligence-producing systems such as signals intelligence and hydrophonic systems. For example, if a

belligerent nation demanded that the U.S. government deny GPS navigation services to its enemy, and if the U.S. were unable or unwilling to comply, the belligerent may have the right to take necessary and proportional acts in self-defense, such as jamming the GPS signal in the combat area.

International consortia present special problems. Information systems built around space-based components require such huge investments and access to such advanced technology that even developed nations prefer to share the costs with other nations. Where an international communications system is developed by a military alliance such as NATO, few neutrality issues are likely to arise. Other international consortia, however, provide satellite communications and weather data that are used for both civilian and military purposes, and they have a breadth of membership that virtually guarantees that not all members of the consortium will be allies in future conflicts. Some current examples are INTELSAT, INMARSAT, ARABSAT, EUTELSAT, and EUMETSAT. NATO operations in the Federal Republic of Yugoslavia in the Spring of 1999 present a striking case in which EUTELSAT, the majority of whose membership is comprised of NATO members, after two months of the bombing campaign, agreed to stop broadcasting Serbian television programs hostile to the NATO mission. The broadcasting at issue materially contributed to the campaign of Serbian human rights violations and thus was deemed inconsistent with EUTELSAT principles.

Some readers may recall that there was an issue among the members of the INMARSAT consortium providing mobile communications services as to what use could be made of the system by the members' military forces under a provision of the INMARSAT agreement stating that the mobile communications service provided by the system could be used "exclusively for peaceful purposes." This issue has largely disappeared because of the recent privatization of the INMARSAT system. The agreements establishing the new privatized system continue to provide that the management and board of the new INMARSAT must "have regard to" certain principles, including "acting exclusively for peaceful purposes, taking into account the past practices of the Organization and the practice of the Company," and that "[t]he Company shall act exclusively for peaceful purposes." However, this language establishes no enforceable obligation, and no legal remedy is provided for any third party. A recent opinion by the Office of General Counsel of COMSAT, which continues to represent the United States in the new INMARSAT, notes that neither INMARSAT or INTELSAT have ever denied service to the military forces of a member nation, and it concludes, "COMSAT envisions no circumstances in

which the 'peaceful purposes' principle would be invoked as a reason to deny service to the U.S. Department of Defense or units thereof."

C. Assessment.

There are novel features of information operations that will require expansion and interpretation of the established principles of the law of war. Nevertheless, the outcome of this process of extrapolation appears to be reasonably predictable. The law of war is probably the single area of international law in which current legal obligations can be applied with the greatest confidence to information operations.

III. INTERNATIONAL LEGAL REGULATION OF THE USE OF FORCE IN "PEACETIME"

A. International Law Concerning the Use of Force among Nations.

As discussed above, the law of war authorizes a nation engaged in an international armed conflict to employ armed force to attack lawful military targets belonging to the enemy. Resolutions of the United Nations Security Council (UNSC) may also authorize the use of armed force as provided in the UN Charter. The focus of this section, however, is on the application of international law principles in circumstances where there is neither a state of armed conflict nor a UNSC mandate—i.e., in peacetime, including the conduct of military operations other than war.

An exploration of the manner in which international law on the use of force among nations is likely to apply to peacetime computer intrusions will serve three distinct purposes: (1) it will enable a government that is resolved to conduct itself in scrupulous compliance with international law to avoid activities that are likely to be regarded by the target nation and the world community as violations of international law; (2) it will enable a government contemplating activities that might be considered to violate international law to weigh the risks of such actions; and (3) it will enable a government that is the victim of an information attack to identify the remedies afforded to it by international law, including appeals to the Security Council, the use of force in self-defense, and other self-help remedies not involving the use of force.

The frequently-heard question, "Is a computer network attack an act of war?" invokes an obsolete concept not mentioned in the UN Charter and seldom heard in modern diplomatic discourse. An act of war is a violation of another nation's rights under international law that is so egregious that the victim would be justified in declaring war. Declarations of war have fallen into disuse, and the act of war concept plays no role in the modern international legal system. In any event, significant sanctions may follow from much less serious violations of another nation's rights that would not be regarded as acts of war.

The members of the United Nations have agreed in Article 2 (4) of the UN Charter to "refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."

This obligation is elaborated in the *Declaration on Principles of International Law Concerning Friendly Relations and Cooperation among States in Accordance with the*

Charter of the United Nations, General Assembly Resolution 2625 (1970), which provides in part:

- "A war of aggression constitutes a crime against the peace for which there is responsibility under international law."

- "States have a duty to refrain from acts of reprisal involving the use of force."

- "Every State has the duty to refrain from organizing, instigating, assisting or participating in acts of civil strife or terrorist acts in another State or acquiescing in organized activities within its territory directed towards the commission of such acts, when the acts referred to in the present paragraph involve a threat or use of force."

- "Nothing in the foregoing paragraphs shall be construed as enlarging or diminishing in any way the scope of the provisions of the Charter concerning cases in which the use of force is lawful."

NOTE: The United States has often expressed the view that most General Assembly resolutions are only recommendations, but that in exceptional cases particular General Assembly resolutions that are meant to be declaratory of international law, are adopted with the support of all members, and are observed by the practice of states, are persuasive evidence of customary international law on a particular subject. Representatives of the United States have on several occasions publicly endorsed the Declaration on Friendly Relations as one of the few General Assembly resolutions that the United States regards as an authoritative restatement of customary international law, at least until the practice of states fails to demonstrate that they consider its principles to be legally binding.

In its 1974 "Definition of Aggression" Resolution, the General Assembly further provided:

- Article 1. Aggression is the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations, as set out in this Definition.

- Article 2. The first use of armed force by a State in contravention of the Charter shall constitute prima facie evidence of an act of aggression

although the Security Council may, in conformity with the Charter, conclude that a determination that an act of aggression has been committed would not be justified in the light of other relevant circumstances, including the fact that the acts concerned or their consequences are not of sufficient gravity.

- Article 3. Any of the following acts, regardless of a declaration of war, shall, subject to and in accordance with the provisions of Article 2, qualify as an act of aggression:
  (a) The invasion or attack by the armed forces of a State of the territory of another State, or any military occupation, however temporary, resulting from such invasion or attack, or any annexation by the use of force of the territory of another State or part thereof;
  (b) Bombardment by the armed forces of a State against the territory of another State or the use of any weapons by a State against the territory of another State;
  (c) The blockade of the ports or coasts of a State by the armed forces of another State;
  (d) An attack by the armed forces of a State on the land, sea or air forces, or marine and air fleets of another State;
  (e) The use of armed forces of one State which are within the territory of another State with the agreement of the receiving State, in contravention of the conditions provided for in the agreement or any extension of their presence in such territory beyond the termination of the agreement;
  (f) The action of a State in allowing its territory, which it has placed at the disposal of another State, to be used by that other State for perpetrating an act of aggression against a third State;
  (g) The sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to the acts listed above, or its substantial involvement therein.

NOTE: The United States delegation noted that the text of this resolution reflected hard bargaining among the 35 states that were members of the Special Committee on the Question of Defining Aggression. After the resolution was adopted by the General Assembly without a vote, the U.S. delegation stated the view that the resolution did not establish rights and obligations of states, but that it was "likely to provide useful guidance" to the Security Council. Translated,

this statement appears to indicate that the United States does not regard the language of this resolution as a completely authoritative restatement of customary international law, but that its essential concepts are correct. In any event, the question of what constitutes an "act of aggression" is unlikely to be as useful for our purposes as is the question, what kinds of information attacks are likely to be considered by the world community to be "armed attacks" and "uses of force."

Turning to the question of when force may lawfully be used by nations, the United Nations Charter provides that in some circumstances the Security Council may authorize the use of coercive measures, including military force:

- Article 39. The Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security.

- Article 41. The Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures. These may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations.

- Article 42. Should the Security Council consider that measures provided for in Article 41 would be inadequate or have proved to be inadequate, it may take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security. Such action may include demonstrations, blockade, and other operations by air, sea, or land forces of Members of the United Nations.

Perhaps most significantly, the Charter also provides in Article 51, "Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security."

Read together, these provisions of the Charter and the related General Assembly resolutions provide a myriad of terms and concepts concerning prohibited uses of force among nations, including the threat or use of force, acts of aggression, wars of aggression, the use of armed force, acts of armed force,

invasion, attack, bombardment, and blockade. These acts may be directed at the victim nation's territorial integrity or political independence, or against its military forces or marine or air fleets. They all have in common the presence of troops and the use of traditional military weapons. The question before us is how they are likely to apply to computer network attacks.

Further, when one looks for provisions describing a sanction or remedy, only two provisions present themselves: the authority of the Security Council to authorize various sanctions, including the use of the members' armed forces, when it finds there is a "threat to the peace, breach of the peace, or act of aggression;" and Article 51's recognition of the inherent right of self defense "if an armed attack occurs."

There is no requirement that a "threat to the peace" take the form of an armed attack, a use of force, or any other condition specified in the charter. The Security Council has the plenary authority to conclude that virtually any kind of conduct or situation constitutes a "threat to the peace" in response to which it can authorize remedial action of a coercive nature. Nothing would prevent the Security Council from finding that a computer network attack was a "threat to the peace" if it determined that the situation warranted such action. It seems unlikely that the Security Council would take action based on an isolated case of state-sponsored computer intrusion producing little or no damage, but a computer network attack that caused widespread damage, economic disruption, and loss of life could well precipitate action by the Security Council. The debate in such a case would more likely center on the offender's intent and the consequences of the offending action than on the mechanism by which the damage was done.

The language of Article 51, on the other hand, requires an "armed attack." A close parsing of the language would tend to limit its effect to attacks and invasions using traditional weapons and forces. On the other hand, there is a well-established view that Article 51 did not create the right of self-defense, but that it only recognized a pre-existing and inherent right that is in some respects broader than the language of Article 51.

History has also seen the emergence of such derivative doctrines as "anticipatory self-defense" and "self-defense in neutral territory," both of which have been relied upon by the United States in certain circumstances. "Anticipatory self-defense" permits a nation to strike the first blow if it has good reason to conclude that it is about to be attacked. The JCS Standing Rules of Engagement implement this doctrine in their authorization of the use of force in response to a demonstration of "hostile intent" by an adversary. "Self-defense in neutral territory" is the right to use force to neutralize a continuing threat located in the

territory of a neutral state, but not acting on its behalf, when the neutral state is unable or unwilling to fulfill its responsibility to prevent the use of its territory as a base or sanctuary for attacks on another nation. This doctrine has venerable roots in U.S. foreign and defense policy, dating at least to the *Caroline* incident. In December 1837, Canada, which was still a British colony, was fighting an insurrection. More than 1,000 insurgents were encamped on both the Canadian and U.S. sides of the Niagara River. A small steamer, the *Caroline*, was used by the insurgents to travel across and along the river. On the night of December 19, 1837, a party of British troops crossed the Niagara and attacked the *Caroline* in the port of Schlosser, New York, setting the vessel on fire and casting it adrift over the Niagara Falls. One U.S. citizen was killed on the dock, another was missing, and several others were wounded. The United States demanded reparations. The British Government responded that it had acted in self-defense. Secretary of State Daniel Webster agreed that the doctrine of self-defense in neutral territory was a valid principle of international law, but asserted that it did not apply in the circumstances of this case. Britain continued to maintain that its action was legal, but nonetheless apologized for the invasion of U.S. territory. No reparations were paid.

In 1986 the United States bombed Libya as a response to Libya's continuing support for terrorism against U.S. military forces and other U.S. interests. In June 1993 U.S. forces attacked the Iraqi military intelligence headquarters because the government of Iraq had conspired to assassinate former President Bush. In August 1998 U.S. cruise missiles struck a terrorist training camp in Afghanistan and a chemical plant in Sudan in which chemical weapons had been manufactured. The rationale articulated for each of these actions was self-defense. Acts of self-defense must satisfy the tests of necessity and proportionality, but there is no requirement that an act of self-defense use the same means, or target the same type of object, or otherwise be symmetrical to the provocation, or that the action taken be contemporaneous with the provocation, particularly if the attacker is responding to a continuing course of conduct.

B. Acts not Amounting to the Use of Force.

In its 1949 decision in the *Corfu Channel Case*, the ICJ ruled that the intrusion of British warships into Albanian territorial waters, which it found to have been without justification under any principle of international law, constituted a violation of Albania's territorial sovereignty. The result seems to be recognition of a general international law of trespass, although the remedy may be limited to a declaratory judgment that the victim's rights have been violated.

The ICJ's predecessor, the Permanent Court of International Justice, in its 1928 *Chorzow Factory Decision*, declared that reparations were due to any nation whose rights under international law were violated by another nation. This concept is often referred to as the doctrine of state responsibility.

There is also a general recognition of the right of a nation whose rights under international law have been violated to take countermeasures against the offending state, in circumstances where neither the provocation nor the response involves the use of armed force. For example, an arbitral tribunal in 1978 ruled that the United States was entitled to suspend French commercial air flights into Los Angeles after the French had suspended U.S. commercial air flights into Paris. Discussions of the doctrine of countermeasures generally distinguish between countermeasures that would otherwise be violations of treaty obligations or of general principles of international law (in effect, reprisals not involving the use of armed force) and retorsions—actions that may be unfriendly or even damaging, but which do not violate any international legal obligation. The use of countermeasures is subject to the same requirements of necessity and proportionality as apply to self-defense. Some examples of countermeasures that have been generally accepted as lawful are the suspension of diplomatic relations, trade and communications embargoes, cutting off foreign aid, blocking assets belonging to the other nation, and prohibiting travel to or from the other nation.

The international law doctrines of self-defense, reprisal, and countermeasures all require that a nation invoking them do so with the intent of protecting itself against further harm, either by directly blocking further hostile acts against itself or by persuading its tormentor to cease and desist. The motive must be protection of the nation or its citizens or other national interests from further harm—the satisfaction of extracting revenge, by itself, is not acceptable. These doctrines also demand that a state do only what is necessary and proportional in the circumstances.

In summary, it appears that one trend in international law is to provide some kind of remedy for every violation of a nation's rights under international law. Some of these remedies are in the nature of self-help, such as armed self-defense, the interruption of commercial or diplomatic relations, or public protest. Other remedies may be sought from international institutions, such as an imposition of coercive measures by the Security Council, or a declaratory judgment or an order to make reparations from an international tribunal. The issue for the victim is to choose the most effective available sanction. The issue for a nation contemplating an action that may be considered to violate the rights of another nation under international law is to accurately predict what sanctions such action may provoke.

C. Application to Computer Network Attacks.

There is no way to be certain how these principles of international law will be applied by the international community to computer network attacks. As with other developments in international law, much will depend on how the nations and international institutions react to the particular circumstances in which these issues are raised for the first time. If we were to limit ourselves to the language of Article 51, the obvious question would be, "Is a computer network attack an 'armed attack' that justifies the use of force in self-defense?" If we focused on the means used, we might conclude that electronic signals imperceptible to human senses don't closely resemble bombs, bullets, or troops. On the other hand, it seems likely that the international community will be more interested in the consequences of a computer network attack than in its mechanism. It might be hard to sell the notion that an unauthorized intrusion into an unclassified information system, without more, constitutes an armed attack. On the other hand, if a coordinated computer network attack shuts down a nation's air traffic control system along with its banking and financial systems and public utilities, and opens the floodgates of several dams resulting in general flooding that causes widespread civilian deaths and property damage, it may well be that no one would challenge the victim nation if it concluded that it was a victim of an armed attack, or of an act equivalent to an armed attack. Even if the systems attacked were unclassified military logistics systems, an attack on such systems might seriously threaten a nation's security. For example, corrupting the data in a nation's computerized systems for managing its military fuel, spare parts, transportation, troop mobilization, or medical supplies may seriously interfere with its ability to conduct military operations. In short, the consequences are likely to be more important than the means used.

If the international community were persuaded that a particular computer network attack or a pattern of such attacks should be considered to be an "armed attack," or equivalent to an armed attack, it would seem to follow that the victim nation would be entitled to respond in self-defense either by computer network attack or by traditional military means in order to disable the equipment and personnel that were used to mount the offending attack. In some circumstances it may be impossible or inappropriate to attack the specific means used in an attack (e.g., because the specific equipment and personnel used cannot be reliably identified or located, or an attack on the specific means used would not be effective, or an effective attack on the specific means used might result in disproportionate collateral damage). Where the specific means cannot be effectively attacked, any legitimate military target could be attacked, including intelligence

and military leadership targets, as long as the purpose of the attack is to dissuade the enemy from further attacks or to degrade the enemy's ability to undertake them.

There has been some support for the proposition that a nation has an inherent right to use force in self-defense against acts that do not constitute a classic armed attack. This view is supported by the inclusion in the General Assembly's definition of aggression of acts that do not entail armed attacks by a nation's armed forces, such as the unlawful extension of the presence of visiting forces, or allowing a nation's territory to be used by another state "for perpetrating an act of aggression against a third State." (See pages A-8–A-11 above). U.S. practice also support this position, as demonstrated in the 1986 bombing of Libyan command and leadership targets to persuade Libya to stop sponsoring terrorist attacks against U.S. interests, and in the 1993 attack on the Iraqi military intelligence headquarters to persuade Iraq to desist from assassination plots against former President Bush. A contrary view was expressed in the International Court of Justice's 1986 ruling in *Nicaragua v. U.S.* that the provision of arms by Nicaragua to the leftist rebels in El Salvador did not constitute an armed attack on El Salvador, so it could not form the basis of a collective self-defense argument that would justify armed attacks in response, such as laying of mines in Nicaraguan waters or certain attacks on Nicaraguan ports, oil installations and a naval base—acts that were "imputable" to the United States. The Court also said it had insufficient evidence to determine whether certain cross-border incursions by Nicaraguan military forces into the territory of Honduras and Costa Rica constituted armed attacks. The extent to which Nicaragua's conduct would justify El Salvador and its ally the United States in responding in ways that did not themselves constitute an armed attack was not before the Court. The opinion of the court nevertheless provides some support for the proposition that the provocation must constitute an armed attack before it will justify an armed attack in self-defense. It seems safe to say that the issue of whether traditional armed force may be used in self-defense in response to provocations that are not technically regarded as armed attacks is far from settled, and that the positions taken by states may be sharply influenced by the nature of the events concerned, together with all attendant policy and political considerations.

By logical implication, to the extent that a nation chooses to respond to a computer network attack by mounting a similar computer network attack of its own, the issue of whether the initial provocation constituted an armed attack may become a tautology. If the provocation is considered to be an armed attack, the victim may be justified in launching its own armed attack in self-defense. If the provocation is not considered to be an armed attack, a similar response will

also presumably not be considered to be an armed attack. Accordingly, the question of the availability of the inherent right of self-defense in response to computer network attacks comes into sharpest focus when the victim of a computer network attack considers acting in self-defense using traditional military means. The issue may also arise if the response causes disproportionately serious effects (e.g., if a state responded to a computer network attack that caused only minor inconvenience with its own computer network attack that caused multiple deaths and injuries). As in all cases when a nation considers acting in self-defense, the nation considering such action will have to make its best judgment on how world opinion, or perhaps a body such as the International Court of Justice (ICJ) or the UNSC, is likely to apply the doctrine of self-defense to electronic attacks. As with many novel legal issues, we are likely to discover the answer only from experience.

It seems beyond doubt that any unauthorized intrusion into a nation's computer systems would justify that nation at least in taking self-help actions to expel the intruder and to secure the system against reentry. An unauthorized electronic intrusion into another nation's computer systems may very well end up being regarded as a violation of the victim's sovereignty. It may even be regarded as equivalent to a physical trespass into a nation's territory, but such issues have yet to be addressed in the international community. Furthermore, the act of obtaining unauthorized access to a nation's computer system creates a vulnerability, since the intruder will have had access to the information in the system and he may have been able to corrupt data or degrade the operating system. Accordingly, the discovery that an intrusion has occurred may call into question the reliability of the data and the operating system and thus reduce its utility. If an unauthorized computer intrusion can be reliably characterized as intentional and it can be attributed to the agents of another nation, the victim nation will at least have the right to protest, probably with some confidence of obtaining a sympathetic hearing in the world community.

D. An "Active Defense" against Computer Network Attacks.

A persistent foreign intruder who gains repeated unauthorized entry into a nation's computer systems by defeating a variety of security measures or who gains entry into a number of computer systems may demand a different response. Such behavior may indicate both that there is a continuing danger and that coercive measures are necessary to stop the intruder's pattern of conduct. Similarly, there may be a right to use force in self-defense against a single foreign electronic attack in circumstances where significant damage is being done to the attacked

system or the data stored in it, when the system is critical to national security or to essential national infrastructures, or when the intruder's conduct or the context of the activity clearly manifests a malicious intent.

If it is capable of doing so, in such circumstances the victim nation may be justified in launching a computer network attack in response, intended to disable the equipment being used by the intruder. Disabling one computer may or may not defeat a state-sponsored operation. It may, however, serve as a "shot across the bow" warning of more serious consequences if the offending behavior continues. It is also an action unlikely to come to public attention unless one of the two governments announces it, making it a potentially useful measure for conflict avoidance. Conducting a responsive computer network attack as a measure of self-defense against foreign computer network attacks would have the major advantage that it would minimize issues of proportionality, which would be more likely to arise if traditional military force were used, such as firing a cruise missile at the building from which a computer network attack is being conducted. Either response would likely be analyzed on the basis of the traditional criteria of necessity and proportionality.

If it is impractical to focus an attack on the equipment used in the provocation, any legitimate military target may be attacked. The primary value of being able to demonstrate a nexus between the provocation and the response is to be able to argue the likely therapeutic effect of the force used in self-defense. As a practical matter, the next most attractive target after the equipment used in the provocation may be the offending nation's communications systems, or its military or intelligence chain of command. The consequences of a large-scale campaign of computer network attacks might well justify a large-scale traditional military response.

As stated above, the discussion up to this point has assumed we know who an intruder is, and that we are confident in characterizing his intent. In practice, this is seldom the case, at least in the early stages of responding to computer intrusions. The above legal analysis may change if the identity and location of an intruder is uncertain, or if his intent is unclear.

Identification of the originator of an attack has often been a difficult problem, especially when the intruder has used a number of intermediate relay points, when he has used an "anonymous bulletin board" whose function is to strip away all information about the origin of messages it relays, or when he has used a device that generates false origin information. Progress has been made, however, in solving the technical problem of identifying the originator of computer messages, and reliable identification of the computer that originated a message may soon be routinely available. Attribution may also be provided by

intelligence from other sources, or it might be reliably inferred from the relationship of the attack to other events.

Locating the computer used by the intruder does not entirely solve the attribution problem, however, since it may have been used by an unauthorized person, or by an authorized user for an unauthorized purpose. A parent may not know that the family computer is being used for unlawful attacks on government computer systems. Universities, businesses, and other government agencies may be similarly unaware that their computer systems are being misused. The owner of a computer system may have some responsibility to make sure it is not being used for malicious purposes, but the extent of such responsibility, and the consequences of failing to meet it, have apparently not been addressed in any U.S. or foreign statute or court decision. These considerations should make us cautious in implementing any "active defense" system for government computer systems. Nevertheless, circumstances may arise in which the urgency of protecting critical information systems from serious damage may warrant adoption of a properly designed "active defense."

Similarly, characterization of an intruder's intentions may be difficult. Nevertheless, such factors as persistence, sophistication of methods used, targeting of especially sensitive systems, and actual damage done may persuasively indicate both the intruder's intentions and the dangers to the system in a manner that would justify use of an "active defense." As with attribution, there may be useful intelligence on this issue from other sources, or it may be possible to reliably infer the intent of the intruder from the relationship of the attack to other events.

A determination that an intrusion originates in a foreign country would be only a partial solution to the attribution problem, since the attack may or may not be state-sponsored. State-sponsored attacks may well generate the right of self-defense. State sponsorship might be persuasively established by such factors as signals or human intelligence, the location of the offending computer within a state-controlled facility, or public statements by officials. In other circumstances, state sponsorship may be convincingly inferred from such factors as the state of relationships between the two countries, the prior involvement of the suspect state in computer network attacks, the nature of the systems attacked, the nature and sophistication of the methods and equipment used, the effects of past attacks, and the damage which seems likely from future attacks.

Attacks that cannot be shown to be state-sponsored generally do not justify acts of self-defense in another nation's territory. States jealously guard their sovereign prerogatives, and they are intolerant of the exercise of military, law-enforcement, and other "core sovereign powers" by other states within their territory without their consent. When individuals carry out malicious acts

for private purposes against the interests of one state from within the territory of a second state, the aggrieved state does not generally have the right to use force in self-defense against either the second state itself or the offending individual. Even if it were possible to conduct a precise computer network attack on the equipment used by such individual actors, the state in which the effects of such an attack were felt, if it became aware of it, could well take the position that its sovereignty and territorial integrity had been violated. The general expectation is that a nation whose interests are damaged by the private conduct of an individual who acts within the territory of another nation will notify the government of that nation and request its cooperation in putting a stop to such conduct.

Only if the requested nation is unwilling or unable to prevent recurrence does the doctrine of self-defense permit the injured nation to act in self-defense inside the territory of another nation. The U.S. cruise missile strikes against terrorists camps in Afghanistan on 20 August 1998 provide a close analogy in which the United States attacked camps belonging to a terrorist group located in the territory of a state which had clearly stated its intention to continue to provide a refuge for the terrorists. At some point, providing safe refuge for those who conduct attacks against another nation becomes complicity in those attacks. At a minimum, the offended nation is authorized to attack its tormenters, the terrorists. As complicity shades into the kinds of active support and direction that are commonly called "state sponsorship," military and leadership targets of the host state may themselves become lawful targets for acts of self-defense.

Attacks on insurgents or on terrorists and other criminals using a neutral nation's territory as a refuge may also be justified when the neutral state is unable to satisfy its obligations. During the Vietnam war, the United States attacked North Vietnamese military supply lines and base camps in Cambodia after the Cambodian government took the position that it was unable to prevent North Vietnam from making such use of its territory. This principle might justify using active defense measures against a computer intruder located in a neutral nation if the government of the neutral nation declared it had no way to locate the intruder and make him stop, or if its behavior made it clear that it could not or would not act, or even if the circumstances did not allow time for diplomatic representations to be effective. As an analogy, it seems unlikely that a nation would complain very loudly if its neighbor nation returned fire against a terrorist sniper firing from its territory.

In summary, the international law of self-defense would not generally justify acts of "active defense" across international boundaries unless the provocation could be attributed to an agent of the nation concerned, or until the sanctuary nation has been put on notice and given the opportunity to put a stop to such

private conduct in its territory and has failed to do so, or the circumstances demonstrate that such a request would be futile. Nevertheless, in some circumstances the National Command Authority (NCA) might decide to defend U.S. information systems by attacking a computer system overseas, and take the risk of having to make an apology or pay compensation to the offended government. Among the factors the NCA would probably consider would be the danger presented to U.S. national security from continuing attacks, whether immediate action is necessary, how much the sanctuary nation would be likely to object, and how the rest of the world community would be likely to respond.

There need be less concern for the reaction of nations through whose territory or communications systems a destructive message may be routed. If only the nation's public communications systems are involved, the transited nation will normally not be aware of the routing such a message has taken. Even if it becomes aware of the transit of such a message and attributes it to the United States, there would be no established principle of international law that it could point to as being violated. As discussed above, even during an international armed conflict international law does not require a neutral nation to restrict the use of its public communications networks by belligerents. Nations generally consent to the free use of their communications networks on a commercial or reciprocal basis. Accordingly, use of a nation's communications networks as a conduit for an electronic attack would not be a violation of its sovereignty in the same way that would be a flight through its airspace by a military aircraft.

A transited state would have somewhat more right to complain if the attacking state obtained unauthorized entry into its computer systems as part of the communications path to the target computer. It would be even more offended if malicious logic directed against a target computer had some harmful effect against the transited state's own equipment, operating systems, or data. The possibility of such collateral damage would have to be carefully considered by the state launching any such attack. If there were a high potential for such collateral damage to transited systems, the weapon might even be considered to be an "indiscriminate" weapon incapable of being reliably directed against a legitimate target.

There are at least two ways in which the availability of improved technology may affect the active-defense equation. First, it might be argued that as a government acquires the ability to build better firewalls and other security systems it will be harder to argue that an active defense is "necessary." This argument might be raised even if the target government has failed to install all possible technological security measures on the system that is under attack. This demanding approach to "necessity" finds little support in the practice of nations.

The focus of self-defense analysis is on events as they unfold, and not as they might have been if different budgeting and acquisition decisions had been made sometime in the past. If such systems are in place, however, their apparent effectiveness should be taken into account in deciding whether active defense measures are necessary. This does not mean that a nation has no right of self-defense where a first attempted intrusion fails, or even when a series of intrusions fail. If an attacker is permitted to continue mounting a campaign of such attacks it may learn by trial and error, it may employ other capabilities, or it may stumble onto a point of vulnerability. Just as an infantry unit exercising the right of self-defense may pursue a force that breaks off an attack and attempts to retreat until the attacker ceases to be a threat, decisions on taking measures of self-defense against computer network attacks must take into account the extent to which an attacker continues to present a threat of continuing attacks.

Another possible implication of a defender's technological prowess may arise when a nation has the capacity for graduated self-defense measures. Some may argue that a nation having such capabilities must select a response that will do minimal damage. This is a variant of the argument that a nation possessing precision-guided munitions must always use them whenever there is a potential for collateral damage. That position has garnered little support among nations and has been strongly rejected by the United States. There is broad recognition that the risk of collateral damage is only one of many military considerations that must be balanced by military authorities planning an attack. One obvious consideration is that a military force that goes into a protracted conflict with a policy of always using precision-guided munitions whenever there is any potential for collateral damage will soon exhaust its supply of such munitions. Similarly, military authorities must be able to weigh all relevant military considerations in choosing a response in self-defense against computer network attacks. These considerations will include the probable effectiveness of the means at their disposal, the ability to assess their effects, and the "fragility" of electronic means of attack (i.e., once they are used, an adversary may be able to devise defenses that will render them ineffective in the future). In the process of reasoning by analogy to the law applicable to traditional weapons, it must always be kept in mind that computer network attacks are likely to present implications that are quite different from the implications presented by attacks with traditional weapons. These different implications may well yield different conclusions.

It may be possible to specify certain information systems that are vital to national security—both government systems and key civilian infrastructure systems. This process should serve both to give such systems high priority for security measures and also to identify a class of systems any attack on which

would immediately raise the issue of whether an active defense should be employed. This should not, of course, eliminate consideration of using an active defense against attacks on systems not on such a "vital systems" list where the circumstances justify such action. For example, a vigorous attack that threatens to overwhelm an information system not on the "vital systems" list but that performs an important national security function could be a more valid occasion to use active defense measures than would be a trivial and easily defeated attack on a designated "vital system." A list of "vital systems" would serve primarily as an alert mechanism that would bring about a prompt high-level evaluation of all the circumstances.

In addition, it would be useful to create a process for determining when the response to a computer intrusion should shift from the customary law enforcement and counter-intelligence modes to a national defense mode. Such a process should include (1) a statement of general criteria to be applied; (2) identification of officials or agencies that will be involved in making the decision; and (3) procedures to be followed.

There are of course a variety of treaty obligations that will have to be considered before adopting an "active defense" against foreign computer network attacks, and these will be discussed below. There are also a variety of domestic legal concerns that will have to be addressed, and these will be discussed in the companion assessment of domestic law issues in information operations.

E. Assessment.

It is far from clear the extent to which the world community will regard computer network attacks as "armed attacks" or "uses of force," and how the doctrines of self-defense and countermeasures will be applied to computer network attacks. The outcome will probably depend more on the consequences of such attacks than on their mechanisms. The most likely result is an acceptance that a nation subjected to a state-sponsored computer network attack can lawfully respond in kind, and that in some circumstances it may be justified in using traditional military means in self-defense. Unless the nations decide to negotiate a treaty addressing computer network attacks, which seems unlikely anytime in the near future, international law in this area will develop through the actions of nations and through the positions the nations adopt publicly as events unfold. U.S. officials must be aware of the implications of their own actions and statements in this formative period.

IV. SPACE LAW

A. Introduction.

International law regulating activities in outer space is important to the information operator because space segments are critical to so many important information systems. These systems perform such functions as communications relay, imagery collection, missile warning, navigation, weather forecasting, and signals intelligence. In fact, it can be said that at the current stage of space activity, the exclusive functions of both military and civilian satellites are to gather and relay information. In the conduct of information operations, there will be strong imperatives to interfere with the space-based information systems belonging to an adversary, and to defend one's own.

One approach to attacking space systems is by targeting their ground stations. Another approach is to jam or "spoof" their communications links. Such actions are subject to the normal international law principles governing other terrestrial activity. Sometimes, however, it may be more effective to attack the satellite or satellites that form the space segment of the system. As we will see, activities in space are subject both to general principles of international law and to a number of treaty obligations that apply specifically to space activities.

B. Space Law Treaties.

There is probably no other field of human endeavor that produced so much international law in such a short period. Within twenty years after the first Sputnik launch in 1957, international diplomatic conferences produced four major widely-accepted multilateral space law treaties. Taken together, these treaties provide the foundations of existing space law.

- *The Treaty on Principles Governing the Activities of States in the Exploration and Use Of Outer Space, including the Moon and Other Celestial Bodies* (the Outer Space Treaty, 1967)

- *The Agreement on the Rescue of Astronauts, Return of Astronauts, and the Return of Objects Launched into Outer Space* (the Rescue and Return Agreement, 1968)

- *The Convention on International Liability for Damages Caused by Space Objects* (the Liability Convention, 1972)

- *The Convention on the Registration of Objects Launched into Outer Space* (the Registration Convention, 1975)

Note: There is another treaty called the Moon Agreement of 1979 which the United States has never signed and which has attracted only 9 parties, among whom only France is active in space operations. In addition, several provisions of the 1980 Environmental Modification Convention apply to space activity. These agreements are not directly relevant to information operations, however, and they will not be discussed further here.

The four major space treaties together establish the following principles that are directly relevant to information operations. These principles have been so widely accepted that they are generally regarded as constituting binding customary international law, even for non-parties to these agreements.

- Space is free for exploration and use by all nations. It is not subject to national appropriation by claim of sovereignty, use, occupation, or any other means.

- Activities in space shall be conducted with due regard for the interests of other states.

- States that launch space objects are liable for any damage they may do in space, in the air, or on the surface of the Earth. Different standards of liability are established for damage done to other items in space, for which a "fault" standard applies, and damage done on the surface of the Earth and to aircraft in flight, for which absolute liability applies.

- Space activities are subject to general principles of international law, including the UN Charter.

Several conclusions are apparent from these general principles. The first is that the rules on the use of force discussed in Section III of this paper apply fully to activities in outer space. Among these are that nations are obliged not to use force in their relations with each other unless they are acting in self-defense or when authorized to do so by the UN Security Council. Once again, however, as with other forms of information operations, one has to consider what actions by or against objects in space will be considered to be uses of force. The world community would probably not hesitate to regard as a use of force the destruction of a satellite by a missile or a laser. It would probably react similarly if it could be

proven that one nation took over control of another nation's satellite by electronic means and caused it to fire its retro rockets and fall out of orbit. In such a case, the consequences will probably matter more than the mechanism used. The reaction of the world community to lesser kinds of interference is hard to predict. For example, if one nation were able by electronic means to suspend the operations of another nation's satellite for a brief period, after which it returned to service undamaged, it seems likely that the world community would consider such action as a breach of the launching nation's sovereign rights, but not as a use of armed force.

One could argue, however, that this argument is unimportant because the space treaties create a specific obligation not to interfere with the space activities of other nations, and to pay reparations for any damages resulting from such interference. This argument appears to have considerable force, at least in peacetime. During an international armed conflict between the two nations concerned, however, the law of armed conflict would apply unless it was trumped by the principle of noninterference with space systems. Resolution of this issue depends largely on whether the four space treaties will be considered to apply during an armed conflict. None of them has any specific provision that indicates whether the parties intended that the agreement apply in wartime.

There appears to be a strong argument that the principle of noninterference established by these agreements is inconsistent with a state of hostilities, at least where the systems concerned are of such high military value that there is a strong military imperative for the adversary to be free to interfere with them, even to the extent of destroying the satellites in the system. As indicated in the discussion of treaty law in the introduction to this paper, the outcome of this debate may depend on the circumstances in which it first arises in practice. Nevertheless, it seems most likely that these agreements will be considered to be suspended between the belligerents for the duration of any armed conflict, as least to the extent necessary for the conduct of the conflict.

If the principle of noninterference is regarded as suspended for the period of the conflict, it also seems likely that the liability provisions in these agreements would also be suspended, at least between the parties. This would not, however, excuse the belligerents from liability to neutral nations if their actions caused damage to their citizens or property

C. Specific Prohibitions of Military Activities in Space.

There is a popular notion that military activities in space are prohibited—that space is a place a little closer to heaven into which the nations have agreed not to

introduce weapons and human conflict. There is a germ of truth in this notion, supported by high flights of rhetoric in international fora, but the existing treaty restrictions on military operations in space are in fact very limited. These restrictions are included in both the space treaties listed above and in various arms control agreements.

The Outer Space Treaty provides that the parties will not "place in orbit around the Earth any objects carrying nuclear weapons or any other kinds of weapons of mass destruction, install such weapons on celestial bodies [i.e., the moon, planets, and asteroids], or station such weapons in outer space in any other manner." The treaty permits placing in orbit weapons other than nuclear weapons and other weapons of mass destruction. Also, the treaty contains no prohibition against nuclear weapons transiting outer space, as long as they do not enter into an earth orbit and they do not explode in outer space.

The Outer Space Treaty also prohibits the establishment of military bases, the testing of weapons, and the conduct of military maneuvers on the moon or other celestial bodies. It permits these activities in orbit around the Earth, and in other places in outer space. Similarly, there is no prohibition against establishing military space stations or operating other satellites with offensive or defensive capabilities.

The Treaty Banning Nuclear Weapons Tests in the Atmosphere, in Outer Space and Under Water (the Limited Test Ban Treaty, 1963) prohibits all nuclear explosions in outer space. Accordingly, a party to this agreement may not lawfully explode a nuclear device in outer space in order to disable an adversary's satellites by means of the electro-magnetic pulse generated by a nuclear explosion, or by its other effects. A nation operating its own satellite systems is unlikely to take such an action in any event, since its own satellites would be subject to the same effects as those belonging to its adversary.

The Treaty on the Limitation of Anti-Ballistic Missile Systems (the ABM Treaty, 1972) provides that no party may "develop, test or deploy space-based ABM systems or components."

Under a 1997 theater missile defense (TMD) agreement not yet ratified by the Senate, the United States and Russia have agreed not to place in space theater missile defense interceptor missiles "or space-based components based on other physical principles, whether or not part of a system, that are capable of substituting for such interceptor missiles."

A number of arms control agreements provide that no party will interfere with the others' "national technical means of verification." Translated, this means no interference with the orbiting imaging systems used to monitor the strategic arms of another party.

Read together, these agreements permit the development, testing, and deployment of anti-satellite and satellite-defense systems unless they involve either the stationing or testing of nuclear devices in outer space or the orbiting of systems that also have ABM or ATM capabilities. Their use is subject only to (1) the general principles of international law relating to the use of force; (2) the principle of non-interference with the space systems of other nations in peacetime, subject to the right to use force in self-defense and when authorized by the UN Security Council; (3) the law of war during international armed conflicts; and (4) obligations under relevant arms-control agreements not to interfere with other parties' national technical means of verification. This leaves a very broad range of permissible "space-control" systems and operations.

In a non-nuclear conflict, the parties might very well determine that the treaty prohibitions against placing nuclear weapons in orbit, against exploding nuclear devices in outer space, and against placing ABM components and ATM interceptors in orbit remain consistent with a state of limited armed conflict. Those obligations may well serve to avoid escalation of the conflict to the nuclear level. The parties' conclusions as to the obligation not to interfere with other parties' national technical means of verification will probably depend to a great extent on the circumstances of the conflict.

D. Domestic Law and Policy.

A federal statute, 18 USC 1367, makes it a felony to intentionally or maliciously interfere with a communications or weather satellite, or to obstruct or hinder any satellite transmission. The application of this statute to national security information operations is discussed in the companion assessment of domestic legal issues.

U.S. domestic policy on developing space control capabilities has been inconsistent at best. By the early 1980s the U.S. Air Force had developed an anti-satellite missile with an explosive warhead that was carried aloft by an F-15 fighter and launched at high altitude. A test of this system was conducted in 1985 against a U.S. satellite whose useful life had expired. Congress soon thereafter decreed that no appropriated funds were to be used to test any weapon against an object in orbit. In 1987 the USAF program was terminated. At the time, it appeared that members of Congress voting for the ban had done so for a variety of reasons, among which were: (1) support for the broad principle that space should be free from human conflict; (2) dismay that the first test had generated 285 pieces of trackable space debris; (3) concern that further testing of an anti-satellite capability might interfere with continuing strategic arms control

negotiations; and (4) concern that the United States should not press ahead with testing an anti-satellite system when the nation had yet to decide where its own long-term interests lie. Concerning this last point, it was obvious that there is a military interest in being able to defend your own space systems and having the ability to interfere with your adversary's, but there was also a contrary consideration that the long-term interests of the United States—as the nation that depends most heavily on space systems—may be better served by promoting the development of a regime of international law that prohibits any interference by one nation with the space systems of another, and inhibits the acquisition of the capability to do so. That fundamental debate has yet to be pursued to a definitive conclusion.

Later, when public attention was drawn to the possible use of lasers as anti-satellite weapons, Congress prohibited the use of appropriated funds to illuminate any object in orbit with a laser. This restriction was removed in 1995. In October 1997 the U.S. Army conducted a test in which it illuminated an Air Force satellite nearing the end of its useful life with the MIRACL laser, located at White Sands, New Mexico. Despite public announcements that the purpose of the experiment was purely defensive in nature—to observe the effects of the laser on the satellite's optical sensors in order to better protect U.S. satellites from deliberate or accidental laser illumination—a public furor ensued. Shortly thereafter President Clinton exercised his short-lived item veto authority to delete funds from the FY 98 DoD Authorization Act for development of an Army Kinetic Energy Anti-Satellite Missile and two other projects that he considered to be related to space control. Congress approved additional funds for space control projects in the FY 1999 DoD Authorization Act and urged expenditure of the FY 98 funds that were restored after the Supreme Court ruled that the item veto was unconstitutional.

At this point, it seems fair to say that the United States has not arrived at a consensus on the fundamental policy issues concerning space control. It seems likely for the near future that the development of such systems will continue, with renewed controversy to be expected as soon as a decision is imminent on the deployment, or even advanced testing, of an operational system.

E. International Efforts to Control "Weaponization of Space".

Over the last decade there has been strong support in the UN General Assembly for negotiation in the Conference on Disarmament (CD) of a draft treaty banning weapons in space. The most recent action by the General Assembly was its adoption on 4 December 1998 by a vote of 165-0-4 of a resolution entitled

"Prevention of an arms race in outer space." This resolution calls for reestablishment by the CD of an Ad Hoc Committee on the Prevention of an Arms Race in Outer Space that existed in prior years. Canada and Egypt are actively promoting consideration of a "no weapons in space" treaty in the CD, but so far they have garnered little active support among the other CD members. Both Russia and China have also announced their support for negotiations to ban "weaponization of space," but neither has advanced a specific proposal with much vigor. In summary, there appears to be widespread lukewarm support for the general idea of a treaty banning an "arms race in space," but the subject enjoys a low priority at the moment and no draft treaty has garnered significant support. This may all change if and when a nation or nations are known to have deployed operational space control systems, or are on the verge of doing so.

Chinese and Russian support for a ban on "weaponization of space" is seen in some quarters as ironic, since China is reported to be developing a ground-based anti-satellite laser system and Russia is the only nation known to have once had an operational anti-satellite missile. There have been a number of reports that the Soviet Union developed a "co-orbital ASAT" that was launched into orbit, where it maneuvered close enough to a target satellite to destroy the target by exploding. Reportedly, the Soviet system was tested against objects in space 20 times and became operational in 1978. Russia consistently denied that it had tested or deployed such a system until September 1997, when press reports indicate that President Yeltsin said in a letter to President Clinton that Russia at one time possessed an anti-satellite capability, but that it had since "renounced" it.

F. Assessment.

There is no legal prohibition against developing and using space control weapons, whether they would be employed in orbit, from an aircraft in flight, or from the Earth's surface. The primary prohibition is against weapons that entail the placing of nuclear weapons in orbit or that would employ a nuclear explosion in outer space. The use of space control systems in peacetime would be subject to both the general principles of international law and to treaty obligations not to interfere with other nations' space systems and national technical means of verification. These obligations would probably be suspended during an international armed conflict, during which the parties' conduct would be governed primarily by the law of war. U.S. domestic policy on space control, however, is at best unsettled.

V. COMMUNICATIONS LAW

A. International Communications Law.

International communications law consists primarily of a number of bilateral and multilateral communications treaties. The most significant of these treaties is the *International Telecommunications Convention of 1982* (ITC), which has over 140 parties and which became effective for the United States in 1986. This agreement, often referred to as the Nairobi Convention, is the latest in a series of widely adhered to multilateral telecommunications conventions signed in this century, which were preceded by multilateral agreements in the late 1800s providing protection for submarine cables. The current series of agreements establishes the International Telecommunication Union (ITU), which has the status of a specialized agency of the United Nations, and they invest the ITU with the authority to formulate telegraph and telephone regulations which become binding legal obligations upon formal acceptance by ITU member nations. These agreements also establish mutual legal obligations among the parties, several of which are directly relevant to information operations.

Perhaps the most significant of these obligations is in Article 35, which provides that all radio "stations, whatever their purpose, must be established and operated in such a manner as not to cause harmful interference to the radio services or communications of other Members or of recognized private operating agencies, which carry on radio service, and which operate in accordance with the provisions of the Radio Regulations." "Harmful interference" is defined in Annex 2 to the Convention as "interference which endangers the functioning of a radio navigation service or of other safety services or seriously degrades, obstructs or repeatedly interrupts a radio communication service operating in accordance with the Radio Regulations." One of the clearest violations of this provision would be the jamming or "spoofing" of a radio navigation service. Without speculating on all the possible permutations of the application of this provision to the broad range of information operations, suffice it to say that this provision on its face would appear to restrict many such operations that involve the use of radio broadcasting.

On the other hand, Article 38 of the ITC provides a specific exemption for military transmissions: "Members retain their entire freedom with regard to military radio installations of their army, naval and air forces." In July 1994, when the United States was considering broadcasting messages to the Haitian people from U.S. military aircraft in international airspace urging them not to set out to sea in hazardous vessels, the Office of Legal Counsel in the Department of

Justice relied on the military exemption in Article 38 as one of several bases for determining that the ITC does not prohibit such activity. Article 38 goes on to say, "Nevertheless, these installations must, so far as possible, observe . . . the measures to be taken to prevent harmful interference, and the provisions of the Administrative Regulations concerning the types of emission and the frequencies to be used, according to the nature of the service performed by such installations." While this provision indicates that military installations do not have carte blanche to interfere with civilian communications, the phrase "so far as possible," read together with the specific exemption for military radio installations, provides considerable room to maneuver for information operations conducted by military forces.

The ITC also provides specific authority for its member nations to interfere with international telecommunications in certain circumstances:

- Article 19 allows members to "stop the transmission of any private telegram which may appear dangerous to the security of the State or contrary to their laws, to public order or to decency, provided that they immediately notify the office of origin of the stoppage of any such telegram or part thereof, except when such notification may appear dangerous to the security of the State."

- Article 19 also permits members to "cut off any other private telecommunications which may appear dangerous to the security of the State or contrary to its laws, to public order or to decency."

- Article 20 reserves the right of members "to suspend the international telecommunication service for an indefinite time, either generally or only for certain relations and/or certain kinds of correspondence, outgoing, incoming or in transit, provided that it immediately notifies such action to each of the other Members through the medium of the Secretary-General."

Finally, it seems clear that the ITC's provisions apply primarily in peacetime. The treaty does not specifically state how—if at all—it will apply during an armed conflict. Nevertheless, there is ample precedent in which nations have demonstrated conclusively that they regard the provisions of international communications conventions as being suspended between belligerents engaged in armed conflicts. Prior to the First World War, for example, all the major European nations were parties to the 1884 *Convention for Protection of Submarine*

Cables. The first day of the war, the British Navy pulled up and cut the five major submarine cables serving Germany. Throughout all the wars of this century, communications facilities of all sorts have been regarded as priority military targets. Since some of the parties to the ITC and other multilateral communications conventions are likely to be neutrals in armed conflicts between other nations, the result may become somewhat complicated. Most ITC obligations will be considered to be suspended among the belligerents, but they will remain in effect between each belligerent and the neutral parties to the agreement, as well as among the neutral parties.

Note: The issue of the extent to which a neutral nation or an international communications consortium may continue to provide communications services to a belligerent is discussed in the law of war section of this paper.

The United States has negotiated bilateral communications only selectively, primarily because the ITC and the ITU provide a framework for handling most international communications issues. As one might expect, the need for bilateral communications agreements has arisen for the United States primarily with Canada and Mexico, because of the potential for interference in broadcast communications across our common borders. A number of bilateral communications agreements have also been negotiated between the United States and nations where U.S. military forces are stationed. There is a potential for such bilateral agreements to either restrict or facilitate information operations by U.S. military forces. The agreements concerned should be consulted when such an issue arises.

B. Domestic Communications Law.

The ITC and its predecessors obligate each Member nation to suppress acts by individuals or groups within its territory that interfere with the communications of other members. In partial satisfaction of this obligation, in 1934 Congress enacted 47 USC 502, which provides, "Any person who willfully and knowingly violates any rule, regulation, restriction, or condition . . . made or imposed by any international radio or wire communications treaty or convention, or regulations annexed thereto, to which the United States is or may hereafter become a party, shall, in addition to any other penalties provided by law, be punished, upon conviction thereof, by a fine of not more than $500 for each and every day during which such offense occurs." In October 1993, when the United States was considering broadcasting radio messages to the people of Haiti supporting the return of democracy in that nation, the Office of Legal Counsel of the Department of Justice concluded in a written opinion that 47 USC 502 would not

apply to the actions of U.S. military members acting on behalf of the President pursuant to the President's foreign affairs and Commander-in-Chief authority.

C. Assessment.

International communications law contains no direct and specific prohibition against the conduct of information operations by military forces, even in peacetime. The established practice of nations provides persuasive evidence that telecommunications treaties are regarded as suspended among belligerents during international armed conflicts. Domestic communications laws do not prohibit properly authorized military information operations. Accordingly, neither international nor domestic communications law appears to present a significant barrier to information operations by U.S. military forces.

VI. IMPLICATIONS OF OTHER TREATIES

The State Department's most recent published list of international agreements to which the United States is a party, TREATIES IN FORCE, January 1, 1998, is 495 pages long. The United States is a party to literally thousands of multilateral and bilateral international agreements. From their sheer numbers, one would think it inescapable that lurking somewhere in those agreements are provisions that will affect particular information operations activities. This section attempts only to highlight certain kinds of "typical" agreements that are likely to contain obligations relevant to the conduct of information operations.

A. Mutual Legal Assistance Agreements.

Mutual legal assistance agreements (sometimes called judicial assistance agreements) obligate each party to gather and provide evidence located in its territory concerning litigation or criminal prosecutions that occur within the jurisdiction of another party requesting such assistance. The United States is a party to several dozen mutual legal assistance agreements. Some of these agreements apply only to the management of particular litigation or to certain types of offenses such as drug trafficking and money laundering. Only a few mutual legal assistance agreements apply broadly to all law enforcement investigations and prosecutions. Such an agreement may supply the only domestic legal authority for the assisting party to investigate offenses that did not occur within its jurisdiction, and it also establishes procedures that expedite the requested assistance. To be effective in helping to suppress computer crimes and other high-tech offenses, mutual legal assistance agreements must either expressly cover such offenses or they must apply broadly to all crimes.

B. Extradition Agreements.

Extradition agreements obligate the parties in certain circumstances to deliver persons accused of crime to the other party for criminal prosecution. The United States is a party to more than a hundred bilateral extradition treaties, as well as to a 1933 Convention on Extradition to which thirteen nations in the Americas are parties. If no extradition treaty is in effect, a national government often will have neither an international obligation nor the domestic authority to deliver custody of an individual to another nation for the purpose of prosecution. It is important that the list of offenses covered by such agreements include computer intrusions and other high-tech crimes. In addition, the effectiveness

of extradition treaties is often frustrated by provisions providing that the requested nation will not extradite its own citizens, or that it will not extradite persons who commit crimes for political reasons.

NOTE: The Department of Justice has undertaken a major initiative with the "G8" countries (the other seven being the United Kingdom, Germany, Japan, Italy, Canada, France, and Russia) to modernize the domestic criminal law of each nation to adequately provide for the investigation and prosecution of computer intrusions and other high-tech crimes, and to put into place any needed improvements to international agreements providing for mutual legal assistance and extradition. In December 1997 the Attorney General hosted a meeting of the G8 Justice and Interior Ministers to discuss these issues, and a number of follow-up working group meetings have been held since that time. The United States has also participated in a project undertaken by the Council of Europe to draft an international convention on "cyber-crime." Recently the United States undertook similar efforts in the Organization of American States and at the United Nations.

C. The United Nations Convention on the Law of the Sea (UNCLOS).

Many provisions of this treaty, which is before the Senate for advice and consent, are considered to express customary international law. Some of the provisions discussed here are among them, and are therefore considered to be binding on all nations whether or not they are parties to the Convention. Others constitute new obligations. One principle widely accepted as existing customary international law is the obligation in Article 19 for a vessel exercising the right of innocent passage through a nation's territorial sea not to engage in activities "prejudicial to the peace, good order, or security of the coastal State." The prejudicial activities listed in Article 19 include:

- "any threat or use of force against the sovereignty, territorial integrity or political independence of the coastal State, or in any other manner in violation of the principles of international law embodied in the Charter of the United Nations

- any act aimed at collecting information to the prejudice of the defence or security of the coastal State

- any act of propaganda aimed at affecting the defence or security of the coastal State

- any act aimed at interfering with any systems of communication or any other facilities or installations of the coastal State"

Once UNCLOS is in general effect, these restrictions on activities aboard vessels in a coastal state's territorial sea will be of relatively minor importance because UNCLOS limits the width of the territorial sea a nation can claim to twelve nautical miles. At present, a number of nations claim territorial seas as wide as 200 miles. The twelve-mile limitation on the width of the territorial sea, together with other important guarantees UNCLOS establishes for the free operation of military aircraft and vessels, have led DoD to strongly support ratification of UNCLOS.

Article 109 of UNCLOS provides that all "States shall co-operate in the suppression of unauthorized broadcasting from the high seas" and defines unauthorized broadcasting, for the purposes of the Convention, as "the transmission of sound radio or television broadcasts from a ship or installation on the high seas intended for reception by the general public contrary to international regulations." The international regulations referred to consist primarily of the provisions of the Nairobi Convention and the ITU's Radio Regulations discussed in section V of this paper. This provision, which is generally regarded as establishing new law, was designed to deal with "pirate radio" broadcasting from vessels and platforms on the high seas, which became a significant problem for a number of countries in the 1960s. These broadcasts were primarily commercial in nature; by operating from the high seas they escaped the coastal state's regulation and taxation. Article 109 confers jurisdiction to prosecute persons engaged in pirate radio broadcasts upon the state whose flag the ship flies, the state where a broadcasting installation is registered, the state of which the broadcasting person is a citizen, any state where the transmissions can be received, and any state where authorized radio communication is suffering interference. Article 109 also provides that any state having jurisdiction to prosecute may "arrest any person or ship engaged in unauthorized broadcasting and seize the broadcasting apparatus."

Article 113 requires parties to adopt domestic criminal legislation punishing willful or culpably negligent damage to submarine cables belonging to other parties by ships or persons under their jurisdiction.

These UNCLOS provisions have the potential to affect only a narrow category of information operations, but they will have to be considered when decisions are made concerning those operations to which they do apply, at least in peacetime. UNCLOS does not expressly address how it will apply during an international armed conflict. In accordance with the general principles discussed

in the introduction to this paper, provisions determined to be incompatible with a state of armed conflict will be regarded as suspended among the belligerents. The established practice of nations leaves no doubt that Article 19's regime governing innocent passage through the territorial sea will be suspended between belligerents. The same can be said with a high degree of confidence concerning Article 113's protections for submarine cables. Article 109's provisions for the suppression of unauthorized radio broadcasting from the high seas are relatively new, with little established practice. Analytically, there would seem to be little reason to suspend its application to commercial broadcasters during an armed conflict, but it would almost certainly not apply to broadcasts from the high seas conducted by a belligerent for military or diplomatic purposes.

D. Treaties on Civil Aviation.

The United States is a party to a number of treaties concerning civil aviation, the most significant of which is the 1944 *Convention on International Civil Aviation*. This treaty, which has more than 180 parties, is often referred to as the Chicago Convention. It establishes the International Civil Aviation Organization (ICAO) and provides the basic legal framework for international civil aviation. The Convention does not directly apply to state aircraft, except for the obligation stated in Article 3(d): "The contracting States undertake, when issuing regulations for their state aircraft, that they will have due regard for the safety of navigation of civil aircraft." This concern for safe navigation by civil aircraft is also reflected in Article 28, which provides that each party will provide navigation and communications services as agreed upon through ICAO procedures, and in Article 37, which provides that the parties will comply with "international standards and recommended practices and procedures" on a variety of subjects including communications systems and air navigation aids. Over the years the ICAO Council has developed and adopted 18 technical Annexes to the Chicago Convention. Annex 10, Aeronautical Telecommunications, contains agreed provisions on aeronautical communications, navigation and surveillance. While military aircraft are not directly bound by these provisions, their obligation of "due regard" for the safety of civil aircraft generally includes an obligation not to interfere with these systems.

The United States is currently engaged in negotiations in ICAO concerning the role to be played by the Global Positioning System in future navigation systems for international civil aviation. In particular, an accommodation must be reached between ICAO's interest in ensuring that navigation services essential to the safety of international civil aviation are not interrupted during an armed

conflict, and the military imperative for the United States to be able to deny the use of GPS to a military adversary. Similar issues are certain to arise in the future in which information operations activities may create implications for the safety of international civil aviation.

The Chicago Convention is rare among multilateral treaties in that it has a specific provision concerning its application during armed conflict. Article 89 provides, "In case of war, the provisions of this Convention shall not affect the freedom of action of any of the contracting States affected, whether as belligerents or as neutrals. The same principle shall apply in the case of any contracting State which declares a state of national emergency and notifies the fact to the Council." Upon reflection, however, this provision is unlikely be applied as broadly as its language indicates. It seems clear that many provisions of the Convention are inconsistent with a state of armed conflict. The most obvious is the principle that aircraft not engaged in scheduled airline service have the right to free passage into or through the airspace of other parties. Other provisions do not appear to be incompatible with a state of armed conflict among some of the parties. For example, the existence of a state of armed conflict among certain parties should not be regarded as suspending the belligerents' obligation to carry out their combatant activities with due regard for the safety of civil aviation. Accordingly, Article 89 does not provide much help in deciding what provisions of the Convention will remain applicable during an armed conflict, and resort will still be required to the general principle that only those obligations that are incompatible with a state of armed conflict will be suspended, and only among the belligerents.

E. Treaties on Diplomatic Relations.

The United States is a party to the 1961 *Vienna Convention on Diplomatic Relations*, a widely adhered to treaty establishing obligations among its parties concerning the treatment of diplomatic personnel and premises. Among the protections afforded a party's diplomatic mission in the territory of another state are the right to inviolability of the premises of the mission (Article 2); its "archives and documents" (Article 24); the private residences, papers, correspondence, and property of diplomatic agents (Article 30); and diplomatic communications (Article 27). The treaty further provides that the mission may communicate with its government and other missions and consulates of its government by "all appropriate means, including diplomatic couriers and messages in code or cipher. However, the mission may install and use a wireless transmitter only with the consent of the receiving State." Conversely, the treaty imposes

certain duties on diplomatic missions. Article 41 provides that personnel of the mission must respect the laws and regulations of the receiving state, that they must not interfere in the receiving state's internal affairs, and that the "premises of the mission must not be used in any manner incompatible with the functions of the mission as laid down in the present Convention or by other rules of general international law or by any special agreements in force between the sending and the receiving State." Article 45 provides that the duties of the receiving state continue in force even in the case of armed conflict between the parties, or if diplomatic relations are broken off between them, even though the staff of the mission is recalled. Planning for any information operations activity that involves diplomatic premises, persons, archives, documents, or communications, either as an instrument or as a target of the operation, must take into account these international legal obligations.

F. Treaties of Friendship, Commerce, and Navigation.

The United States is a party to a large number of bilateral agreements with other nations providing reciprocal arrangements for expedited tourism, trade, and transportation between the parties. These agreements have various titles, and their provisions differ somewhat. Most such agreements do not contain specific provisions on telecommunications, and they constitute perhaps the archetype of agreements that are likely to be regarded as suspended during an armed conflict because their provisions expediting free travel and trade between the parties are incompatible with hostilities between them. Nevertheless, planning for information operations, especially in peacetime, should include a review of all significant international agreements between the United States and any other nation that may be affected.

G. Status of Forces and Stationing Agreements.

When the military forces of one nation are present in the territory of another nation with its consent, it is customary for the nations involved to execute written agreements establishing the rights and obligations of the parties concerning the visiting forces. "Stationing agreements" establish the consent of the host nation to the presence of foreign troops; set agreed limits on their numbers, equipment, and activities; and identify facilities for their use. These topics may also be dealt with in a "defense cooperation agreement" or some other agreement providing for the overall defense relationship between the parties. It is also common for the parties to execute a "status of forces" agreement (SOFA) that addresses

the allocation of various kinds of legal jurisdiction over the visiting forces. The best known of these agreements is the 1951 *Agreement Between the Parties to the North Atlantic Treaty Regarding the Status of Their Forces* (NATO SOFA). As of the end of 1998 the United States was a party to 103 SOFAs, most of which follow the general pattern of the NATO SOFA. SOFAs are necessary because of an overlap of legal jurisdiction exercised by the sending and receiving states. The receiving state has jurisdiction over persons and activities in its territory, while the sending state has both the right and the duty to exercise control over its armed forces, which is clearly a core sovereign function.

Since the full concurrent exercise of the normal jurisdiction of the sending and receiving states is impractical, status of forces agreements allocate criminal and civil court jurisdiction between the sending and receiving states, and also exempt the visiting force and its members from certain taxes, customs fees and procedures, immigration formalities, and most host nation licensing and inspection requirements. Typically, an administrative claims procedure is established for personal injuries and property damage caused by the visiting force. Another common provision requires that the visiting force and its members "respect" the host nation's laws. (This requirement will be discussed in detail in the next section of this paper). The NATO SOFA is implemented in most NATO countries by separate, more detailed, bilateral supplementary agreements, and by numerous other bilateral agreements on specific subjects including communications.

These agreements contain provisions that must be taken into account if U.S. military forces intend to engage in information operations activities while present in the territory of the receiving state.

• For example, many such agreements require that the United States notify the host nation of any significant change in the capabilities or uses of installations made available for the use of U.S. military forces. If U.S. authorities intend to conduct information operations activities from such installations, a determination must be made as to whether the relevant agreements require notifying the host nation, and perhaps even requesting its consent.

• Stationing agreements often provide that the visiting U.S. forces may install and use various communications equipment, but they often provide as well that such equipment must not interfere with host nation communications systems and that it must be used in accordance with host nation laws and regulations. If this equipment is to be used for information operations activities, it must be determined whether the contemplated activities are consistent with these obligations.

• Many stationing agreements authorize or even obligate the visiting force to use the receiving state's military and civilian communications systems. Commonly, there are obligations that any U.S. use of host nation communications systems must not cause interference and that such use must be in accordance with host nation laws and regulations. The potential for information operations to cause interference with the host nation's communications system and the possible application of host nation laws and regulations must be carefully considered, along with the fact that the conduct of offensive information operations through host nation communications systems may subject them to possible countermeasures and acts of self-defense in peacetime, and may make them legitimate military targets during an armed conflict.

Finally, if a host nation discovers that its territory and facilities have been used without its knowledge as a base for U.S. information operations of a nature that may tend to involve it against its will in a conflict or dispute, U.S. diplomatic and military relationships with the host nation are likely to suffer. The host nation could well take the view that in principle there is little difference between using an ally's territory to launch air strikes and using it to launch computer network attacks or other information operations activities. As a practical matter, computer network attacks are much more difficult to identify, trace, and attribute. However, it will not always be impossible to do so, particularly when information on such attacks is available from intelligence sources. Accordingly, decisions concerning whether to conduct information operations from the territory of an ally, and especially whether to do so without the host nation's knowledge and consent, must be made at senior policy levels.

H. U.S.-Soviet Dangerous Military Activities Agreement.

During the Cold War there were a number of incidents in which U.S. and Soviet forces followed each other closely in international waters and airspace, especially during military exercises, and sometimes physically interfered with each other's operations. Lest these incidents inadvertently escalate into an armed confrontation, on June 11, 1988 the Chairman of the Joint Chiefs of Staff and the Soviet Chief of General Staff issued a joint statement in which they declared their intent to avoid dangerous military activities in the vicinity of each other, and on July 11, 1988 the United States and the Soviet Union signed the *Agreement on the Prevention of Dangerous Military Activities*. In Section 1(d) of Article II of that agreement, the parties agreed that, when operating in proximity to personnel and equipment of the armed forces of the other party during peacetime,

they will not interfere "with command and control networks in a manner which could cause harm to personnel or damage to equipment of the armed forces of the other Party." Article I, Section 9 of the agreement defines "interference with command and control networks" as "actions that hamper, interrupt or limit the operation of the signals and information transmission means and systems providing for the control of personnel and equipment of the armed forces of a Party." The United States has recognized the Russian Federation as a successor state to the Soviet Union for purposes of this agreement. The question of succession under this agreement by other nations that were part of the Soviet Union has not been authoritatively addressed. In the rather narrow circumstances in which this agreement applies, it remains a binding international legal obligation.

VII. FOREIGN DOMESTIC LAWS

A. Introduction.

Laws enacted by other nations may have important implications for information operations activities conducted by U.S. military forces. U.S. criminal statutes addressing computer-related offenses, space activities, communications, and the protection of classified information all raise important issues for information operations. Similarly, foreign laws affecting U.S. information operations activities will most likely also consist of criminal statutes.

The sophistication of foreign domestic law on high-tech activities varies enormously, and it will continue to do so for the foreseeable future. The more technologically advanced countries tend to be more aware of the dangers created by computer hackers and other high-tech criminals, so they typically take the lead in putting legislation into place to criminalize such behavior. It is no accident that the Justice Department's international program to promote appropriate changes to mutual legal assistance treaties and other nations' domestic laws, which was discussed in Section VI of this paper, concentrated first on the G8 countries and the Council of Europe. There are other important variables at work besides technological advancement, however, including each nation's public opinion and policy positions concerning high-tech offenses, especially computer hacking. There are persons in every country, including the United States, who regard hackers as essentially harmless pranksters. There is a well-established minority view that the Internet and all the computer systems connected to it should be free game, and that defeating attempts to gain unrestricted access to these resources or imposing regulations on personal conduct on the Internet are repressive violations of the hackers' civil liberties. The argument is even advanced that hackers provide valuable assistance to the operators of the computer systems they attack, by revealing vulnerabilities that otherwise might have been exploited by sinister persons with malicious motives. On the international scene, there is the additional factor that many individuals love to see one of their fellow citizens succeed in pulling the tail of richer and more powerful nations, especially the United States.

As a result, the state of domestic laws dealing with high-tech misconduct varies enormously from country to country. This has important implications for U.S. information operations for two basic reasons: (1) The state of a nation's domestic criminal law directly impacts the assistance that the nation's public officials can provide in suppressing certain behavior by persons operating in its territory; and (2) The state of a nation's domestic criminal law may have a

significant effect on U.S. information operations conducted in the nation's territory or involving communications routed through the nation's communications systems.

B. Cooperation in Investigations and Prosecutions.

It should be readily apparent that law enforcement officials cannot prosecute an individual for conduct that is not defined as a crime in the applicable criminal law. It may be less obvious, but equally important, that in most constitutional governments law enforcement officials may not use their authority to conduct criminal investigations unless the alleged conduct constitutes a crime. If a hacker in Country X uses the Internet to gain access to a DoD computer in the Pentagon, copies sensitive data, deletes or corrupts data, and installs malicious logic, the law enforcement officials of Country X may be able to assist in investigating that conduct and may be able to extradite the offender to the United States only if one or more of the hacker's actions constitute a crime under that nation's law. Even where such legislation exists, the legal system may still not be able to provide either extradition or meaningful criminal punishment, as occurred in the case of a young Israeli hacker given a suspended sentence by an Israeli court after he participated in a series of unlawful intrusions into DoD computer systems in early 1998.

The domestic laws of some nations may also permit the use of devices specifically designed to frustrate attempts to trace Internet communications to their source. Since geography is essentially irrelevant to communications on the Internet, devices such as anonymous remailers, which strip off all information about the originator of a message, make it possible for a hacker located anywhere —even in the United States or other country—to avoid identification by routing his or her message through the anonymous remailer. In this way, weaknesses in the domestic law of one state may provide impunity to hackers everywhere. The weakest link therefore threatens law enforcement even in countries with robust and sophisticated laws. Accordingly, the imperative to bring domestic laws in every nation up to a reasonable standard should be readily apparent.

C. Effect of Foreign Domestic Law on Actions of U.S. Information Operators.

If a CINC or a JTF commander decides to order execution of a certain information operations activity by forces under his or her command who are deployed in a foreign country, the commander may have to consider whether or

not such activity is prohibited under local law. The answer may be important at two different levels of analysis: (1) The individuals who issue or execute such an order might be subject to prosecution in a host nation criminal court; and (2) The commander might feel obligated on a policy basis to refrain from issuing such an order.

If a U.S. military member issued an order or performed an act in the course of his or her official duties overseas that was a crime under host nation law, the member could very well be subject to prosecution in a host nation criminal court. Under many SOFAs, an act done in the course of a military member's official duties falls within the primary right to exercise jurisdiction of the sending state, but that rule applies only when the conduct constitutes an offense under the law of both nations, or only under U.S. law. Where the conduct alleged constitutes an offense only under the law of the host nation, the host nation has exclusive jurisdiction to prosecute. The United States has consistently taken the position that it would be intolerable for a U.S. military member to be criminally prosecuted for performing an act that is legal under applicable U.S. law, such as the Uniform Code of Military Justice (UCMJ), and which he or she was instructed to perform in the execution of an official duty. A similar issue arose recently in connection with the adoption by several NATO member nations of domestic laws making it a crime to possess anti-personnel land mines (APLs). There is no similar crime under the UCMJ. In several cases, the nations concerned have agreed to permit the U.S. forces to retain their APL stockpiles in the host nation's territory for at least some period of time. In these cases, either specific exemptions from the host nation law or agreed screening procedures for prosecutions have had to be devised to prevent prosecutions of U.S. military members for performing their official duties.

In practice, such prosecutions are most unlikely because if U.S. military authorities become aware that performance of certain information operations within the territory of a specific host nation, or that produce harmful effects within its territory, will subject military personnel to possible host nation criminal prosecution, those U.S. military authorities are most unlikely to order that such operations be conducted. The result will be that U.S. forces are unable to conduct certain activities they would otherwise conduct, or perhaps they will have to use forces elsewhere to conduct the operation. The issue thus becomes not so much one of the prospect of criminal prosecution of individual service members but rather of a limitation on the conduct of U.S. information operations.

This consideration may be not only a policy issue— it may involve binding legal obligations under a status of forces or similar agreement. For example, Article II of

the NATO SOFA provides, "It is the duty of a force and its civilian component and the members thereof as well as their dependents to respect the law of the receiving State . . . ." Similar language appears in most other SOFAs to which the United States is a party. Considerable practice has accumulated concerning the application of this obligation to "respect" the law of the receiving state. It has often been argued that the drafters could have said the visiting force must "comply" with host nation law but instead chose the less definite term "respect." The product of almost fifty years of U.S. practice in implementing SOFAs worldwide appears to be that U.S. visiting forces will generally observe the content of host nation law, but are exempt from the law's procedural requirements such as licensing, inspection, and reporting. If U.S. visiting forces seek to avoid the application of the substance of a foreign law, they generally request the host nation to grant them a specific exemption or at least to reach an understanding that a particular host nation law will not be enforced against the visiting forces.

If a contemplated information operation activity appears to conflict with host nation law, the commander concerned might choose to consult with host nation officials in an effort to resolve the issue. If time or other circumstances do not permit such consultations, the commander should carefully consider whether the activities in question should be conducted by forces outside the territory of the host nation concerned, and in a manner that would not make use of or affect that nation's communications systems. U.S. military and diplomatic authorities should be able to manage host nation legal issues if we identify them early on and carefully consider the available courses of action.

VIII. IMPLICATIONS OF ESPIONAGE LAW

A brief review of the treatment of espionage under international law may be instructive in predicting how the international community will react to information operations, especially in those mission areas in which the same technical capabilities may be used for both espionage and information operations, and also in other areas where reasonably persuasive analogies present themselves.

A. Espionage under International Law.

For our present purposes, espionage may be defined as the covert collection of intelligence about other nations. Espionage is a much narrower topic than "intelligence," much of which is collected via open source information, voluntary exchanges of information among nations, and technical means such as satellite imagery and signals intelligence that are generally accepted as legal by the international community. Roughly stated, covert methods of collecting intelligence are in most cases designed to go undetected by their target, and if detected they are designed to be unattributable to the sponsoring state. Nevertheless, discovery, attribution, and public disclosure occur fairly often.

B. Espionage during Armed Conflict.

The treatment of spies during armed conflict is well established in the law of war. A "spy" is defined in the law of war as any person who, when acting clandestinely or under false pretenses, obtains or endeavors to obtain information in the area controlled by a belligerent, with the intention of communicating it to a hostile party. A spy may be a military member or a civilian, and his or her citizenship is irrelevant. Military personnel wearing their own uniforms are not considered to be spies, even if they engage in collecting intelligence behind enemy lines. Only a person gathering intelligence while relying on protected civilian status or while wearing an enemy uniform is considered to be a spy under the law of war. Accordingly, information operations during an armed conflict will not raise any issue of spying under the law of war unless they involve the presence of individuals inside enemy-controlled territory who (1) are engaged in collecting information with the intent of communicating it to a hostile party, and (2) are wearing civilian clothing or enemy uniforms. It seems highly unlikely that the notions of "electronic presence" or "virtual presence" will ever find their way into the law of war concept of spying, for two reasons: (1) If an individual is not physically behind enemy lines he or she is not subject to capture during the

mission; and (2) There will be no issue of acting under false pretenses by abusing protected civilian status or by wearing the enemy's uniform. This will exclude most information operations activities from being considered espionage in wartime. Nevertheless, behind-the-lines missions to collect information, or to install devices that enable the collection of information, may well raise wartime spying issues.

If caught in enemy territory, a spy can be punished, after an appropriate trial, under the domestic law of the captor. The punishment can include the death penalty. The nation on whose behalf the spy was acting, however, will not be considered to have violated any international legal obligation. In addition, if individuals who may have engaged in espionage but successfully complete their missions (that is, they have returned to friendly lines) and subsequently are captured while not engaged in acts of spying, they may not be punished for their previous acts of espionage.

C. Espionage in Peacetime.

Unlike the relatively well developed treatment of espionage under the law of war, there is very little authority on the treatment of espionage under international law in peacetime. There have of course been many domestic criminal trials of peacetime spies in many countries, including the United States. By contrast, there has been almost no activity concerning peacetime espionage within the international legal system except for public complaints and the expulsion of implicated diplomats. This may be because the primary harm done to the victim nation consists of the fact that certain secret information has been compromised, which is a more abstract and indirect type of injury than dead or injured citizens, property damage, or invasions of territory. The lack of strong international legal sanctions for peacetime espionage may also constitute an implicit application of the international law doctrine called "*tu quoque*" (roughly, a nation has no standing to complain about a practice in which it itself engages). Whatever the reasons, the international legal system generally imposes no sanctions upon nations for acts of espionage except for the political costs of public denunciation, which don't seem very onerous.

The consequences for individuals caught spying, however, can be very serious. Such individuals can be tried for whatever crimes their conduct may constitute under the victim nation's domestic law, whether charged as espionage, as unlawful entry into its territory, or as a common crime such as burglary, murder, theft, bribery, obtaining unauthorized access to state secrets, or unauthorized computer intrusions. This fact accounts to some extent for the widespread

practice of assigning intelligence operatives to embassy staff positions in which they enjoy diplomatic immunity from prosecution. The only remedy for an offended host nation is to declare such persons to be persona non grata, which obligates the sending nation to remove them from the country.

The treatment of espionage under international law may help us make an educated guess as to how the international community will react to information operations activities. As discussed in Section III of this paper on the use of force, international reaction is likely to depend on the practical consequences of the activity. If lives are lost and property is destroyed as a direct consequence, the activity may very well be treated as a use of force. If the activity results only in a breach of the perceived reliability of an information system, it seems unlikely that the world community will be much exercised. In short, information operations activities are likely to be regarded much as is espionage—not a major issue unless significant practical consequences can be demonstrated.

That leaves the issue of the possible criminal liability of an information operator who may later come into the custody of a nation that has been the victim of an operation in which he or she has engaged. As with a spy, there is no evident theoretical reason why such an individual could not be prosecuted for violation of the victim nation's criminal laws. As a practical matter, however, the problems of detection and attribution of information operations activities at the national level are daunting; the likelihood of being able to prove in court that an individual engaged in a certain information operations activity—while not impossible—seems small.

Finally, it deserves mention that there is an established division of labor within the U.S. government between the intelligence community and the uniformed military forces concerning "covert action." Generally speaking, the intelligence community conducts covert action operations in peacetime that do not consist of traditional military activities. It remains to be seen how information operations activities will fall within this division of labor, especially when they are associated with military operations other than war.

D. Assessment.

Information operations activities are unlikely to fall within the definition of spying in wartime, although a limited category of activities related to information operations may so qualify. Information operations activities are more likely to fall within the category of peacetime espionage. Perhaps more importantly, the reaction of the world community to information operations that do not

generate widespread dramatic consequences is likely to be very similar to its reaction to espionage, which has traditionally been tepid.

IX. INTERNATIONAL EFFORTS TO RESTRICT "INFORMATION WARFARE"

As soon as the concept of "information warfare" began to receive broad press coverage, discussion began of negotiating a treaty that would prohibit or restrict it. A draft treaty text that circulated on the Internet in 1995 said simply, "The Parties to this Convention agree not to engage in information warfare against each other." The first public governmental initiative was a resolution tabled by Russia in the UN's First Committee in October 1998 that apparently reflected a serious effort to get the UN to focus on the subject. The Russian resolution included a call for states to report their views regarding the "advisability of elaborating international legal regimes to ban the development, production and use of particularly dangerous information weapons." The United States has taken the position that it is premature at this point to discuss negotiating an international agreement on information warfare, and that the energies of the international community would be better spent on topics of immediate concern such as helping each other to secure information systems against criminals and terrorists. So far there has been little support expressed for the Russian initiative.

There are both similarities and differences between the concept of a treaty to ban or restrict information warfare and similar efforts to prohibit "weaponization of space." One similarity is the political reality that nations lacking a significant new military capability that they perceive will be dominated by a few wealthy and powerful states have a strong incentive to agree to ban or restrict that capability. There may be an even greater incentive to prevent interference with information systems, which all nations possess to some degree, than with space systems, in which only 30 nations are currently active and which are dominated by the United States, Russia, and the European Space Agency. On the other hand, the number of nations that have any reasonable expectation of developing their own space control systems anytime soon can be counted on the fingers of one hand, while anyone with a desk-top computer and an Internet connection thereby has access both to hacker tools and to a wide variety of important information targets worldwide. Accordingly, as nations appraise where their long-term national interests lie, the calculus is quite different as between international legal restriction of the "weaponization of space" and similar control of information warfare. With space systems, most states do not expect to be either an attacker or a defender in the near future. With information systems, all states can reasonably expect to be both.

As with space control, the United States has not yet addressed fundamental policy decisions about where its long-term interests lie in connection with the

possible international legal restriction of information operations. On the one hand, there is an obvious military interest in being able to interfere with an adversary's information systems, and in being able to protect one's own. Used as an instrument of military power, information operations capabilities have the significant advantage that they minimize both collateral damage and friendly losses of personnel and equipment. Their use may avoid unwanted escalation of a dispute or conflict. They are relatively cheap and require much less in the way of forward basing, deployment, and logistical support than do traditional weapons and their delivery platforms.

On the other hand, as the nation that relies most heavily on advanced information systems, the United States has the greatest vulnerability to attack. This concern would seem to drive U.S. policymakers to consider the merits of international restrictions on information operations. If we could negotiate an effective international ban on certain types of information operations activities, might signing such a treaty best serve our long-term national interests?

The subject of information operations is of course much more complex than that of space control, since there are so many more information systems subject to attack, so many more ways of attacking them, so many more potential players, plus constant rapid changes in the relevant systems and technologies. As we have learned in our internal U.S. policy deliberations, there are great difficulties in even agreeing on definitions of what ought to be included in discussions of "information warfare" and "information operations." In these circumstances, it seems unlikely that there will be much enthusiasm anytime soon for negotiating an international agreement that would significantly restrict information operations.

X. OBSERVATIONS

There seems to be little likelihood that the international legal system will soon generate a coherent body of "information operations" law. The most useful approach to the international legal issues raised by information operations activities will continue to be to break out the separate elements and circumstances of particular planned activities and then to make an informed judgment as to how existing international legal principles are likely to apply to them. In some areas, such as the law of war, existing legal principles can be applied with considerable confidence. In other areas, such the application of use of force principles to adopting an "active defense," it is much less clear where the international community will come out, and the result will probably depend more on the perceived equities of the situations in which the issues first arise in practice than on legal analysis. The growth of international law in these areas will be greatly influenced by what decision-makers say and do at those critical moments.

There seems to be no particularly good reason for the United States to support negotiations for new treaty obligations in most of the areas of international law that are directly relevant to information operations. The principal exception is international criminal cooperation, where current U.S. efforts to improve mutual legal assistance and extradition agreements should continue to receive strong emphasis. Another idea that might prove fruitful is to negotiate a treaty to suppress "information terrorism," but there seems to be little concept at present how such an agreement would operate or how it would reliably contribute value to information assurance and critical infrastructure protection.

There are no "show-stoppers" in international law for information operations as now contemplated in the Department of Defense. There are, however, many areas where legal uncertainties create significant risks, most of which can be considerably reduced by prudent planning. Since so many of these potential issues are relatively novel, and since the actions taken and public positions announced by nations will strongly influence the development of international law in this area, the involvement of high-level policy officials in planning and executing information operations is much more important at present than is the case with more traditional military activities.

XI. NOTES FOR FURTHER RESEARCH

I. INTRODUCTION

There are many textbooks and casebooks that provide general surveys of international law. Some of the more recent of these are:

Ian Brownlie, PRINCIPLES OF PUBLIC INTERNATIONAL LAW (4th ed. 1990)

Barry E. Carter & Phillip R. Trimble, INTERNATIONAL LAW (1991)

Stephen Dycus, Arthur L. Berney & William C. Banks, NATIONAL SECURITY LAW (2nd ed. 1997)

Louis Henkin, Richard C. Pugh, Oscar Schachter & Hans Smit, INTERNATIONAL LAW: CASES AND MATERIALS (3rd ed. 1993)

John Norton Moore, Frederick S. Tipson & Robert F. Turner, NATIONAL SECURITY LAW (1990)

Malcolm N. Shaw, INTERNATIONAL LAW (4th ed. 1997)

Useful collections of materials on U.S. practice concerning international legal issues include:

RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES (1986)

Hackworth, DIGEST OF INTERNATIONAL LAW, 7 Volumes (1940–1943)

Whiteman, DIGEST OF INTERNATIONAL LAW, 15 Volumes (1963–1973)

Contemporary Practice of the United States Relating to International Law, a regular feature in THE AMERICAN JOURNAL OF INTERNATIONAL LAW; and INTERNATIONAL LEGAL MATERIALS; both of which are publications of the American Society of International Law. (Web site at www.asil.org)

The United Nations Charter has been widely reprinted. It can also be found at 59 Stat. 1031; TS 993; 3 Bevans 1153.

The quotation from Chief Justice Holmes appears in THE COMMON LAW (1881).

Discussions of the effect of war on treaty obligations can be found in the following:

RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES, Vol. I 218-222 (1986)

Whiteman, DIGEST OF INTERNATIONAL LAW, Vol. 14 490-510 (1970)

Lester B. Orfield & Edward D. Re, CASES AND MATERIALS ON INTERNATIONAL LAW 68-78 (1955)

Ian Brownlie, PRINCIPLES OF PUBLIC INTERNATIONAL LAW 616-617 (1990)

There have been relatively few books and articles published to date addressing international legal issues in information operations. Among these are:

M.E. Bowman, *Is International Law Ready for the Information Age?* 19 FORDHAM INT'L. L. J. 1935 (1996)

Lawrence T. Greenberg, Seymour E. Goodman & Kevin J. Soo Hoo, OLD LAW FOR A NEW WORLD? THE APPLICABILITY OF INTERNATIONAL LAW TO INFORMATION WARFARE (1997). Published as a monograph by the Institute for International Studies, Stanford University, and in revised form in 1998 by the Institute for National Strategic Studies, National Defense University, the latter under the title INFORMATION WARFARE AND INTERNATIONAL LAW

Sean P. Kanuck, *Information Warfare: New Challenges for Public International Law*, HARV. INT'L. L. J. 272 (Winter 1996)

Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. INT'L. L. 885 (1999)

Roger D. Scott, *Legal Aspects of Information Warfare: Military Disruption of Telecommunications*, 45 NAVAL L. REV. 57 (1998)

W Gary Sharp, Sr., CYBERSPACE AND THE USE OF FORCE (1999)

II. THE LAW OF WAR

The views of the U.S. military services on law of war matters are summarized in military publications such as the U.S. Army's Field Manual 27-10, LAW OF LAND WARFARE (1956); Air Force Pamphlet 110-31, INTERNATIONAL LAW—THE CONDUCT OF ARMED CONFLICT AND AIR OPERATIONS (1976); and Naval Warfare Publication 1-14M, THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS (1995). In addition, Burrus Carnahan has compiled a comprehensive research report on U.S. practice relating to customary law of war principles for use by the International Committee of the Red Cross in its ongoing study of worldwide practice relating to the customary law of war. Unfortunately, neither Mr. Carnahan's study nor the ICRC study is yet available in published form. Finally, the DoD Law of War Working Group chartered by DoD Directive 5100.77, "The DoD Law of War Program," December 1998, has for several years been composing a DOD LAW OF WAR MANUAL. When it is published it will constitute the most current and comprehensive statement of the Department's views on law of war matters.

There are also a large number of books and articles commenting on law of war issues, which are far too numerous to list here.

Information on law of war issues that arose during the 1991 Persian Gulf conflict can be found in Appendix O, "The Role of the Law of War," in the DoD report to the Congress on the conduct of the Persian Gulf War, which is reprinted in 31 INTERNATIONAL LEGAL MATERIALS (1992).

The 1907 Hague Convention Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land is published at 36 Stat. 2310, T.S. 540.

EUTELSAT's actions during NATO's 1999 bombing campaign in Kosovo are described in Steven Pearlstein, *Serb TV Gets Notice It's Canceled,* WASHINGTON POST, May 23, 1999.

The significance of the "peaceful purpose" principle to the new INMARSAT is discussed in a April 15, 1999 letter from the COMSAT Corporation's Office of Legal Counsel to Mobile Datacom Corporation.

III. USE OF FORCE

Indicators that the United States considers the 1970 Declaration on Friendly Relations to constitute an authoritative statement of international law include "Statement by Richard H. Ginger, U.S. Alternate Representative to the U.N. General Assembly," DEPT OF STATE BULLETIN 623 (November 1970) and "Statement by Robert Rosenstock, U.S. Representative to the Sixth Committee (Legal)" in Boyd, DIGEST OF UNITED STATES PRACTICE IN INTERNATIONAL LAW 1977.

The statement by the U.S. delegation to the effect that the 1974 "Definition of Aggression" Resolution does not constitute an authoritative statement of international law is reported at DEPT OF STATE BULLETIN 155 (February 1975).

The 1994 JCS Standing Rules of Engagement for U.S. Forces are published as Chairman of the Joint Chiefs of Staff Instruction 3121.01. Some portions of this publication are classified, but its discussion of the use of force in self-defense against "hostile intent" is unclassified. At this writing in November 1999 a revised version of the SROE was nearing publication. No change is expected in the principle cited here.

The *Caroline* incident is reported in many texts, one of the most detailed of which is 2 Moore, A DIGEST OF INTERNATIONAL LAW 409–414 (1906).

For an authoritative U.S. statement of the legal basis for the 1986 bombing of Libya, see "President's Address to the Nation," April 14, 1986, reprinted in "U.S. Exercises Right of Self-Defense against Libyan Terrorism," DEPT OF STATE BULLETIN 1 (June 1986).

A collection of authoritative U.S. statements of the legal basis for the August 1998 cruise missile attacks on terrorist camps in Afghanistan and a chemical plant in Sudan, as well as other relevant materials, can be found at 93 AM. J. OF INT'L LAW 161-170 (1999).

The *Corfu Channel* case is published at 1949 I.C.J. 4.

The *Chorzow Factory* decision is published at 1928 P.C.I.J. (ser. A) No. 17.

The U.S. French air traffic tribunal decision is published as *Case Concerning Air Services Agreement Between France and the United States*, Arbitral Award of December 9, 1978, UNRIAA 417, 443-446.

The International Court of Justice decision in *Nicaragua v. United States of America* is published at 1986 I.C.J. 14.

A statement by the State Department's Legal Advisor concerning the legal basis for U.S. attacks on North Vietnamese forces in Cambodia is published at 62 DEPT OF STATE BULLETIN 765 (1970).

Timothy Guiden has published an extensive article on U.S. operations in Cambodia: *Defending America's Cambodian Incursion,* ARIZ. J. INTL & COMP L. 217 (1994).

IV: SPACE LAW

The treaties cited in this section are published as follows:

Outer Space Treaty, 18 UST 2410; TIAS 6347; 610 UNTS 205

Rescue and Return Agreement, 19 UST 7570; TIAS 6599; 672 UNTS 119

Liability Convention, 24 UST 2389; TIAS 7762; 961 UNTS 187

Registration Convention, 28 UST 695; TIAS 8480; 1023 UNTS 15

Moon Agreement, U.N. Doc. A/RES/34, 68 (1979)

Environmental Modification Convention, 31 UST 333; TIAS 9614; 1108 UNTS 151

Limited Test Ban Treaty, 14 UST 1313; TIAS 5433; 480 UNTS 13

ABM Treaty, 23 UST; TIAS 7503; 944 UNTS 13

V. COMMUNICATIONS LAW

At this writing in November 1999 the International Telecommunications Convention of 1982 has not yet been published in the UST series, which is the State

Department's official compilation of international agreements to which the United States is a party. This agreement is probably most accessible in S. TREATY DOC. No. 99-6. The United States is also a party to the Constitution and Convention of the International Telecommunications Union of 1992, which replaces the 1982 agreement as between parties to the 1992 agreement.

The two memorandum opinions of the Justice Department's Office of Legal Counsel concerning broadcasting into Haiti are entitled "Applicability of 47 USC Section 502 to Certain Broadcast Activities" (October 15, 1993) and "Memorandum for the Deputy Attorney General" (July 8, 1994).

The 1884 Convention for Protection of Submarine Cables and associated documents are published at 24 Stat.989, 25 Stat. 1424, TS 380, 1 Bevans 89, 112, 114.

The major bilateral and regional communications agreements to which the United States is a party are listed in TREATIES IN FORCE. Many others are unpublished.

VI. OTHER TREATIES

Citations to the agreements described in this section can generally be found in the current TREATIES IN FORCE. Pursuant to DoD Directive 5530.3, "International Agreements," June 11, 1987, a DoD repository and index of unpublished international agreements relating to military operations and installations is maintained in the Office of the Deputy General Counsel (International Affairs).

VII. FOREIGN DOMESTIC LAWS

None.

VIII. IMPLICATIONS OF ESPIONAGE LAW

None.

IX. INTERNATIONAL EFFORTS TO RESTRICT "INFORMATION WARFARE"

The effort by Russia in the fall of 1998 to get the United Nations to take a firm stand on restricting information warfare produced only a resolution passed by the

General Assembly on 4 January 1999 entitled "Developments in the field of information and telecommunications in the context of international security," which "calls upon Member States to promote at multilateral levels the consideration of existing and potential threats in the field of information security," "invites all Member States to inform the Secretary-General of their views and assessments" on information security issues, "requests the Secretary-General to submit a report to the General Assembly" at its next session, and "decides to include information security in the provisional agenda for its next session." U.N. Doc. A/RES/53/70 (1999). In August 1999 the Secretary General submitted his report to the General Assembly. It contained the statements submitted by ten Member States (Australia, Belarus, Brunei, Cuba, Oman, Qatar, Russia, Saudi Arabia, the United Kingdom, and the United States). The Russian statement referred to "information weapons . . . the use of which . . . can have devastating consequences, comparable to the effect of weapons of mass destruction." It proposed that the General Assembly "adopt resolutions on the question of information security with a view to reducing the threat of the use of information for terrorist, criminal or military purposes," which would help generate "international principles (e.g., a regime, a code of conduct for States) with a view to strengthening international information security," and ultimately to a "multilateral international legal instrument." Aside from Russia, only Belarus and Cuba expressed support for the development of international legal principles in the field of information security other than cooperation in suppressing computer crime and terrorism. The United States and the United Kingdom stated that it was premature to attempt to formulate overarching principles pertaining to information security, and that, for the present, international efforts should focus on measures to combat computer crime and terrorism. The Secretary General ventured no opinion on the subject. U.N. DOC. A/54/213, 10 August 1999.

X. OBSERVATIONS

None

Contributors

Lieutenant Colonel Douglas S. Anderson, US Air Force, is presently Senior Military Advisor, Strategic Arms Control Policy, Office of the Assistant Secretary of Defense for International Security Policy. He has served as the Chief of the Foreign Relations Branch, International and Operations Law Division, Office of the Judge Advocate General, Headquarters Air Force. In that capacity, his responsibilities included advising the Air Staff and legal offices worldwide on international, aviation, and space law. He is a graduate of the University of Oregon, B.S., 1978; Pepperdine University School of Law, 1981; and the Army Judge Advocate General School, LL.M. in Military Law (International Law specialty), 1995.

Dr. Roger W. Barnett is Professor Emeritus at the Naval War College, where, until his retirement in September 2001, he held the Jerry O. Tuttle Military Chair of Information Operations. He retired from the Navy as a Captain in 1984, having served in cruisers, destroyers, and headquarters staffs in Washington DC. Dr. Barnett was a member of the US delegation to strategic arms talks with the Soviet Union in 1970–71. From 1983 to 1984 he led the Strategic Concepts Branch of the Office of the Chief of Naval Operations. Dr. Barnett earned a B.A. from Brown University, and M.A. and Ph.D. degrees from the University of Southern California.

Vice Admiral Arthur K. Cebrowski, US Navy (Ret.), commanded Fighter Squadron 41 and Carrier Air Wing 8, both embarked in USS NIMITZ (CVN 68). He later commanded the assault ship USS GUAM (LPH 9) and, during Operations DESERT SHIELD and DESERT STORM, the aircraft carrier USS MIDWAY (CV 41). Following promotion to flag rank, he became Commander, Carrier Group 6 and Commander, USS America Battle Group. In addition to combat deployments to Vietnam and the Persian Gulf, he deployed in support of United Nations operations in Iraq, Somalia, and Bosnia. He served with the US Air Force; the staff of Commander in Chief, Atlantic Fleet; the staff of the Chief of Naval Operations, on four occasions; with the Joint Staff (as J6); and as Director, Navy Space, Information Warfare, and Command and Control (N6). Vice Admiral Cebrowski became the forty-seventh President of the Naval War College in July 1998. Following retirement, in November 2001, Vice Admiral Cebrowski was appointed as Director of the Office of Force Transformation within the Office of the Secretary of Defense.

Mr. David M. Crane became the Deputy Assistant Inspector General of the Department of Defense for Intelligence Review in May of 1997. In January of 1998 that office became a separate organization and Mr. Crane was designated as the Director, Office of Intelligence Review. A member of the Senior Executive Service, Mr. Crane's duties include, among others, advising the Office of the Inspector General on intelligence policy and programs and in that capacity reviews the management, policies, procedures, and functions of the intelligence community within the Department of Defense. Prior to his appointment to his current position, Mr. Crane was the Assistant General Counsel, Defense Intelligence Agency. In government for over 28 years, Mr. Crane served the majority of that time as an infantry officer and judge advocate in the United States Army, serving in airborne, special operations, special forces, and intelligence units throughout the world.

Mr. Crane graduated *summa cum laude* in History with a Bachelor of General Studies degree from Ohio University in 1972. He received his Master of Arts degree in International Affairs also from Ohio University in 1973. In 1980, Mr. Crane received his Doctor of Law (J.D.) degree from Syracuse University. He is currently completing his Doctor of Juridical Science (S.J.D.) degree at the University of Virginia School of Law.

Professor Anthony D'Amato is the Judd and Mary Morris Leighton Professor of Law at Northwestern University School of Law, a position he has held since 1990. An active litigator in international human rights, he was the first American lawyer to argue (and win) a case before the European Court of Human Rights in Strasbourg. Professor D'Amato also litigated the only court of appeals victory against the government in a military service case during the Vietnam era. He is the author of over 20 books and over 110 articles, including Analytic Jurisprudence Anthology and Introduction to Law and Legal Thinking.

Professor Yoram Dinstein is currently a Humbolt Fellow at the Max Planck Institute of Foreign, Comparative and International Law in Heidelberg, Germany. He was the Charles H. Stockton Professor of International Law at the US Naval War College (1999–2000). Previously, he served as Professor of International Law, Yanowicz Professor of Human Rights, President (1991–98), Rector (1980–85), and Dean of the Faculty of Law (1978–80) at Tel Aviv University. Professor Dinstein started his career in Israel's Foreign Service and served as Consul of Israel in New York and a member of Israel's Permanent Mission to the United Nations (1966–70). He is a member of the Institute of International Law and the Council of the International Institute of Humanitarian Law in San Remo. He was among the group of international lawyers and naval experts that produced the San Remo Manual on International Law Applicable

to Armed Conflicts at Sea. Formerly, he served as Chairman of the Israel national branch of Amnesty International and was also a member of the Executive Council of the American Society of International Law. Professor Dinstein is the editor of the Israel Yearbook of Human Rights and has written extensively on subjects relating to international law, human rights, and the law of armed conflict.

Colonel Christopher R. Dooley, US Air Force, is presently Chief of the International Law Division, Office of the Staff Judge Advocate, Headquarters United States Air Forces in Europe (USAFE), Ramstein Air Base, Germany. He previously served as the Chief of the Operations Law Branch, International and Operations Law Division, Office of the Judge Advocate General, Headquarters Air Force, Pentagon. In that position he was responsible for advising the Air Staff and legal offices worldwide on international, operations, aviation, and space law. He is a graduate of Bob Jones University, B.A., 1979, and the University of South Carolina, J.D., 1982.

Ms. Louise Doswald-Beck is Secretary-General of the International Commission of Jurists. She previously served as the Head of the Legal Division of the International Committee of the Red Cross. A former lecturer in international law at the University of London, she has published widely on many humanitarian law and international law issues. Ms. Doswald-Beck was among a group of international lawyers and naval experts that produced the San Remo Manual on International Law Applicable to Armed Conflicts at Sea, for which she served as editor.

Vice Admiral James H. Doyle, Jr., US Navy (Ret.), completed thirty-seven years of service including assignments as Deputy Chief of Naval Operations (Surface Warfare); Commander Third Fleet; Commander Cruiser-Destroyer Group Twelve; Commander Attack Carrier Striking Group Two; Chief, International Negotiations Division, Joint Staff; member of the US delegation at the Third United Nations Conference on the Law of the Sea; and Commanding Officer of four surface ships, including the first nuclear-powered destroyer, USS BAINBRIDGE. He is a graduate of the National Law Center, George Washington University, where he taught International Law of the Sea from 1982–89. Vice Admiral Doyle was among the group of international lawyers and naval experts that produced the San Remo Manual on International Law Applicable to Armed Conflicts at Sea. He is a member of the Naval War College Advisory Board on Operational Law and Vice Chairman of the Strike, Land Attack and Air Defense Committee of the National Defense Industrial Association.

Colonel Charles J. Dunlap, Jr., US Air Force, is the Staff Judge Advocate, Air Education and Training Command, Randolph Air Force Base, Texas. He holds a B.A. from St. Joseph's University, a J.D. from Villanova University, an Air War College degree, and is a Distinguished Graduate of the National War College.

Colonel Dunlap's assignments include duties as a trial lawyer, staff officer, instructor, and military judge. He has served overseas in England and Korea, and has deployed to Africa during operations in Somalia (Operation PROVIDE RELIEF/RESTORE HOPE 1992-93), and to the Middle East (Operation VIGILANT WARRIOR, 1994; Operation DESERT FOX, 1998). In 1992, the Judge Advocates Association named Colonel Dunlap the US Air Force's "Outstanding Career Armed Forces Attorney," and in 1996 he received the Thomas P. Keenan, Jr. Award for contributions to international and operations law. In 2001 he was honored as the winner of the first-ever Special Operations' Command Essay Contest. Colonel Dunlap speaks widely on national security issues and is the author of many essays. He has appeared on a number of television programs and served as a consultant for the HBO movie *The Enemy Within* and for a recent BBC production about the future of war.

Colonel Phillip A. Johnson, US Air Force (Ret.), served thirty years as an Air Force judge advocate and is currently a consultant supporting the Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence. His military assignments included service in Vietnam and Germany; service as base Staff Judge Advocate at Travis Air Force Base, California; a faculty appointment in the Department of Law at the US Air Force Academy; service as the Staff Judge Advocate of Air Force Space Command and Legal Advisor of US Space Command and North American Aerospace Defense Command; a tour as a senior appellate judge of the Air Force Court of Criminal Appeals; service as Chief of the International and Operations Law Division in the Office of the Judge Advocate General; and service as Associate Deputy General Counsel in the International Affairs Division of the Office of the General Counsel, Department of Defense.

Lieutenant Commander James C. Kraska, JAGC, US Navy, is currently the head of the Center for Operational Law & Training in the Office of the Navy Judge Advocate General (International and Operational Law Division). Prior to this assignment, he served as Staff Judge Advocate for Commander, Amphibious Group ONE in Okinawa, Japan and has served as the Legal Advisor for US Commander in Chief Pacific Command's Joint Interagency Task Force West. Lieutenant Commander Kraska earned degrees from Indiana University School of Law; School of Economics and Politics, Claremont

University in Claremont, California; and Mississippi State University. He is the author of more than ten articles on foreign affairs and international law.

Professor Daniel T. Kuehl teaches military strategy and national security policy in the Information Resources Management College at National Defense University in Washington, DC. He is the Director of the Information Strategies Concentration Program, a specialized curriculum for selected students at the National War College and Industrial College of the Armed Forces, in which he teaches on national security in the information age, the law of war, the strategic use of the Internet, and information warfare and strategy. He retired as a Lieutenant Colonel in 1994 after nearly 22 years active duty in the US Air Force. In his final assignment at the Air Staff he was part of the "Checkmate" planning team that in August 1990 developed the "Instant Thunder" plan for a strategic air campaign against Iraq, after which he served as chief of the Air Staff division which supported the Secretary of the Air Force's landmark Gulf War Air Power Survey (GWAPS). Professor Kuehl has edited or written several books and numerous publications, and serves on the editorial board of the *Joint Force Quarterly*. He is on the faculty of the American Military University. He earned a Ph.D. in History from Duke University.

Mr. Gordon N. Lederman is a member of the Arnold & Porter law firm's public policy/legislative group, and practices in the fields of government relations (focusing on national security affairs, especially cybersecurity and bioterrorism) and international litigation. He is a *magna cum laude* graduate of both Harvard College and Harvard Law School and clerked for the Honorable Robert E. Cowen of the Third Circuit Court of Appeals. Mr. Lederman's book on the Defense Department's organizational politics, entitled Reorganizing the Joint Chiefs of Staff: The Goldwater-Nichols Act of 1986, was published in 1999. Former Senator Sam Nunn wrote the book's foreword. He also is the co-author of a May 2001 Center for Strategic and International Studies (CSIS) report entitled Combating Chemical, Biological, Radiological, and Nuclear Terrorism: A Comprehensive Strategy. Finally, Mr. Lederman is the founder and co-chair of the Council on Foreign Relations' study group on new national security threats.

Lieutenant Colonel Perry G. Luzwick, US Air Force (Ret.), is Director, Information Assurance Architectures at Northrop Grumman Information Technology, a Northrop Grumman company. He is a senior consultant throughout the corporation for Information Operations (IO), Information Assurance (IA), Information Superiority, Critical Infrastructure Protection, and Knowledge Management (KM) from conceptualization through design and implementation. In his last assignment with the US Air Force, he served as

Military Assistant to the Principal Deputy Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)). Lieutenant Colonel Luzwick earned an M.A. and was a Distinguished Graduate, in Computer Resources Management from Webster University; an MBA from the University of North Dakota; and a B.S., Psychology from Loyola University of Chicago. He was an Adjunct Faculty member for the University of Maryland, the City Colleges of Chicago, and NSA's National Cryptologic School. He is a member of ShockwaveWriters.com and a 1998 member of the International Who's Who of Information Technology.

Professor John F. Murphy is Professor of Law at Villanova University. In addition to teaching, his career has included a year in India on a Ford Foundation Fellowship, private practice in New York and Washington, DC, and service in the Office of the Assistant Legal Adviser for United Nations Affairs, US Department of State. He was previously on the law faculty at the University of Kansas, and has been a visiting professor at Cornell University and Georgetown University. From 1980–1981 he was the Charles H. Stockton Professor of International Law at the US Naval War College.

Professor Murphy is the author or editor of several books and monographs, and is also the author of numerous articles, comments, and reviews on international law and relations. Twice the recipient of the Ethel and Raymond F. Rice Prize for faculty scholarship at the University of Kansas Law School, as well as a recipient of the Certificate of Merit from the American Society of International Law in 1992, Professor Murphy has served as consultant to the US Departments of State and Justice, the ABA Standing Committee on Law and National Security, and the United Nations Crime Bureau, and has testified before Congress on several occasions. He is currently the American Bar Association's Alternate Observer at the US Mission to the United Nations.

Lieutenant Commander Brian T. O'Donnell, JAGC, US Navy, is the Legal Advisor for International and Operational Law at the Navy Warfare Development Command (NWDC), the Navy's center for integrating advanced concepts, doctrine and emerging technology into the US fleet. Prior to his tour at NWDC, he has served as a military professor of International Law at the Naval War College and Deputy Fleet Judge Advocate, Commander, US SEVENTH Fleet, forward deployed in Yokosuka, Japan on board USS BLUE RIDGE (LCC 19). He served as the Navy Senior Prosecutor in Yokosuka, Japan, as the Staff Judge Advocate for Naval Air Station North Island (NASNI), Coronado, California, and as Deputy Staff Judge Advocate on board USS ABRAHAM LINCOLN (CVN 72). Lieutenant Commander O'Donnell is a graduate of the University of Richmond School of Law and Virginia Polytechnic Institute and

State University. He previously served as an editor of the Report of the 15th International Seapower Symposium.

Rear Admiral Horace B. Robertson, Jr., JAGC, US Navy (Ret.), served 31 years on active duty with the US Navy, first as a general line officer (surface warfare) and later as a law specialist and judge advocate. Included among his assignments were tours as Commanding Officer of an amphibious landing ship, Special Counsel to the Secretary of the Navy, Special Counsel to the Chief of Naval Operations, and Judge Advocate General of the Navy. Following retirement, Rear Admiral Robertson was appointed Professor of Law at Duke University School of Law, where he assumed Emeritus status in 1990. He is the editor of The Law of Naval Operations, Volume 64 of the Naval War College's International Law Studies (the "Blue Book") series. He was among a group of academics and naval experts that worked together to produce the San Remo Manual on International Law Applicable to Armed Conflicts at Sea. During 1991–92, he served as the Charles H. Stockton Professor of International Law at the US Naval War College.

Professor Michael Schmitt is Director, Executive Program in International and Security Affairs and Professor of International Law, George C. Marshall European Center for Security Studies in Garmisch-Partenkirchen, Germany. He has previously served on the faculties of the US Air Force Academy and US Naval War College, and currently is an adjunct faculty member of both the NATO (SHAPE) School at Oberammergau, Germany, and the International Institute of Humanitarian Law in San Remo, Italy. Professor Schmitt is a retired Air Force judge advocate and former Visiting Scholar at Yale Law School. He is the contributing editor of numerous books, including three in the Naval War College's "Blue Book" series, and has authored many articles on international law and military operations.

Professor Walter Gary Sharp, Sr., is a Principal Information Security Engineer at The MITRE Corporation, McLean, Virginia; an Adjunct Professor of Law at Georgetown University Law Center; the Editor-in-Chief of the National Security Law Report, ABA Standing Committee on Law & National Security; a member of the Advisory Committee to the ABA Standing Committee on Law & National Security; a member of the Board of Advisors for Three Oaks Capital, LLC; and a member of the Executive Advisory Board for the Maryland Journal of International Law and Trade. He has authored three books on international and national security law. He retired in December 1997 as a US Marine Corps Lieutenant Colonel with prior enlisted service and 25 years of active duty. His assignments included Deputy Legal Counsel to the Chairman of the Joint Chiefs of Staff and Commanding Officer, Headquarters Battery, 2nd Battalion,

11th Marines, 1st Marine Division (REIN) FMF, Camp Pendleton, California. Professor Sharp holds an LL.M. from the US Army's Judge Advocate General's School; an LL.M. from Georgetown University Law Center; a J.D. from Texas Tech School of Law; and a B.S. from the United States Naval Academy.

Mr. Daniel B. Silver is Counsel to the international law firm of Cleary, Gottlieb, Steen & Hamilton, from which he retired as a partner in January 1997, having served in the firm's Washington and Brussels offices. From March 1978 to May 1979, he was General Counsel of the National Security Agency and from May 1979 to May 1981 General Counsel of the Central Intelligence Agency. In 1998 he served as General Counsel of the House Select Committee on Technology Transfers to the People's Republic of China (the "Cox Committee"). He has served as a Distinguished Visitor from Practice and Adjunct Professor at the Georgetown University Law Center, where he has taught intelligence law and European Communities law, among other subjects.

Mr. Jeffrey H. Smith is a partner in the law firm of Arnold & Porter and heads the firm's Public Policy and Legislative Practice Group. In October 1996, he rejoined the firm after serving as General Counsel of the Central Intelligence Agency from May 1995 to September 1996. In May of 1993, Secretary of Defense Perry appointed Mr. Smith to the Congressionally-mandated Commission to Review the Roles and Missions of the Armed Services. Previously, he chaired the Joint Security Commission, established by Secretary of Defense Les Aspin and Director of Central Intelligence James Woolsey, to review security policy and practices in the defense and intelligence communities. In late 1992 and early 1993, he served as the Chief of the Clinton Transition Team at the Department of Defense.

Prior to joining Arnold & Porter, Mr. Smith served as the General Counsel of the Senate Armed Services Committee. Prior to working for the Senate, he was an assistant Legal Adviser at the State Department. Earlier, as an Army Judge Advocate General Officer, he served as the Pentagon's lawyer for the Panama Canal negotiations.

Mr. Smith is a 1966 graduate of the US Military Academy and a 1971 graduate of the University of Michigan Law School. He is also a member of the boards of trustees of Aerospace Corporation and the Henry L. Stimson Center, and serves as General Counsel of the Goldwater Foundation. He has lectured and written on national security and international law, and is a member of the Council on Foreign Relations.

Colonel James P. Terry, US Marine Corps (Ret.), is currently serving as the Deputy Assistant Secretary (Global) in the Bureau of legislative Affairs of the US Department of State. Immediately prior to his retirement from the US

Marine Corps he served as Legal Counsel to the Chairman of the Joint Chiefs of Staff from June 1992 through June 1995. During this tenure, he provided legal guidance on military operations in Iraq, Somalia, Rwanda, and Haiti, and legal advice on support initiatives in Russia and other States within the former Soviet Union. After retirement, Colonel Terry was appointed to a senior position within the Department of the Interior in Washington. A graduate of the University of Virginia, Colonel Terry received the Doctor of Juridical Science (S.J.D) Degree in International Law from The George Washington University.

Mr. David Tubbs is the Executive Vice President, Chief Technology Officer, and a cofounder of eRiskSecurity, Inc. eRiskSecurity is a California corporation with the mission of securing information systems from all avenues of attack through a systems-level review of vulnerabilities and threats, including hardware, software, physical, and social engineering attacks. He received five Department of Defense awards for research project excellence while employed with McDonnell Douglas. Mr. Tubbs has a B.A. in Physics and Mathematics (*magna cum laude*) from Point Loma College in San Diego and has completed coursework in such areas as Mathematical Methods of Physics, Microprocessor Design, and Optical System Design. He has designed and taught courses entitled Fiber Optics—Theory and Applications. Additionally, Mr. Tubbs is a member of the International Computer Security Association (ICSA) and the High Technology Crime Investigators Association (HTCIA).

Professor George K. Walker is Professor of Law, Wake Forest University School of Law. He was the Charles H. Stockton Professor of International Law at the US Naval War College from 1992–93. Professor Walker retired as a Captain in the US Naval Reserve after serving aboard destroyers, qualifying as a Surface Warfare Officer, and duty as Commanding Officer of six Naval Reserve units. He was a Woodrow Wilson fellow at Duke University and received a Sterling Fellowship while holding a research position at Yale Law School. Professor Walker has edited or written ten books and over forty book chapters, law journals, and continuing education publications, as well as several state statutes. Professor Walker was among the group of international lawyers and naval experts that produced the San Remo Manual on International Law Applicable to Armed Conflicts at Sea. He has served as a vice president of the North Carolina Bar Association and on the Executive Council of the American Society of International Law. Professor Walker is also a member of the American Law Institute.

Professor Ruth G. Wedgwood is a Professor of Law at Yale Law School, and is also Senior Fellow and Director of the Project on International Organizations and Law at the Council in Foreign Relations in New York City. Currently on a leave of absence from Yale Law School, she is serving as the Edward B.

Burling Professor of International Law at the Johns Hopkins University Nitze School of Advanced International Studies in Washington, DC. Professor Wedgwood is a member of the Secretary of State's Advisory Committee on International Law, and is Vice President of the International Law Association (American branch). During 1998–99, she served as the Charles H. Stockton Professor of International Law at the US Naval War College. She has written and lectured widely on Security Council politics, United Nations peacekeeping, war crimes, and UN reform. She is a former law clerk to judge Henry Friendly of the US Court of Appeals for the Second Circuit and Justice Harry Blackmun of the U.S. Supreme Court, and Executive Editor of the Yale Law Journal. Professor Wedgwood served as *amicus curiae* in the case of Prosecutor v. Blaskic at the International Criminal Tribunal for the former Yugoslavia.

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

Y