UNITED STATES v. DANIEL DAVID RIGMAIDEN
CR08-814-PHX-DGC
EXHIBIT INDEX
SECOND SUBMISSION OF CONSOLIDATED EXHIBITS
RELATING TO DISCOVERY AND SUPPRESSION ISSUES

EXHIBIT 001: Letter from AUSA Frederick A. Battista to Daniel Rigmaiden RE: the prosecution claiming that the defendant never referred to himself as a "self-described Hacker" and that the statement in the U.S. Attorney's Office, District of Arizona, *press release No. 2010-060 (Rigmaiden, et al.)* was "inartfully drafted."; (Letter date: July 21, 2010);

[Highlighting added by the defendant.]

EXHIBIT 002: United States Patent and Trademark Office, Trademark Reg. No. 2,762,468 [StingRay] (registered Sep. 9, 2003), **Harris StingRay Product Pictures**, *all associated trademark documents available via search at* http://tmportal.uspto.gov/external/portal/tow (last accessed: Mar. 11, 2011), p. 9 & 15 of 88 page compilation;

EXHIBIT 003: Miami, FL, USA – Legislative Files, **Harris StingRay Product Datasheet**, *available at* http://egov.ci.miami.fl.us/Legistarweb/Attachments/34769.pdf (last accessed: Mar. 9, 2011), p. 1;

EXHIBIT 004: United States Patent and Trademark Office, Trademark Reg. No. 2,762,468 [StingRay] (registered Sep. 9, 2003), **Harris StingRay Product Datasheet**, *all associated trademark documents available via search at* http://tmportal.uspto.gov/external/portal/tow (last accessed: Mar. 11, 2011), p. 60-61 of 88 page compilation;

EXHIBIT 005: United States Patent and Trademark Office, Trademark Reg. No. 2,762,468 [StingRay] (registered Sep. 9, 2003), **Harris StingRay Product Description**, *all associated trademark documents available via search at* http://tmportal.uspto.gov/external/portal/tow (last accessed: Mar. 11, 2011), p. 10 of 88 page compilation;

EXHIBIT 006: United States Patent and Trademark Office, Trademark Reg. No. 2,867,227 [KingFish] (registered Jul. 27, 2004), **Harris KingFish Product Picture**, *all associated trademark documents available via search at* http://tmportal.uspto.gov/external/portal/tow (last accessed: Mar. 11, 2011), p. 7 of 67 page compilation;

EXHIBIT 007: Miami, FL, USA – Legislative Files, **Harris KingFish Product Datasheet**, *available at* http://egov.ci.miami.fl.us/Legistarweb/Attachments/34771.pdf (last accessed: Mar. 9, 2011), p. 2;

EXHIBIT 008: United States Patent and Trademark Office, Trademark Reg. No. 2,867,227 [KingFish] (registered Jul. 27, 2004), **Harris KingFish**

Product Description, *all associated trademark documents available via search at* http://tmportal.uspto.gov/external/portal/tow (last accessed: Mar. 11, 2011), p. 10 of 67 page compilation;

EXHIBIT 009: Miami, FL, USA – Legislative Files, **Harris Geolocation Product Datasheet**, *available at* http://egov.ci.miami.fl.us/Legistarweb/Attachments/34771.pdf (last accessed: Mar. 9, 2011), p. 1;

EXHIBIT 010: Miami, FL, USA – Legislative Files, **Harris AmberJack Product Datasheet**, *available at* http://egov.ci.miami.fl.us/Legistarweb/Attachments/34769.pdf (last accessed: Mar. 9, 2011), p. 2;

EXHIBIT 011: Miami, FL, USA – Legislative Files, **Harris AmberJack Product Datasheet**, *available at* http://egov.ci.miami.fl.us/Legistarweb/Attachments/40003.pdf (last accessed: Mar. 9, 2011), p. 6-7;

EXHIBIT 012: Harris, Government Communications Systems Division, *Phased Array Antennas Brochure* (2004), *available at* http://download.harris.com/app/public_download.asp?fid=450 (last accessed: Sept. 22, 2010);

EXHIBIT 013: Maricopa County, FL, USA – **Harris Price List** (Feb 24, 2010), *available at* http://www.maricopa.gov/materials/Awarded_Contracts/PDF/09041-c.pdf (last accessed Mar. 9, 2011), p. 21-25;

EXHIBIT 014: Miami, FL, USA – Legislative Files, **Harris GCSD Price List** (Sep. 2008) (Nov. 29, 2006), *available at* http://egov.ci.miami.fl.us/Legistarweb/Attachments/48000.pdf (last accessed: Mar. 9, 2011), p. 4;

EXHIBIT 015: Durham, NC, USA - City Council Agenda No. 7503, **Harris Sole Source Vendor Letter** (Sept. 29, 2010), *available at* http://www.durhamnc.gov/agendas/2010/cws20110103/251951_7503_342363.pdf (last accessed Mar. 9, 2011);

EXHIBIT 016: Miami, FL, USA – Legislative Files, **Harris Sole Source Vendor Letter** (Nov. 29, 2006), *available at* http://egov.ci.miami.fl.us/Legistarweb/Attachments/34768.pdf (last accessed: Mar. 9, 2011), p. 1;

EXHIBIT 017: Miami, FL, USA – Legislative Files, **Harris Sole Source Letter** (Aug. 25, 2008), *available at* http://egov.ci.miami.fl.us/Legistarweb/Attachments/40003.pdf (last accessed: Mar. 9, 2011), p. 2;

EXHIBIT 018: Maricopa County, FL, USA – **Harris Contract**, Serial No. 09041-SS (May 27, 2010), *available at* http://www.maricopa.gov/materials/Awarded_Contracts/PDF/09041-c.pdf (last accessed Mar. 9, 2011), p. 1, 13-14;

EXHIBIT 019: Valentino-DeVries, Jennifer, *'Stingray' Phone Tracker Fuels Constitutional Clash*, The Wall Street Journal, p. A1 (Sept. 22, 2011) (original article addressing CR08-814-PHX-DGC) *available at* http://online.wsj.com/article/SB10001424053111904194604576583112723197574.html (last accessed: Sept. 22, 2011);

EXHIBIT 020: Valentino-DeVries, Jennifer, *Feds Shift Tracking Defense: Prosecutors in Arizona Case Drop Position That 'Stingray' Use Didn't Require Warrant*, The Wall Street Journal, (Nov. 3, 2011) *available at* http://online.wsj.com/article/SB10001424052970204621904577014363024341028.html (last accessed: Nov. 15, 2011);

EXHIBIT 021: USDOJ [M.D.La.] Aug. 12, 2008, Response to ACLU FOIA Request No. 07-4130, *available at* http://www.aclu.org/pdfs/freespeech/cellfoia_release_074130_20080812.pdf (last accessed: Jan. 11, 2011); Note: only relevant pages are included with footers added containing the page numbers from the full PDF available at the above URL;

EXHIBIT 022: Altron, *GSM/UMTS Grabber: Deploying local mobile networks and secret grabbing of identification information in GSM and UMTS bands*, PDF provided at ISS World Europe 2008, *available at* http://wikileaks.org/spyfiles/files/0/87_ALTRON-GRABBER.pdf (last accessed: Apr. 10, 2012);

EXHIBIT 023: NeoSoft [website], *Portable IMSI/IMEI GSM catcher NS-17-1*, http://www.neosoft.ch/products/emerg_tracking/detail.php?ID=1017&IBLOCK_ID=39 (last accessed: Feb. 1, 2012);

EXHIBIT 024: MMI Research Trading as Cobham Surveillance, *Tactical Lawful Intercept*, PDF presentation provided at ISS World Europe 2008, *available at* http://wikileaks.org/spyfiles/files/0/43_200906-ISS-PRG-COBHAM.pdf (last accessed: Apr. 5, 2012);

EXHIBIT 025: Elaman, *Active Off-Air System 3GN UMTS*, Product Brochure, *available at* http://wikileaks.org/spyfiles/files/0/124_ELAMAN-200805-CATALOGUE-P1.zip (last accessed: May 14, 2012) [Active Off-Air System 3GN UMTS Technical Specification.pdf];

EXHIBIT 026: Elaman, *GSM Vehicle Direction Finder (VDF)*, Product Brochure, *available at* http://wikileaks.org/spyfiles/files/0/124_ELAMAN-200805-CATALOGUE-P1.zip (last accessed: May 14, 2012) [GSM Vehicle Direction Finder-VDF.pdf];

EXHIBIT 027: Ability, *3G Interception & Advanced GSM Active Solution*, PDF provided at ISS World Europe 2008, *available at* http://wikileaks.org/spyfiles/files/0/80_ABILITY-GSM_3G_Intercept.pdf (last accessed: Apr. 10, 2012);

EXHIBIT 028: Meganet [website], *Meganet Corporation - VME Undetectable Cell Phone*

Interceptors, http://www.meganet.com/meganet-products-cellphoneinterceptors.html (last accessed: Nov. 20, 2011);

EXHIBIT 029: Shoghi Communications Ltd., *Semi Active GSM Monitoring System*, PDF provided at ISS World Europe 2008, *available at* http://wikileaks.org/spyfiles/files/0/160_SHOGI-2006-semiactive_gsm_monitoring.pdf (last accessed: Apr. 10, 2012);

EXHIBIT 030: Verint, *ENGAGE GI2 Models*, Product Brochure, *available at* http://files.cloudprivacy.net.s3.amazonaws.com/wikileaks-verint-location-tracking.pdf (last accessed: Apr. 5, 2012);

EXHIBIT 031: View Systems, *Cell Phone Intercept Apparatus*, Product Brochure, *available at* http://www.viewsystems.com/pdf/CIA_11_20_06.pdf (last accessed: Apr. 5, 2012);

EXHIBIT 032: Stratign, *Strategic Defense Technologies*, 2011 Product Catalog, PDF provided at ISS World Europe 2008, *available at* http://wikileaks.org/spyfiles/files/0/278_STRATIGN-Catalogue-2011.pdf (last accessed: Apr. 10, 2012); Relevant pages attached: 1-3, 12, 19, and 100;

EXHIBIT 033: Ability [website], *Passive CDMA Interceptor, ACIS – Advanced CDMA Interception System*, *available at* http://www.interceptors.com/intercept-solutions/Passive-CDMA-Interceptor.html (last accessed: May 6, 2012);

EXHIBIT 034: srlabs.de [website], *Catcher Catcher - Wiki – Redmine*, *available at* http://opensource.srlabs.de/projects/catcher/wiki/Wiki (last accessed: Apr. 5, 2012);

EXHIBIT 035: Daviscomms [datasheet], *GSM/GPRS/GPS Mobile Tracking Device: EaziTRAC 1000*, *available at* http://www.daviscommsusa.com/pdf/EaziTRAC%201000_Brochure_RevE1.pdf (last accessed: Jan. 5, 2012);

EXHIBIT 036: Collection of various web pages from http://www.alibaba.com advertising GPS based mobile tracking devices;

EXHIBIT 037: FBI Jul. 2, 2007, Response to EFF FOIA Request Nos. 1056287-000 & 1056307-1, *available at* http://www.eff.org/files/filenode/061708CKK/070207_dcs08.pdf [EFF PDF Set 8 of 8] (last accessed: Oct. 25, 2010); Note: only relevant pages are included with footers added containing the page numbers from the full PDF available at the above URL;

EXHIBIT 038: FBI Aug. 27, 2007, Response to EFF FOIA Request Nos. 1056287-000 & 1056307-1, *available at* http://www.eff.org/files/filenode/061708CKK/082707_dcs01.pdf [EFF PDF Set 1 of 6] (last accessed: Oct. 25, 2010); Note: only relevant pages are included with footers added containing the page numbers from the full PDF available at the above URL;

EXHIBIT 039: FBI Aug. 27, 2007, Response to EFF FOIA Request Nos. 1056287-000 & 1056307-1, *available at* http://www.eff.org/files/filenode/061708CKK/082707_dcs05.pdf [EFF PDF Set 5 of 6] (last accessed: Oct. 25, 2010); Note: only relevant pages are included with footers added containing the page numbers from the full PDF available at the above URL;

EXHIBIT 040: FBI Sept. 24, 2007, Response to EFF FOIA Request Nos. 1056287-000 & 1056307-1, *available at* http://www.eff.org/files/filenode/061708CKK/092407_dcs01.pdf [EFF PDF Set 1 of 3] (last accessed: Oct. 25, 2010); Note: only relevant pages are included with footers added containing the page numbers from the full PDF available at the above URL;

EXHIBIT 041: FBI Oct. 22, 2007, Response to EFF FOIA Request Nos. 1056287-000 & 1056307-1, *available at* http://www.eff.org/files/filenode/061708CKK/20071022_dcs02.pdf [EFF PDF Set 2 of 6] (last accessed: Oct. 25, 2010); Note: only relevant pages are included with footers added containing the page numbers from the full PDF available at the above URL;

EXHIBIT 042: FBI Oct. 22, 2007, Response to EFF FOIA Request Nos. 1056287-000 & 1056307-1, *available at* http://www.eff.org/files/filenode/061708CKK/20071022_dcs03.pdf [EFF PDF Set 3 of 6] (last accessed: Oct. 25, 2010); Note: only relevant pages are included with footers added containing the page numbers from the full PDF available at the above URL;

EXHIBIT 043: FBI Oct. 22, 2007, Response to EFF FOIA Request Nos. 1056287-000 & 1056307-1, *available at* http://www.eff.org/files/filenode/061708CKK/20071022_dcs04.pdf [EFF PDF Set 4 of 6] (last accessed: Oct. 25, 2010); Note: only relevant pages are included with footers added containing the page numbers from the full PDF available at the above URL;

EXHIBIT 044: FBI Nov. 19, 2007, Response to EFF FOIA Request Nos. 1056287-000 & 1056307-1, *available at* http://www.eff.org/files/filenode/061708CKK/20071119_dcs01.pdf [EFF PDF Set 1 of 4] (last accessed: Oct. 25, 2010); Note: only relevant pages are included with footers added containing the page numbers from the full PDF available at the above URL;

EXHIBIT 045: FBI Dec. 17, 2007, Response to EFF FOIA Request Nos. 1056287-000 & 1056307-1, *available at* http://www.eff.org/files/filenode/061708CKK/20071217_dcs03.pdf [EFF PDF Set 3 of 5] (last accessed: Oct. 25, 2010); Note: only relevant pages are included with footers added containing the page numbers from the full PDF available at the above URL;

EXHIBIT 046: FBI Dec. 17, 2007, Response to EFF FOIA Request Nos. 1056287-000 & 1056307-1, *available at*

http://www.eff.org/files/filenode/061708CKK/20071217_dcs05.pdf [EFF PDF Set 5 of 5] (last accessed: Oct. 25, 2010); Note: only relevant pages are included with footers added containing the page numbers from the full PDF available at the above URL;

EXHIBIT 047: FBI Jan. 14, 2008, Response to EFF FOIA Request Nos. 1056287-000 & 1056307-1, *available at* http://www.eff.org/files/filenode/20080114_dcs03.pdf [EFF PDF Set 3 of 4] (last accessed: Oct. 25, 2010); Note: only relevant pages are included with footers added containing the page numbers from the full PDF available at the above URL;

EXHIBIT 048: FBI Jan. 14, 2008, Response to EFF FOIA Request Nos. 1056287-000 & 1056307-1, *available at* http://www.eff.org/files/filenode/061708CKK/20080114_dcs04.pdf [EFF PDF Set 4 of 4] (last accessed: Oct. 25, 2010); Note: only relevant pages are included with footers added containing the page numbers from the full PDF available at the above URL;

EXHIBIT 049: FBI Feb. 11, 2008, Response to EFF FOIA Request Nos. 1056287-000 & 1056307-1, *available at* http://www.eff.org/files/filenode/061708CKK/20080211_dcs01.pdf [EFF PDF Set 1 of 3] (last accessed: Oct. 25, 2010); Note: only relevant pages are included with footers added containing the page numbers from the full PDF available at the above URL;

EXHIBIT 050: FBI Feb. 11, 2008, Response to EFF FOIA Request Nos. 1056287-000 & 1056307-1, *available at* http://www.eff.org/files/filenode/061708CKK/20080211_dcs02.pdf [EFF PDF Set 2 of 3] (last accessed: Oct. 25, 2010); Note: only relevant pages are included with footers added containing the page numbers from the full PDF available at the above URL;

EXHIBIT 051: FBI Feb. 11, 2008, Response to EFF FOIA Request Nos. 1056287-000 & 1056307-1, *available at* http://www.eff.org/files/filenode/061708CKK/20080211_dcs03.pdf [EFF PDF Set 3 of 3] (last accessed: Oct. 25, 2010); Note: only relevant pages are included with footers added containing the page numbers from the full PDF available at the above URL;

EXHIBIT 052: U.S. Dep't of Justice, Electronic Surveillance Manual; Note: includes section on CELL SITE SIMULATORS / DIGITAL ANALYZERS / TRIGGERFISH, p. 40-41 and 44-45.

[Redacted by the defendant (for relevance) using white squares with black borders.]

EXHIBIT 053: U.S. Dep't of Justice, Electronic Surveillance Manual; Note: includes section on MOBILE TRACKING DEVICES, p. 48.

[Redacted by the defendant (for relevance) using white squares with black borders.]

EXHIBIT 054: Department of Justice, *Retention Periods of Major Cellular Service Providers* (Aug. 2010), *available at* http://www.wired.com/images_blogs/threatlevel/2011/09/retentionpolicy.pdf (last accessed: Dec. 7, 2011); Note: Verizon Wireless stores "Cell towers used by phone" for "1 rolling year" and does not store LAESP messages, call-identifying information, or Pen/Trap data;

EXHIBIT 055: Telecommunications Industry Association, ANSI/TIA-878-2 (Addenda to TIA-878), *Interoperability Specification (IOS) for High Rate Packet Data (HRPD) Radio Access Network Interfaces with Session Control in the Access Network* (Arlington, VA: May 2008), § 3.1.1, p. 3.1, "Figure 3.1.1-1 Initial AT Origination with HRPD Session Establishment and Key Exchange"; Note: shows 1xEV-DO registration process occurring between PCF and PDSN over the A11 interface, *i.e.*, not between the Access Terminal and Access Network;

EXHIBIT 056: Telecommunications Industry Association, TIA/EIA/J-STD-025A, *Lawfully Authorized Electronic Surveillance*, Annex A, p. 89, Figure No. 21 (Arlington, VA: May 31, 2000); Note: showing diagram of CALEA network Looped Access;

EXHIBIT 057: DiBuduo, Marcus, Denso Corp., U.S. Patent No. 6,999,778 (Oceanside, CA: Feb. 14, 2006), *available at* http://www.freepatentsonline.com/6999778.html (last accessed Sept. 29, 2010), Sheet 9 of 11, Fig. 10; Note: Fig. 10 is a diagram showing five regions of a cell site radiation pattern with each region corresponding to a location signature deduced from historical cell site location information;

EXHIBIT 058: Thales [PDF presentation], *New solutions for massive monitoring*, ISS World Europe, p. 4 (Oct. 3, 2008), *available at* ttp://wikileaks.org/spyfiles/files/0/40_200810-ISS-PRG-THALES.pdf (last accessed: Apr. 10, 2012); Note: page No. 4 attached; "spectrum activity"chart showing *some* electromagnetic frequencies used by modern day radio communication systems;

EXHIBIT 059: Verizon Wireless FCC Cellular license documents: (1) FCC [website], *ULS License - Cellular License - KNKA211 - GTE MOBILNET OF CALIFORNIA LIMITED PARTNERSHIP*, http://wireless2.fcc.gov/UlsApp/UlsSearch/license.jsp?licKey=12154 (last accessed: Mar. 4, 2012); (2) FCC [website], *ULS License - Cellular License - KNKA211 - GTE MOBILNET OF CALIFORNIA LIMITED PARTNERSHIP – Frequencies*, http://wireless2.fcc.gov/UlsApp/UlsSearch/frequenciesCell.jsp?licKey=12154&channelBlock=B (last accessed: Mar. 4, 2012);

EXHIBIT 060: Verizon Wireless FCC Cellular license documents: FCC [website], *ULS License - PCS Broadband License - WQIQ264 - Verizon Wireless Telecom Inc.*, http://wireless2.fcc.gov/UlsApp/UlsSearch/license.jsp?licKey=3003123 (last accessed: Apr. 9, 2012);

EXHIBIT 061: Metadata screenshot of "aircard 4152649596.xls" provided to the FBI by Mark Denton, Verizon Wireless law enforcement liaison, on July 12, 2008;

Note: respective .xls (Excel) file is the original **first set** of historical cell site information for the aircard provided by Verizon Wireless in response to District of Arizona 08-3298MB-LOA order; Metadata shows that the file was created by "dentoma" on July 12, 2008;

[Redacted by the defendant (for defense security reasons) using white squares with black borders.]

EXHIBIT 062: Metadata screenshot of "9596.xls" provided to the FBI by John Profaca, Verizon Wireless law enforcement liaison, on August 1, 2008; Note: respective .xls (Excel) file is the original **second set** of historical cell site information for the aircard provided by Verizon Wireless in response to District of Arizona 08-3298MB-LOA order; Metadata shows that the file was created by "profajo" on August 1, 2008;

[Redacted by the defendant (for defense security reasons) using white squares with black borders.]

EXHIBIT 063: (1) Two page chart of text messages sent and received by FBI Agent Richard J. Murray while the aircard was being located on July 16-17, 2008; Note: created by the defense using ITEM No. 6 of December 9, 2011 discovery set; and (2) page Nos. 1, 2, 3, 9, and 10 of original chart of text messages provided by the government; (ITEM No. 6 of December 9, 2011 discovery set);

[Redacted by the defendant (for relevance) using white squares with black borders.]

EXHIBIT 064: Chart of text messages sent by the FBI technical agents while the aircard was being located on July 16-17, 2008; Note: page Nos. 1 (cover sheet), 2, 12, 3, and 13 of text messages; (ITEM No. 2 of March 22, 2012 discovery set);

[Redacted by the defendant (for relevance) using white squares with black borders.]

EXHIBIT 065: Case write ups by FBI Agent Richard J. Murray; Note: indicates that FBI Agent Murray "ran a field test with IRS of a similar aircard and communicated with OTD to ensure that the tracking would not be detected by the subject."; (10/6/11 BATES Nos. 000009-000010 of October 6, 2011 discovery set);

EXHIBIT 066: Summary of an internal FBI memorandum prepared by one of the three FBI technical agents that operated the equipment used to locate the aircard; Note: states that "Verizon gave a distance from the tower to the target."; (ITEM No. 4 of December 9, 2011 discovery set);

EXHIBIT 067: Letter from AUSA Frederick A. Battista to Daniel Rigmaiden RE: the aircard Pen/Trap data transmitted to the FBI by Verizon Wireless was only buffered for an extremely short period prior to transmission; Note: page Nos. 1, 4, and 10; Note: exhibit includes only relevant pages; (Letter date: January 28, 2011);

[Redacted by the defendant (for relevance) using white squares with black borders.]

EXHIBIT 068: Letter from AUSA Frederick A. Battista to Daniel Rigmaiden (relevant sections) RE: definitions and explanations relating to the aircard locating mission – response to defendant's March 9, 2011 discovery request letter; Note: exhibit includes only relevant pages; (Letter date: May 2, 2011);

[Redacted by the defendant (for relevance) using white squares with black borders.]

EXHIBIT 069: Letter from AUSA Frederick A. Battista to Daniel Rigmaiden RE: (1) the FBI technical agents called the aircard in order to generate real-time cell site location information; and (2) the aircard hardware never answered the FBI's surreptitious phone calls placed to the aircard; (Letter date: June 7, 2011);

[Redacted by the defendant (for relevance) using white squares with black borders.]

EXHIBIT 070: Letter from AUSA Frederick A. Battista to Daniel Rigmaiden (relevant sections) RE: (1) the government destroyed the evidence obtained via the N.D.Cal. 08-90330MISC-RS order; Note: exhibit includes only relevant pages; (Letter postmark date: June 18, 2010);

[Redacted by the defendant (for relevance) using white squares with black borders.]

EXHIBIT 071: Letter from AUSA Frederick A. Battista to Daniel Rigmaiden RE: (1) the FBI policy requiring that FBI technical agents ensure that portable/transportable wireless device locators are cleared of prior case data, (2) the FBI repeatedly called the aircard in order to force it to connect to the cell tower providing the strongest signal, (3) no man-in-the-middle attack was conducted on the aircard connection, and (4) the devices used to locate the aircard are not capable of conducting a man-in-the-middle attack; (Letter date: December 2, 2011);

EXHIBIT 072: Letter from AUSA Frederick A. Battista to Daniel Rigmaiden RE: (1) incoming calls were placed to the aircard in order to stimulate it to provide location information; and (2) encryption was not used while locating the aircard; (Letter date: December 9, 2011);

[Redacted by the defendant (for relevance) using white squares with black borders.]

EXHIBIT 073: Letter from AUSA Frederick A. Battista to Daniel Rigmaiden RE: (1) there were three FBI technical agents who operated the equipment used to locate the aircard; (2) the N.D.Cal. 08-90330MISC-RS and 08-90331MISC-RS proposed orders that were drafted by the government were not altered by the magistrate prior to signing, and (3) no man-in-the-middle attack was conducted on the aircard connection; Note: exhibit includes only relevant pages; (Letter date: December 16, 2011);

[Redacted by the defendant (for relevance) using white squares with black borders.]

EXHIBIT 074: FBI FD-302 Report by FBI Agent Richard J. Murray RE: subpoenaed DVD of June 12, 2008 video camera footage for Verizon Wireless store located at 768 Market St., San Francisco, CA, 94102 where aircard payment was made; (Investigation date: July 17, 2008); (2/12/09 BATES No. 482 of February 17, 2009 discovery set);

EXHIBIT 075: Still images of individual paying aircard account bill; Note: PDF file was created from still images extracted from the June 12, 2008 video camera footage for Verizon Wireless store located at 768 Market St., San Francisco, CA, 94102 (obtained by the government via District of Arizona Grand Jury Subpoena Grand Jury subpoena No. 07-03-665), provided as ITEM NO. 1 of the March 24, 2010 discovery set;

EXHIBIT 076: Government picture (cropped) of "Black Adidas 'Clima 365'" pants with three white stripes seized from apartment No. 1122 on August 3-4, 2008; Note: picture was taken during search of apartment No. 1122; (file name DSC00739.JPG of December 9, 2011 discovery set);

EXHIBIT 077: FBI FD-302 Report by FBI Agent Richard J. Murray RE: two physical cash payments made on aircard account at Verizon Wireless store located at 768 Market St., San Francisco, CA, 94102; (Investigation date: June 27, 2008); (2/12/09 BATES No. 485 of February 17, 2009 discovery set);

EXHIBIT 078: Paper print-out of emails sent from IRS-CI Agent Tracy L. Daun to FBI Agent Richard J. Murray, IRS-CI Agent Denise L. Medrano, and IRS-CI Agent Michael P. Fleischmann RE: matching aircard destination IP addresses to IP addresses used to file alleged fraudulent tax returns; (Email sent dates: (1) June 25, 2008 7:29pm, (2) June 25, 2008 11:41pm); (10/6/11 BATES Nos. 001029-001032 of October 6, 2011 discovery set);

[Redacted by the defendant (for relevance) using white squares with black borders.]

EXHIBIT 079: Paper print-out of email sent from IRS-CI Agent Tracy L. Daun to IRS-CI Agent Denise L. Medrano and IRS-CI Agent Michael P. Fleischmann RE: aircard account login records found on computer seized from apartment No. 1122 with tr_verizon_info.txt attachment; (Email sent date: August 20, 2008 4:50pm); (12/09/11 BATES Nos. 000132-000133 of December 9, 2011 discovery set);

[Redacted by the defendant (for relevance) using white squares with black borders.]

EXHIBIT 080: Jorcal, Inc. [website], *JORCAL Hat Co.- San Jose*, http://www.jorcalinc.com (last accessed: Apr. 6, 2012);

EXHIBIT 081: Hats Of The Fillmore [website], *Welcome to Hats Of The Fillmore*, http://hatsofthefillmore.com/hatsofthefillmore.com/Welcome.html (last accessed: Apr. 6, 2012);

EXHIBIT 082: BJA/FBI/JRIC, Tripwire, *Communities Against Terrorism: Potential Indicators of Terrorist Activities Related to Military Surplus Stores* (PDF flyer), *download from* http://www.publicintelligence.net/fbi-suspicious-activity-reporting-flyers (last access: Mar. 18, 2012); Note: flyer indicates that people who "[m]ake bulk purchases of items to include: [] Meals Ready to Eat" is a suspicious activity indicative of possible "terrorism.";

EXHIBIT 083: Northern District of California 08-70503-PVT search warrant return; Note: listing household items and clothing seized from apartment No. 1122; (Magistrate Judge: Patricia V. Trumbull; Signature Date: August 5, 2008); (3/2/09 BATES Nos. 6456-6470 of March 2, 2009 discovery set);

EXHIBIT 084: Paper print-out of emails sent from USPIS Inspector James L. Wilson to Bill Atwell, Lenovo Corporate Security RE: legitimate purchase of host laptop computer used with aircard to access the Internet; (Email sent dates: (1) October 4, 2011 1:23pm; (2) October 4, 2011 11:55am; (3) October 4, 2011 1:29pm; (4) October 4, 2011 1:56pm); (ITEM No. 1 of October 6, 2011 discovery set);

[Redacted by the defendant (pursuant to Fed. R. Crim. P. 49.1(a)) using white squares with black borders.]

EXHIBIT 085: Report of investigation by USPIS Inspector James L. Wilson RE: contact with Lenovo about purchase of host laptop computer used with the aircard; Note: indicating that the laptop was purchased with a prepaid debit card; (Report date: October 12, 2011); (ITEM No. 8 of December 9, 2011 discovery set);

[Redacted by the defendant (pursuant to Fed. R. Crim. P. 49.1(a)) using white squares with black borders.]

EXHIBIT 086: Bancorp Bank subpoena response materials (incorporating the original filed subpoena) for District of Arizona Grand Jury Subpoena; Note: subpoena requests account information on the prepaid debit card used to purchase the host laptop computer used with the aircard to access the Internet; (Originator: AUSA Frederick A. Battista; Subpoena service date: November, 17 2011); (ITEM No. 6 of December 16, 2011 discovery set);

[Redacted by the defendant (pursuant to Fed. R. Crim. P. 49.1(a)) using white squares with black borders.]

EXHIBIT 087: Computer Forensic Report by IRS-CI Agent Tracy L. Daun RE: search of physical storage devices and virtual drives seized from apartment No. 1122 under the reissued/amended version of the N.D.Cal. 08-70460-HRL warrant; Note: exhibit includes only relevant sections; (ITEM No. 23A of the February 25, 2010 discovery set);

[Redacted by the defendant (for relevance) using white squares with black borders.]

EXHIBIT 088: March 7, 2012 IRS Memorandum for Transmittal of Electronically Stored

Information by IRS-CI Agent Tracy L. Daun; (ITEM No. 1 of March 22, 2012 discovery set);

EXHIBIT 089: Select documents for Domicilio apartment complex, apartment No. 1122, leasing agreement for Steven Brawner covering October 21, 2008 through April 30, 2008; (2/19/09 BATES Nos. 4968, 4970, 4969, 4975-4976, and 4994 of UNKNOWN discovery set);

[Redacted by the defendant (pursuant to Fed. R. Crim. P. 49.1(a)) using white squares with black borders.]

EXHIBIT 090: (1) March 18, 2008 letter from Domicilio management inviting Steven Brawner to renew his lease on apartment No. 1122; and (2) Domicilio apartment complex records indicating that Steven Brawner would continue renting apartment No. 1122 "month to month" after April 30, 2008; (2/19/09 BATES Nos. 4992 and 4988 of UNKNOWN discovery set);

EXHIBIT 091: FBI FD-302 Reports by FBI Agent Richard J. Murray RE: Domicilio management indicated that occupant of apartment No. 1122 paid his rent with money orders for May, June, July and August of 2008; (Investigation dates: July 29, 2008 and July 31, 2008); (2/12/09 BATES Nos. 231-232 of February 17, 2009 discovery set);

EXHIBIT 092: Leasingdesk.com eRenterPan insurance policy for Domicilio apartment No. 1122; (2/19/09 BATES Nos. 4936-4940 of UNKNOWN discovery set);

EXHIBIT 093: Domicilio apartment complex, apartment No. 1122, electronic gate access key fob receipt (fob No. 58261); (2/19/09 BATES No. 4967 of UNKNOWN discovery set);

EXHIBIT 094: Paper print-out of email sent from Richard J. Murray to IRS-CI Agent Denise L. Medrano, AUSA Frederick A. Battista, USPIS Inspector James L. Wilson, and IRS-CI Agent Michael P. Fleischmann RE: apartment 1122 electricity bills are paid using money orders, checks, etc.; (Email sent date: July 22, 2008 5:20pm); (ITEM No. 3 of September 24, 2010 discovery set);

EXHIBIT 095: Bill from Silicon Valley Power to Steven Brawner RE: 431 El Camino Real, Apartment No. 1122, Santa Clara, CA. 95050; (Letter date: January 16, 2009);

EXHIBIT 096: Comcast subpoena response materials for District of Arizona Grand Jury Subpoena No. 07-03-708; Attached materials includes letter/notice that no Comcast Cable Communications, LLC customer or subscriber information (*i.e.*, no Internet service) is associated with 431 El Camino Real, Apartment No. 1122, Santa Clara, CA. 95050; (Originator: IRS-CI Agent Denise L. Medrano; Subpoena service date: July 23, 2008; Comcast response date: August 5, 2008); (3/2/09 BATES Nos. 6896-6901 of March 2, 2009 discovery set);

EXHIBIT 097: Various physical surveillance logs of 431 El Camino Real, Santa Clara, CA with no individuals reported seen coming or going from apartment No. 1122; (2/12/09 BATES Nos. 104-107, 111-114, 130, 134, 140, and 145 of February 17, 2009 discovery set);

EXHIBIT 098: Paper print-out of email sent from USPIS Inspector James L. Wilson to IRS-CI Agent Denise L. Medrano, IRS-CI Agent Michael P. Fleischmann, AUSA Frederick A. Battista, and FBI Agent Richard J. Murray RE: as of July 21, 2008, no evidence that someone is living in apartment No. 1122; (Email sent date: July 21, 2008 2:49pm); (ITEM No. 2 of September 24, 2010 discovery set [p. 30]);

EXHIBIT 099: FBI FD-302 Report by FBI Agent Richard J. Murray RE: Domicilio management indicated that the process for obtaining electronic gate key access records for apartment residents is extremely time consuming; (Investigation date: July 22, 2008); (2/12/09 BATES No. 138 of February 17, 2009 discovery set);

EXHIBIT 100: FBI FD-302 Report by FBI Agent Richard J. Murray RE: Quality Alarm Service indicated that the Domicilio apartment complex crashed the electronic gate key access database for apartment residents; (Investigation date: July 23, 2008); (2/12/09 BATES No. 139 of February 17, 2009 discovery set);

EXHIBIT 101: Paper print-out of emails sent between FBI Agent Richard J. Murray and AUSA Frederick A. Battista *et al.* RE: (1) Quality Alarm Service technician canceled his day off to physically retrieve electronic gate key access records from various Domicilio electronic gates, and (2) AUSA Battista's electronic gate key access analysis; (Email sent dates: (1) July 24, 2008 6:15pm; (2) July 24, 2008 9:05pm); (ITEM No. 3 of September 24, 2010 discovery set [p. 137-139]);

EXHIBIT 102: FBI FD-302 Report by FBI Agent Richard J. Murray RE: Quality Alarm Service responded to District of Arizona Grand Jury Subpoena No. 07-03-709 by providing Domicilio electronic gate key access records for June 25, 2008 to July 24, 2008; (Investigation date: July 24, 2008); (2/12/09 BATES No. 483 of February 17, 2009 discovery set);

EXHIBIT 103: Paper print-out of email sent from AUSA Frederick A. Battista to AUSA Shawna Yen RE: We have confirmed that the target is in the Santa Clara Area and visited the target apartment on 7/23; (Email sent date: July 25, 2008 11:18am); (ITEM No. 2 of September 24, 2010 discovery set [p. 52]);

EXHIBIT 104: FBI FD-302 Report by FBI Agent Robert L. Kay RE: August 2, 2008 visual surveillance of apartment No. 1122; (Investigation date: August 2, 2008); (2/12/09 BATES No. 145 of February 17, 2009 discovery set);

EXHIBIT 105: FBI FD-302 Report by FBI Agent Wade Luders RE: August 3, 2008 visual surveillance of apartment No. 1122; (Investigation date: August 3, 2008); (2/12/09 BATES No. 130 of February 17, 2009 discovery set);

EXHIBIT 106: FBI FD-302 Report by FBI Agent Aleksandr Kobzanets RE: (1) arrest of unknown male (by Santa Clara, CA police officers) who was seen within the Domicilio apartment complex, and (2) FBI Agent Kobzanets' keyhole search of apartment No. 1122; (Investigation date: August 3, 2008); (2/12/09 BATES Nos. 122-24 of February 17, 2009 discovery set);

EXHIBIT 107: Paper print-out of email sent from FBI Agent Richard J. Murray to FBI Agent William T. Ng RE: awards for the Santa Clara, CA police officers for arresting the unknown male who was seen within the Domicilio apartment complex on August 3, 2008; (Email sent date: September 17, 2008 4:29pm); (ITEM No. 15 of November 24, 2010 discovery set [p. 45-46]);

EXHIBIT 108: Defendant's August 3, 2008 Santa Clara police department booking photo compared to the picture contained on the "Steven Brawner" ID on record with the Domicilio apartment complex; (ITEM No. 38 of November 9, 2010 discovery set);

[Redacted by the defendant (pursuant to Fed. R. Crim. P. 49.1(a)) using white squares with black borders.]

EXHIBIT 109: Page No. 1 of rough notes prepared by IRS-CI Agent Denise L. Medrano RE: (1) three apartments identified at Domicilio apartment complex (1120, 1122, and 1124), and (2) "StingRay" listed at end of checklist; (Notes date: July 15, 2008); (ITEM No. 6 of September 24, 2010 discovery set [p. 269]);

EXHIBIT 110: Relevant documents from: United States v. Luis Soto, Crim. No. 03:09CR200 (AWT), Doc. #112-1 (D. Conn., Jun. 28, 2010); Note exhibit includes sample of cell site information provided to the government by Sprint Nextel Corporation in response to a court order obtained under 18 U.S.C. § 2703(d); all documents are public record with full versions available on PACER;

EXHIBIT 111: Relevant documents from: In The Matter Of An Application Of The United States Of America For An Order Authorizing The Release Of Historical Cell-Site Information, Case No. 1:10-mc-00550-RRM-JO, Doc. #004-2 (E.D.N.Y., Aug. 24, 2010); Note: exhibit includes sample of cell site information provided to the government by an unknown wireless carrier in response to a court order obtained under 18 U.S.C. § 2703(d); all documents are public record with full versions available on PACER;

EXHIBIT 112: Relevant documents from In The Matter Of An Application Of The United States Of America For An Order Authorizing The Disclosure Of Latitude And Longitude Data..., 11-MC-00393-SMG (E.D.N.Y. 2010); Note: includes copies of Doc. #001, p. 1-15 (Affidavit); p. 16-19 (order); and p. 20-22 (warrants); all documents are public record with full versions available on PACER;

EXHIBIT 113: Relevant documents from: United States v. Velasquez, No. S3-08-CR-0730-WHA (N.D.Cal, Aug. 17, 2010); Note: includes historical cell site location information orders attached to "Declaration Of W.S. Wilson

Leung In Support Of Government's Opposition To Danilo Velasquez's Suppression Motion," Doc. No. 2130-1, p. 4-12; all documents are public record with full versions available on PACER;

EXHIBIT 114: Relevant documents from: In the Matter of the Search of The wireless signal broadcasting the SSID "BELKIN54G" further described in Attachment A, No. 07-MC-9082 (D.Or., Apr. 2, 2007) (sealed warrant application, affidavit, warrant, and return), *available at* United States v. Ahrndt, No. 08-468-KI, Doc. No. 025, p. 62-81 (D.Or., Jan. 28, 2010); Note: exhibit includes (1) warrant to search/seize wireless router and source IP address therefrom, (2) warrant return, and (3) select sections from warrant application; all documents are public record with full versions available on PACER;

[Redacted by the defendant (for relevance) using white squares with black borders.]

EXHIBIT 115: Relevant documents from: In The Matter Of An Application For An Order Authorizing The Installation, Use, Monitoring, Repair, Replacement And Removal Of A Tracking Device, 11-MC-031-ALC (E.D.N.Y. 2011); Note: includes copies of Doc. #005, p. 1-4 (Tracking Warrant and Return); and Doc. #001, p. 22-25 (Tracking Order); all documents are public record with full versions available on PACER;

EXHIBIT 116: Relevant documents from: In The Matter Of The Application Of The United States Of America For An Order..., Mag. No. 99-4061-01 (D.N.J., May 8, 1999), *available at* http://web.archive.org/web/20061209091739/http://www2.epic.org/crypto/scarfo/order_5_99.pdf (last accessed: May 6, 2012); Note: includes order authorizing the surreptitious installation of software/firmware on a target home computer; all documents are public record with full versions available on PACER;

EXHIBIT 001

Letter from AUSA Frederick A. Battista to Daniel Rigmaiden RE: the prosecution claiming that the defendant never referred to himself as a "self-described Hacker" and that the statement in the U.S. Attorney's Office, District of Arizona, *press release No. 2010-060 (Rigmaiden, et al.)* was "inartfully drafted."; (Letter date: July 21, 2010);

[Highlighting added by the defendant.]

U.S. Department of Justice

United States Attorney
District of Arizona

Two Renaissance Square
40 North Central Avenue, Suite 1200
Phoenix, Arizona 85004-4408

Main: (602) 514-7500
Main Fax: (602) 514-7693

July 21, 2010

Daniel Rigmaiden
Agency No. 10966111
CCA-CADC
Post Office Box 6300
Florence, Arizona 85132

Re: United States v. Daniel David Rigmaiden,et al.,
CR-08-814-001- PHX-DGC

Dear Mr. Rigmaiden:

This is in response to your letter dated June 27, 2010, requesting additional discovery regarding the April 8, 2010, press conference concerning this case. Please be advised that all notes and/or background materials for the representatives of the United States Attorney's Office, Internal Revenue Service - Office of Investigation, and Federal Bureau of Investigation have been reviewed to determine whether there is any information related to the statement in Press Release No. 2010-06, regarding this case, which stated " . . . a self-described California based 'Hacker' named Daniel David Rigmaiden led a complex tax fraud conspiracy . . . " Please be advised that there is no mention of this matter in any of the materials. In addition, please be advised that the representative of the Postal Inspection Service destroyed his personal notes immediately after the press conference. As a courtesy to you, we are disclosing the proposed text of statements for the representatives of the United States Attorney's Office, Internal Revenue Service - Office of Investigation, and Federal Bureau of Investigation; none of these materials mention this matter. For your information, these statements are generally not read verbatim during press conferences by agency representatives.

1. Proposed statement of U.S. Attorney's Office representative.

2. Proposed statement of Internal Revenue Service - Office of Investigation representative.

3. Proposed statement of Federal Bureau of Investigation representative.

In preparing this response to your request, we again have not reviewed each line of the over 20,000 pages of discovery in this case but, at present, are unaware of any item wherein you personally referred to yourself as the "Hacker" in any manner, e.g., verbally, in writing or via an e-mail, etc. The inartfully drafted reference in the press release was not based upon any known reference within the discovery. In addition, please be advised again that the government does not have a recording of the press conference related to the subject press release and we do not intend to attempt to obtain one from any of the representatives of the press who attended the conference.

A copy of this cover letter is also being mailed separately to you at CCA. Additional discovery will continue to be released to you as it becomes available.

Sincerely yours,

DENNIS K BURKE
United States Attorney
District of Arizona

FREDERICK A. BATTISTA
Assistant United States Attorney

Enclosures

cc: Philip Seplow
Taylor Fox

EXHIBIT 002	United States Patent and Trademark Office, Trademark Reg. No. 2,762,468 [StingRay] (registered Sep. 9, 2003), **Harris StingRay Product Pictures**, *all associated trademark documents available via search at* http://tmportal.uspto.gov/external/portal/tow (last accessed: Mar. 11, 2011), p. 9 & 15 of 88 page compilation;
EXHIBIT 002	
EXHIBIT 002	
EXHIBIT 002	
EXHIBIT 002	
EXHIBIT 002	
EXHIBIT 002	
EXHIBIT 002	
EXHIBIT 002	
EXHIBIT 002	
EXHIBIT 002	
EXHIBIT 002	
EXHIBIT 002	
EXHIBIT 002	
EXHIBIT 002	
EXHIBIT 002	
EXHIBIT 002	
EXHIBIT 002	
EXHIBIT 002	
EXHIBIT 002	
EXHIBIT 002	
EXHIBIT 002	
EXHIBIT 002	
EXHIBIT 002	
EXHIBIT 002	
EXHIBIT 002	
EXHIBIT 002	
EXHIBIT 002	
EXHIBIT 002	
EXHIBIT 002	
EXHIBIT 002	
EXHIBIT 002	
EXHIBIT 002	

USPTO StingRay Trademark [all docs.]; Reg. No. 2,762,468 [Sep. 9, 2003]; Page # 9 of 88;
Download at <http://tmportal.uspto.gov/external/portal/tow> [last accessed Mar. 11, 2011];

SPECIMEN

Internet Transmission Date:
06/05/2003

Serial Number:
76303503

International Class:
009

USPTO StingRay Trademark [all docs.]; Reg. No. 2,762,468 [Sep. 9, 2003]; Page # 15 of 88;
Download at <http://tmportal.uspto.gov/external/portal/tow> [last accessed Mar. 11, 2011];

EXHIBIT 003

Miami, FL, USA – Legislative Files, **Harris StingRay Product Datasheet**, *available at* http://egov.ci.miami.fl.us/Legistarweb/Attachments/34769.pdf (last accessed: Mar. 9, 2011), p. 1;

HARRIS

WIRELESS
products grou

StingRay™

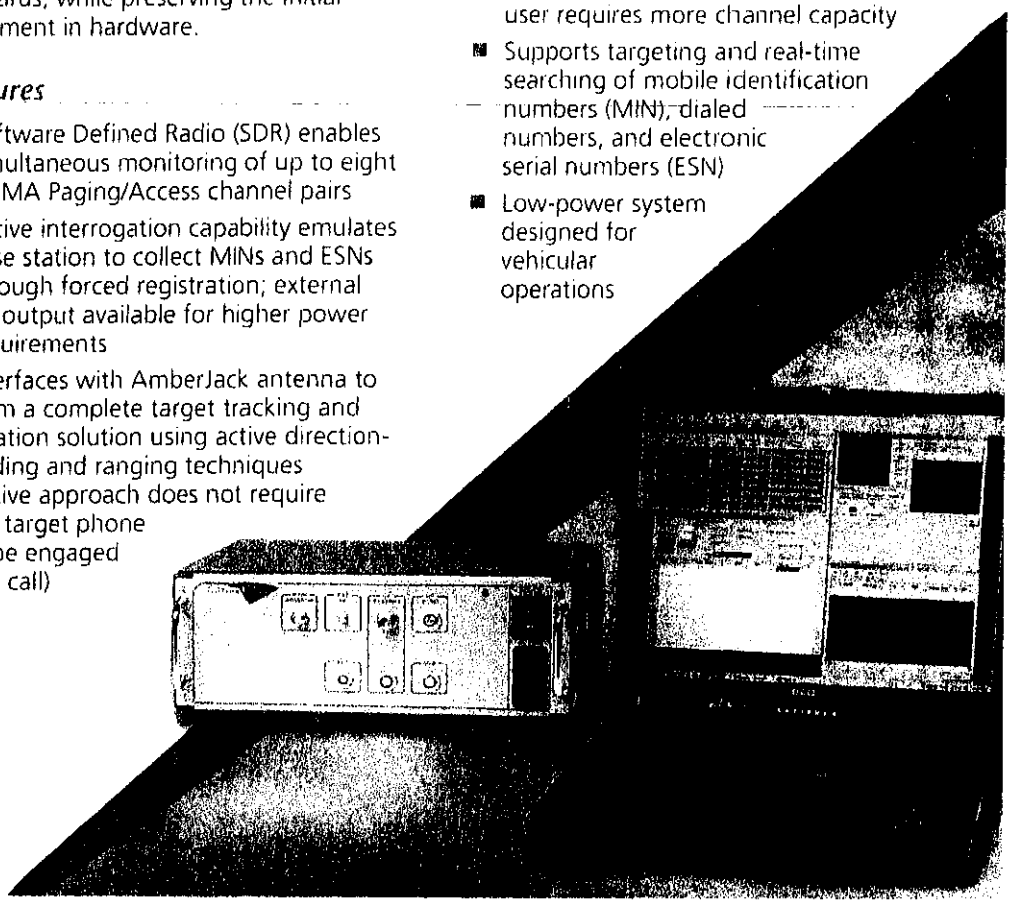
Transportable CDMA Interrogation, Tracking and Location, and Signal Information Collection System

Product Description

StingRay™ is Harris' latest offering in a long line of advanced wireless surveillance products. StingRay is a multichannel software defined radio that performs network base station surveys, Dialed Number and registration collection, mobile interrogation, and target tracking and location with Harris' AmberJack™ Direction-Finding Antenna. This low-power transportable surveillance system is designed with the future in mind—its reconfigurable architecture lends itself to upgrades of new capabilities and wireless standards, while preserving the initial investment in hardware.

Features

- Software Defined Radio (SDR) enables simultaneous monitoring of up to eight CDMA Paging/Access channel pairs
- Active interrogation capability emulates base station to collect MINs and ESNs through forced registration; external PA output available for higher power requirements
- Interfaces with AmberJack antenna to form a complete target tracking and location solution using active direction-finding and ranging techniques (active approach does not require the target phone to be engaged in a call)
- Optional geolocation software overlays target tracks and tracking vehicle location on a digital map
- Wideband RF front-end provides simultaneous operation in the U.S. cellular 800 and PCS 1900 MHz bands and is preconfigured to support iDEN (low band), GSM 900, and DCS 1800 bands
- PC-based controller running Windows® XP provides an intuitive Graphical User Interface (GUI)
- Industry-standard USB interface enables plug-n-play networking of multiple StingRay surveillance systems if the user requires more channel capacity
- Supports targeting and real-time searching of mobile identification numbers (MIN), dialed numbers, and electronic serial numbers (ESN)
- Low-power system designed for vehicular operations



next level solutions

EXHIBIT 004	United States Patent and Trademark Office, Trademark Reg. No. 2,762,468 [StingRay] (registered Sep. 9, 2003), **Harris StingRay Product Datasheet**, *all associated trademark documents available via search at* http://tmportal.uspto.gov/external/portal/tow (last accessed: Mar. 11, 2011), p. 60-61 of 88 page compilation;
EXHIBIT 004	
EXHIBIT 004	
EXHIBIT 004	
EXHIBIT 004	
EXHIBIT 004	
EXHIBIT 004	
EXHIBIT 004	
EXHIBIT 004	
EXHIBIT 004	
EXHIBIT 004	
EXHIBIT 004	
EXHIBIT 004	
EXHIBIT 004	
EXHIBIT 004	
EXHIBIT 004	
EXHIBIT 004	
EXHIBIT 004	
EXHIBIT 004	
EXHIBIT 004	
EXHIBIT 004	
EXHIBIT 004	
EXHIBIT 004	
EXHIBIT 004	
EXHIBIT 004	
EXHIBIT 004	
EXHIBIT 004	
EXHIBIT 004	
EXHIBIT 004	
EXHIBIT 004	
EXHIBIT 004	
EXHIBIT 004	

HARRIS

[redacted]

WIRELESS products group

StingRay™

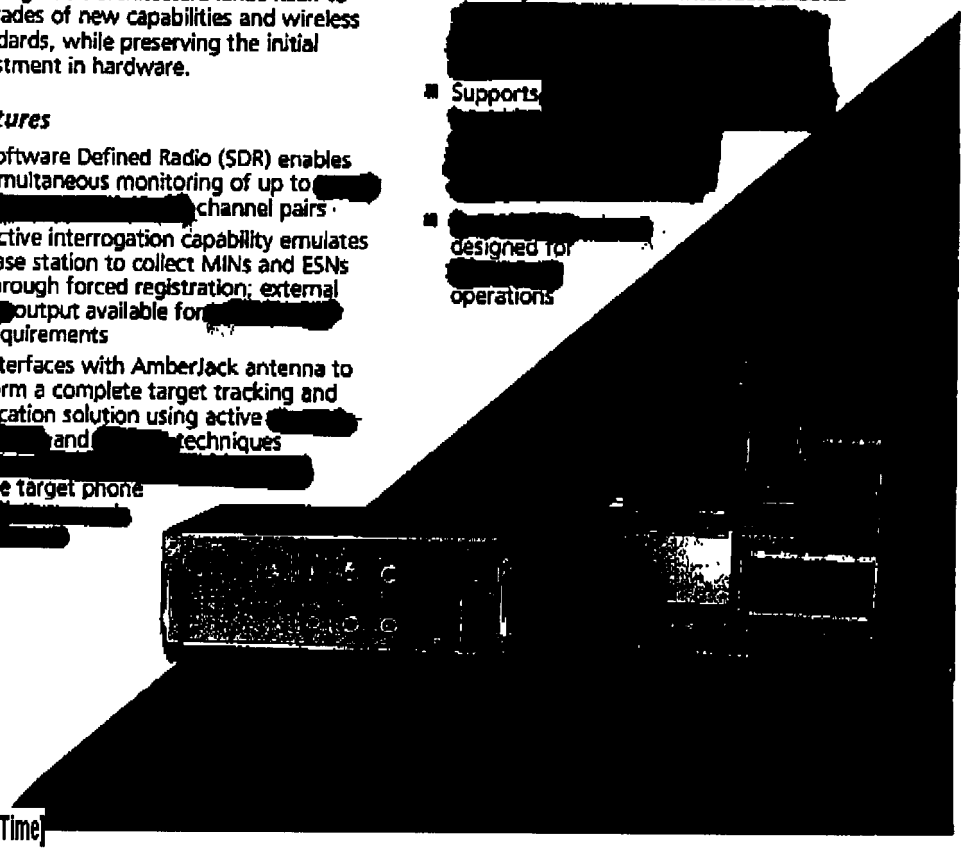
Transportable CDMA Interrogation, Tracking and Location, and Signal Information Collection System

Product Description

StingRay™ is Harris' latest offering in a long line of advanced wireless surveillance products. StingRay is a multichannel software defined radio that performs network base station surveys, Dialed Number and registration collection, mobile interrogation, and target tracking and location with Harris' AmberJack™ Direction-Finding Antenna. This low-power transportablesurveillance system is designed with the future in mind—its reconfigurable architecture lends itself to upgrades of new capabilities and wireless standards, while preserving the initial investment in hardware.

Features

- Software Defined Radio (SDR) enables simultaneous monitoring of up to [redacted] channel pairs
- Active interrogation capability emulates base station to collect MINs and ESNs through forced registration; external [redacted] output available for [redacted] requirements
- Interfaces with AmberJack antenna to form a complete target tracking and location solution using active [redacted] and [redacted] techniques [redacted] the target phone [redacted]
- Optional [redacted]
- [redacted] RF front-end provides [redacted] operation in the U.S. cellular [redacted] bands and is [redacted] reconfigured to support [redacted] bands
- PC-based controller running [redacted] provides an intuitive Graphical User Interface (GUI)
- Industry-standard USB interface enables [redacted]
- Supports [redacted]
- [redacted] designed for [redacted] operations



next level solutions

EXHIBIT C

Received from < > at 7/18/02 11:31:01 AM [Eastern Daylight Time]

USPTO StingRay Trademark [all docs.]; Reg. No. 2,762,468 [Sep. 9, 2003]; Page # 60 of 88;
Download at <http://tmportal.uspto.gov/external/portal/tow> [last accessed Mar. 11, 2011];

[redacted] *Wireless Products Group*

Standards Currently Supported

- [redacted]

Future Standards Supported

- Software reconfigurable architecture will allow for future software upgrades to support other wireless standards and capabilities

Operating Bands

- [redacted]

Transmit Capabilities

(For Interrogation and Active Tracking and Location)

- Up to [redacted] dBm output
- Interfaces with an [redacted]

Compatible Accessories

- [redacted]

Interfaces

- [redacted]
- Power
  - [redacted]

Physical Characteristics

- Housing: Standard aluminum case
- Wheeled transit case
  - Stows [redacted]
  - Conforms to airline carry-on weight and size limits

PC Controller Characteristics

- [redacted] perating system
- GUI is easily configured by user for mission scenarios
- Enables field upgrade of system firmware
- Integrated [redacted] GUI with optional [redacted]

1. Hardware is preconfigured to work in these bands. Future software upgrades will provide operation in these bands—consult Harris Wireless Products Group for availability.

Specifications are subject to change without notice.

StingRay and AmberJack are trademarks of Harris Corporation.

Windows XP is a registered trademark of Microsoft Corporation.

This product is a restricted use item and can be sold only to authorized law enforcement and government agencies. Its use shall comply with all local, state and federal statutes associated with the intercept and monitoring of oral communications. Harris Corporation assumes no liability for any misuse or improper use of the product and makes no representation as to its suitability for any specific application.

DISTRIBUTION WARNING

This brochure may be provided only to persons eligible under 18 USC 2512 (Government law enforcement agencies or communications service providers).

This brochure may only be given to U.S. citizens, permanent residents of the U.S. (green card holders), or Canadians eligible under 22 CFR 126.5.

HARRIS
next level solutions

Government Communications Systems Division | P.O. Box 37 | Melbourne, FL USA 32902-0037
1-800-358-5297 or wpg@harris.com | www.harris.com

Copyright © 2002 Harris Corporation
Printed in USA on Recyclable Paper 07/02 VPS-506690-9 d0108

USPTO StingRay Trademark [all docs.]; Reg. No. 2,762,468 [Sep. 9, 2003]; Page # 61 of 88;
Download at <http://tmportal.uspto.gov/external/portal/tow> [last accessed Mar. 11, 2011];

EXHIBIT 005

United States Patent and Trademark Office, Trademark Reg. No. 2,762,468 [StingRay] (registered Sep. 9, 2003), **Harris StingRay Product Description**, *all associated trademark documents available via search at* http://tmportal.uspto.gov/external/portal/tow (last accessed: Mar. 11, 2011), p. 10 of 88 page compilation;

Int. Cl.: 9

Prior U.S. Cls.: 21, 23, 26, 36, and 38

United States Patent and Trademark Office

Reg. No. 2,762,468
Registered Sep. 9, 2003

TRADEMARK
PRINCIPAL REGISTER

STINGRAY

HARRIS CORPORATION (DELAWARE CORPORATION)
1025 WEST NASA BOULEVARD
MELBOURNE, FL 32919

FOR: MULTI-CHANNEL, SOFTWARE-DEFINED, TWO-WAY ELECTRONIC SURVEILLANCE RADIOS FOR AUTHORIZED LAW ENFORCEMENT AND GOVERNMENT AGENCIES FOR INTERROGATING, LOCATING, TRACKING AND GATHERING INFORMATION FROM CELLULAR TELEPHONES, IN CLASS 9 (U.S. CLS. 21, 23, 26, 36 AND 38).

FIRST USE 3-2-2003; IN COMMERCE 3-2-2003.

SN 76-303,503, FILED 8-21-2001.

MELVIN AXILBUND, EXAMINING ATTORNEY

USPTO StingRay Trademark [all docs.]; Reg. No. 2,762,468 [Sep. 9, 2003]; Page # 10 of 88;
Download at <http://tmportal.uspto.gov/external/portal/tow> [last accessed Mar. 11, 2011];

EXHIBIT 006

EXHIBIT 006 (repeated 31 times in total down the left column)

United States Patent and Trademark Office, Trademark Reg. No. 2,867,227 [KingFish] (registered Jul. 27, 2004), **Harris KingFish Product Picture**, *all associated trademark documents available via search at* http://tmportal.uspto.gov/external/portal/tow (last accessed: Mar. 11, 2011), p. 7 of 67 page compilation;

REMOTE ANTENNA
USB
DF ANTENNA
EXT PA
DC INPUT
MAIN ANTENNA
MASTER POWER
KingFish

EXHIBIT 007
EXHIBIT 007
EXHIBIT 007
EXHIBIT 007
EXHIBIT 007
EXHIBIT 007
EXHIBIT 007
EXHIBIT 007
EXHIBIT 007
EXHIBIT 007
EXHIBIT 007
EXHIBIT 007
EXHIBIT 007
EXHIBIT 007
EXHIBIT 007
EXHIBIT 007
EXHIBIT 007
EXHIBIT 007
EXHIBIT 007
EXHIBIT 007
EXHIBIT 007
EXHIBIT 007
EXHIBIT 007
EXHIBIT 007
EXHIBIT 007
EXHIBIT 007
EXHIBIT 007
EXHIBIT 007
EXHIBIT 007
EXHIBIT 007
EXHIBIT 007
EXHIBIT 007
EXHIBIT 007

ATTACHED EXHIBITS
SECOND SUBMISSION OF CONSOLIDATED EXHIBITS RELATING TO DISCOVERY AND SUPPRESSION ISSUES
CR08-814-PHX-DGC

Miami, FL, USA – Legislative Files, **Harris KingFish Product Datasheet**, *available at* http://egov.ci.miami.fl.us/Legistarweb/Attachments/34771.pdf (last accessed: Mar. 9, 2011), p. 2;

HARRIS

WIRELESS products group

KingFish™ (Preliminary)

Portable CDMA Interrogation, Direction-Finding, and Collection System

Product Description

KingFish™ provides investigators with a tool that extracts the telephone number (MIN) and Electronic Serial Number (ESN) from a CDMA mobile telephone. The Active Direction-Finding (DF) capability enables location of a powered-on phone without depending on the suspect to be involved on a call. Additionally, KingFish provides passive Dialed Number Recorder (DNR) and Registration Collection capabilities. Passive operations identify calling patterns and provide information on the suspect's area of operation.

KingFish is based on a Software Defined Radio (SDR) architecture, which enables upgrades to future cellular standards, while preserving the initial investment in hardware. As initially offered, KingFish provides CDMA operation in both the Cellular and PCS bands.

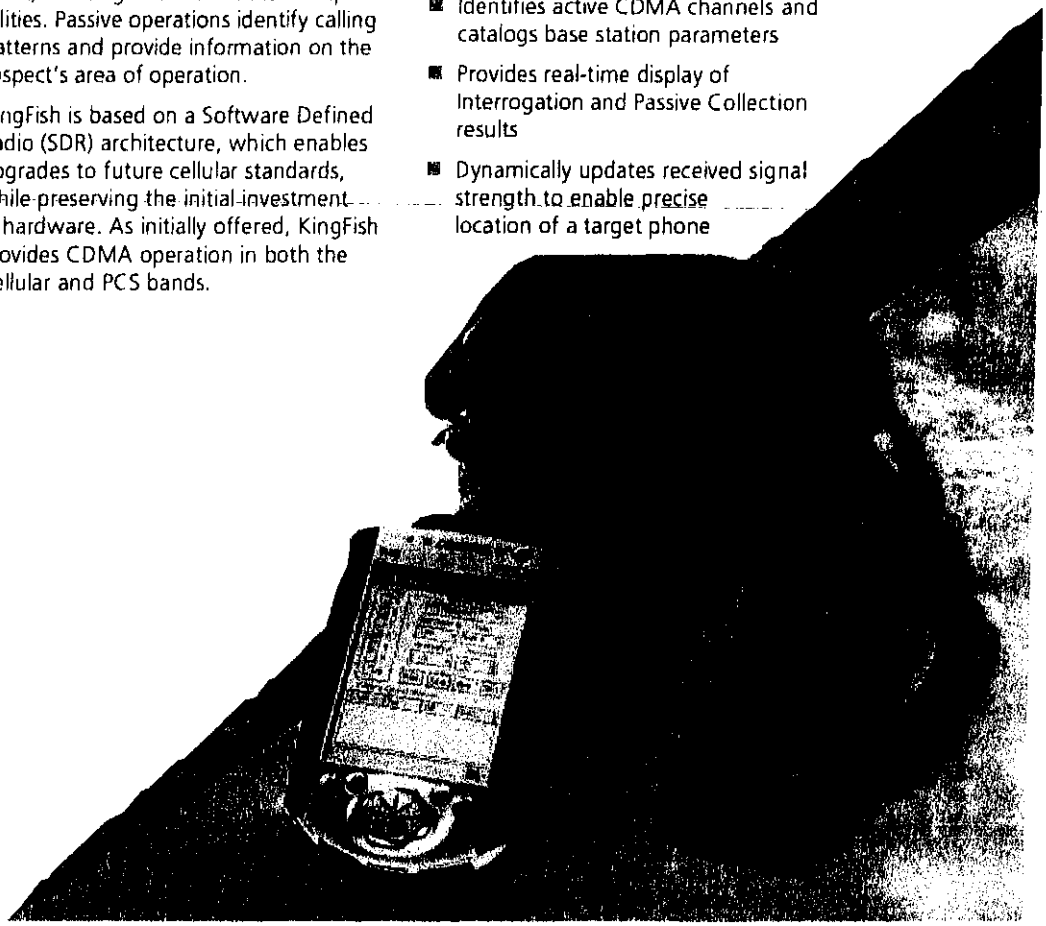
Features

Covert Packaging

- Concealed radio, antennas, and battery power supply
- Wireless remote control from commercially available Pocket PC

Intuitive Application Software

- Windows® interface
- Identifies active CDMA channels and catalogs base station parameters
- Provides real-time display of Interrogation and Passive Collection results
- Dynamically updates received signal strength to enable precise location of a target phone



next level solutions

EXHIBIT 008	United States Patent and Trademark Office, Trademark Reg. No. 2,867,227 [KingFish] (registered Jul. 27, 2004), **Harris KingFish Product Description**, *all associated trademark documents available via search at* http://tmportal.uspto.gov/external/portal/tow (last accessed: Mar. 11, 2011), p. 10 of 67 page compilation;
EXHIBIT 008	
EXHIBIT 008	
EXHIBIT 008	
EXHIBIT 008	
EXHIBIT 008	
EXHIBIT 008	
EXHIBIT 008	
EXHIBIT 008	
EXHIBIT 008	
EXHIBIT 008	
EXHIBIT 008	
EXHIBIT 008	
EXHIBIT 008	
EXHIBIT 008	
EXHIBIT 008	
EXHIBIT 008	
EXHIBIT 008	
EXHIBIT 008	
EXHIBIT 008	
EXHIBIT 008	
EXHIBIT 008	
EXHIBIT 008	
EXHIBIT 008	
EXHIBIT 008	
EXHIBIT 008	
EXHIBIT 008	
EXHIBIT 008	
EXHIBIT 008	
EXHIBIT 008	
EXHIBIT 008	

Int. Cl.: 9

Prior U.S. Cls.: 21, 23, 26, 36, and 38

United States Patent and Trademark Office

Reg. No. 2,867,227
Registered July 27, 2004

TRADEMARK
PRINCIPAL REGISTER

KINGFISH

HARRIS CORPORATION (DELAWARE CORPORATION)
1025 WEST NASA BOULEVARD
MELBOURNE, FL 32919

FOR: ELECTRONIC SURVEILLANCE TRANSCEIVERS FOR TRACKING, LOCATING AND GATHERING INFORMATION FROM CELLULAR TELEPHONES, IN CLASS 9 (U.S. CLS. 21, 23, 26, 36 AND 38).

FIRST USE 12-10-2003; IN COMMERCE 12-10-2003.

SN 76-303,814, FILED 8-23-2001.

MELVIN AXILBUND, EXAMINING ATTORNEY

USPTO KingFish Trademark [all docs.]; Reg. No. 2,867,227 [Jul. 27, 2004]; Page # 10 of 67;
Download at <http://tmportal.uspto.gov/external/portal/tow> [last accessed Mar. 11, 2011];

ATTACHED EXHIBITS
SECOND SUBMISSION OF CONSOLIDATED EXHIBITS
RELATING TO DISCOVERY AND SUPPRESSION ISSUES
CR08-814-PHX-DGC

EXHIBIT 009

Miami, FL, USA – Legislative Files, **Harris Geolocation Product Datasheet**, *available at* http://egov.ci.miami.fl.us/Legistarweb/Attachments/34771.pdf (last accessed: Mar. 9, 2011), p. 1;

HARRIS

WIRELESS products grou

Geolocation (Preliminary)

PC-Based Intelligent AMPS/TDMA and CDMA Tracking and Location

Product Description

Geolocation is a PC-based software application that allows the user to intelligently track and locate targeted AMPS/TDMA or [illegible] cellular phones in the 800 and [illegible] MHz bands. Geolocation consists of software and an external GPS receiver. Geolocation will be offered in two options: an AMPS/TDMA Option to be used in conjunction with the Harris LoggerHead™ Interrogator plus the PC Controller™ and the AmberJack™ DF Antenna; and a CDMA Option to be used in conjunction with the Harris StingRay™ system plus the AmberJack™ DF Antenna.

Geolocation provides a user-friendly, geospatially accurate mapping routine which shows on-screen the exact location of the tracking vehicle, plus Direction of Arrival (DOA) information and/or estimated range/location information on the targeted phone.

Providing a visual screen of an accurate local map, the exact location of the tracking vehicle, and the approximate location of the targeted phone, allows for a much more intelligent and expedient method for tracking and location.

Features

- User-friendly application running on Windows® 98/2000/XP provides an intuitive Graphical User Interface (GUI)
- AMPS/TDMA: Interfaces with the LoggerHead™ Handheld Interrogator plus the PC Controller™ and the AmberJack™ Direction-Finding (DF) Antenna
- CDMA: Interfaces with the StingRay™ plus the AmberJack™ Direction-Finding (DF) Antenna
- Provided GPS receiver integrates with PC running the application
- Real-time viewing of tracking vehicle location
- Real-time viewing of approximate targeted cellular phone location
- Tracking missions can be stored for post-mission analysis
- Migration path to GSM and future cellular standards[1]

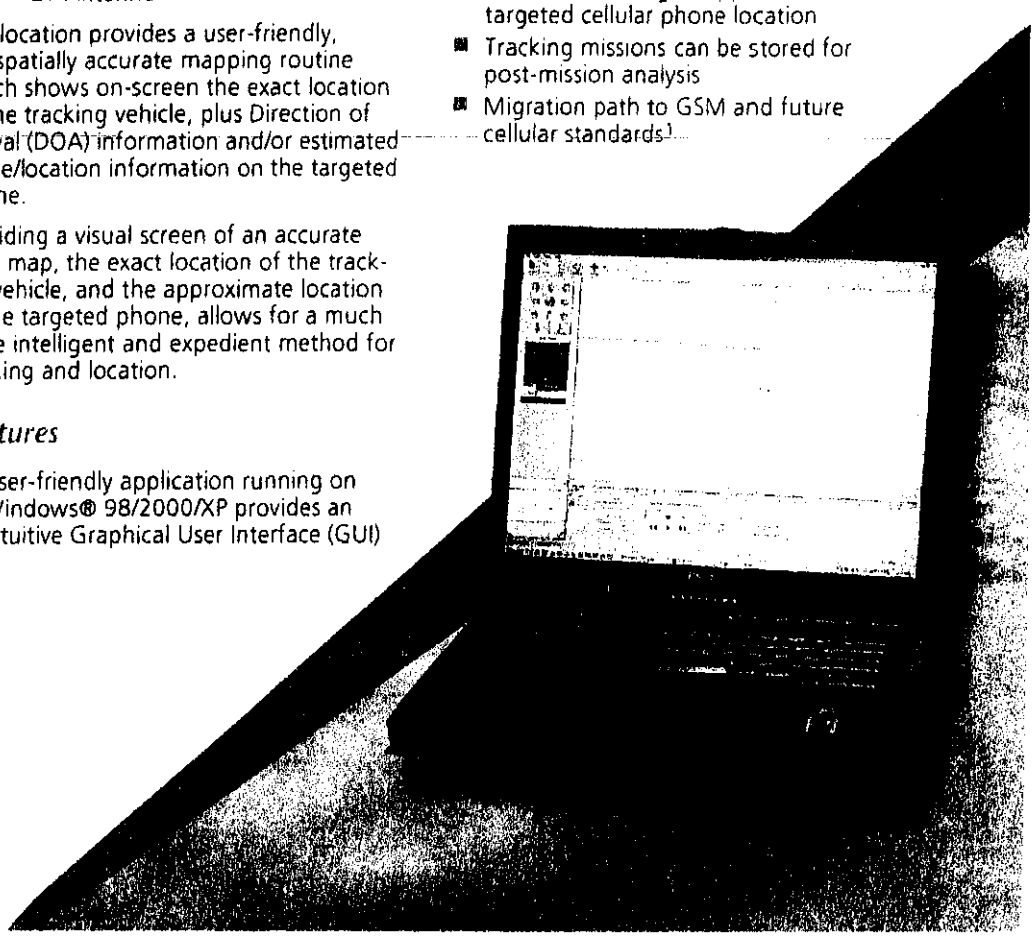


EXHIBIT 010
EXHIBIT 010
EXHIBIT 010
EXHIBIT 010
EXHIBIT 010
EXHIBIT 010
EXHIBIT 010
EXHIBIT 010
EXHIBIT 010
EXHIBIT 010
EXHIBIT 010
EXHIBIT 010
EXHIBIT 010
EXHIBIT 010
EXHIBIT 010
EXHIBIT 010
EXHIBIT 010
EXHIBIT 010
EXHIBIT 010
EXHIBIT 010
EXHIBIT 010
EXHIBIT 010
EXHIBIT 010
EXHIBIT 010
EXHIBIT 010
EXHIBIT 010
EXHIBIT 010
EXHIBIT 010
EXHIBIT 010
EXHIBIT 010
EXHIBIT 010
EXHIBIT 010

ATTACHED EXHIBITS
SECOND SUBMISSION OF CONSOLIDATED EXHIBITS RELATING TO DISCOVERY AND SUPPRESSION ISSUES
CR08-814-PHX-DGC

Miami, FL, USA – Legislative Files, **Harris AmberJack Product Datasheet**, *available at* http://egov.ci.miami.fl.us/Legistarweb/Attachments/34769.pdf (last accessed: Mar. 9, 2011), p. 2;

HARRIS

WIRELESS products group

AmberJack™

Dual-Band Direction Finding System

Product Description

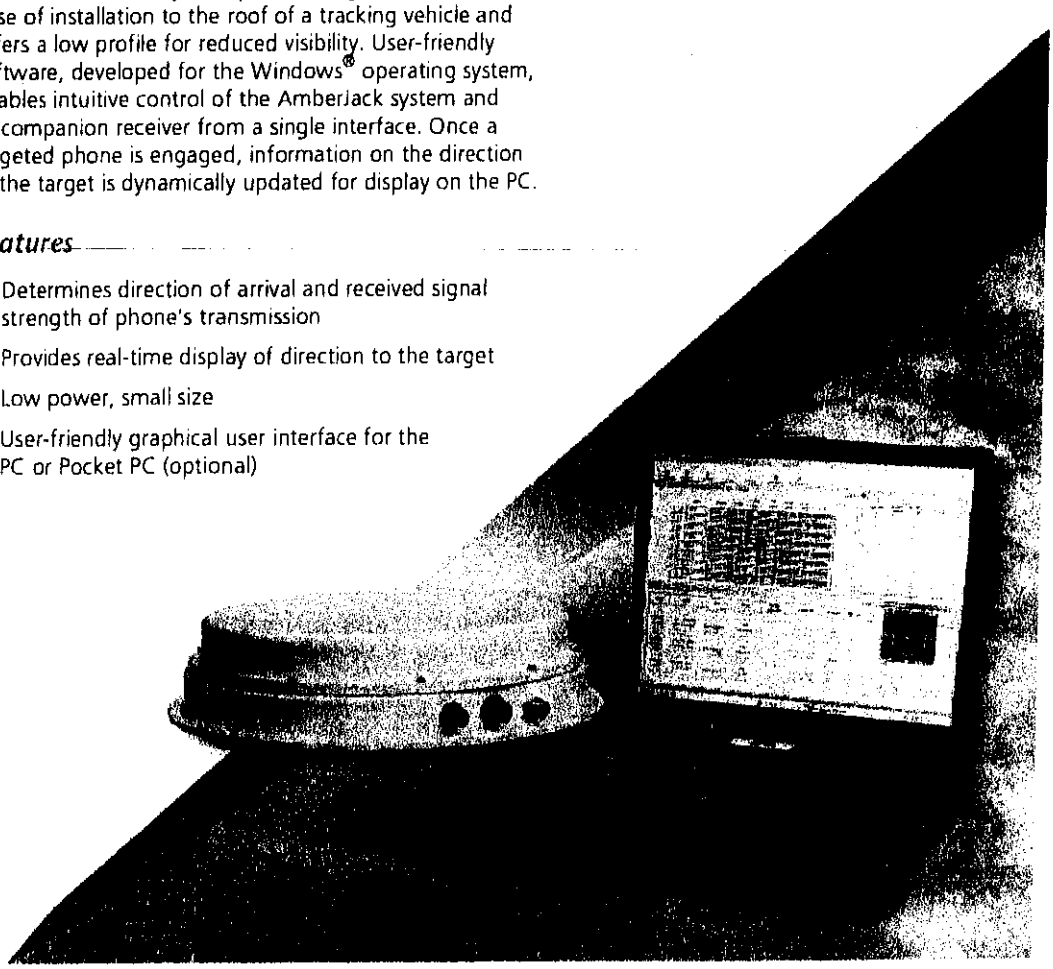
AmberJack™ is a phased array direction finding (DF) antenna system capable of tracking and locating mobile phone users. The DF antenna array is designed to operate with Harris' Loggerhead™ and StingRay™ products enabling tracking and location of AMPS, TDMA and CDMA phones. AmberJack operates in both the cellular and PCS bands.

AmberJack combines Harris' expertise in phased array antenna technology and tracking and locating systems to offer a state-of-the-art direction finding system. Beam forming technology offers a universal DF antenna for existing as well as future cellular standards.

The DF antenna array incorporates magnetic mounts for ease of installation to the roof of a tracking vehicle and offers a low profile for reduced visibility. User-friendly software, developed for the Windows® operating system, enables intuitive control of the AmberJack system and its companion receiver from a single interface. Once a targeted phone is engaged, information on the direction to the target is dynamically updated for display on the PC.

Features

- Determines direction of arrival and received signal strength of phone's transmission
- Provides real-time display of direction to the target
- Low power, small size
- User-friendly graphical user interface for the PC or Pocket PC (optional)



next level solutions

ATTACHED EXHIBITS
SECOND SUBMISSION OF CONSOLIDATED EXHIBITS
RELATING TO DISCOVERY AND SUPPRESSION ISSUES
CR08-814-PHX-DGC

EXHIBIT 011

EXHIBIT 011 (repeated 32 times down the left column)

Miami, FL, USA – Legislative Files, **Harris AmberJack Product Datasheet**, *available at* http://egov.ci.miami.fl.us/Legistarweb/Attachments/40003.pdf (last accessed: Mar. 9, 2011), p. 6-7;

HARRIS®
assuredcommunications®

Wireless Products Group

AmberJack®

Direction-Finding System

Product Description

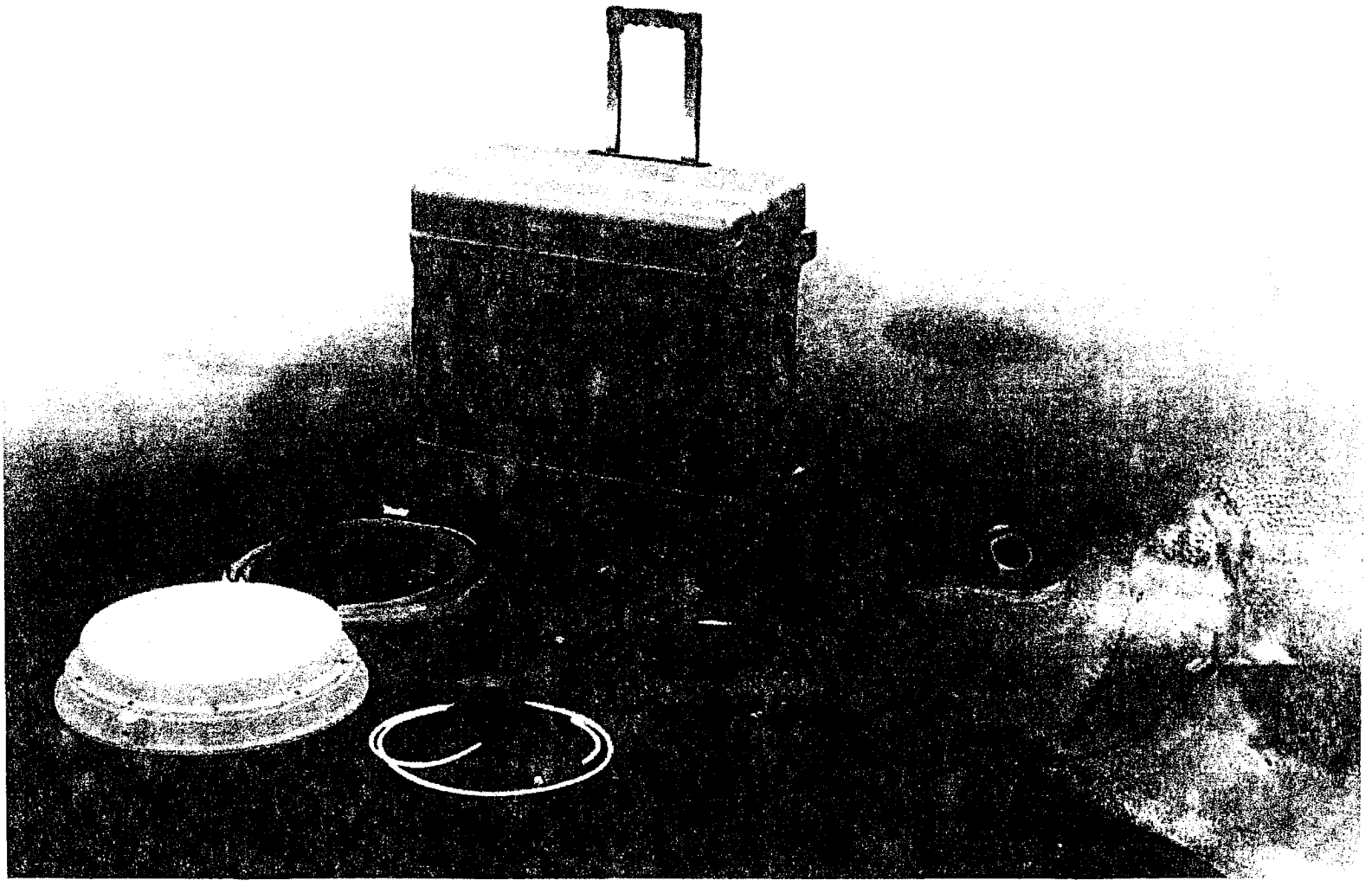
AmberJack® is a phased array direction-finding (DF) antenna system capable of tracking and locating mobile phone users and base stations. The DF antenna array is designed to operate with Harris' Gossamer®, KingFish®, StingRay®, and StingRay II® products, enabling tracking and location of targeted mobile phones, as well as base stations. AmberJack-X operates in the U.S. cellular 850 and PCS 1900 bands, and AmberJack-G operates in the EGSM 900 and DCS 1800 bands. AmberJack-W operates in all the bands above as well as iDEN™ and UMTS bands I and IV.

AmberJack combines Harris' expertise in phased array antenna technology and tracking and locating systems to offer a state-of-the-art direction-finding system. Phased array technology offers a universal DF antenna for existing, as well as future cellular standards.

The DF antenna array incorporates magnetic mounts for ease of installation on the roof of a tracking vehicle and offers a low profile for reduced visibility. User-friendly software, developed for the Windows® operating system, enables intuitive control of the AmberJack system and its companion receiver from a single interface. Once a target is engaged, information on the direction to the target is dynamically updated for display on the PC.

Operations Supported

- Locating mobile phones and base stations
- Tracking mobile phones



AmberJack®

Direction-Finding System

WIRELESS products group

Features

- Determines direction of arrival and received signal strength of a targeted mobile phone's transmission
- Determines direction of arrival and received signal strength of a targeted base station's transmission
- Provides real-time display of direction to the target
- Low power and portable
- User-friendly Graphical User Interface (GUI) for the PC

Frequency Coverage

- AmberJack-X (U.S. Cellular/PCS 1900)
  - Cellular reverse: 824–849 MHz
  - Cellular forward: 869–894 MHz
  - PCS reverse: 1850–1910 MHz
  - PCS forward: 1930–1990 MHz
- AmberJack-G (EGSM 900/DCS 1800)
  - EGSM reverse: 880–915 MHz
  - EGSM forward: 925–960 MHz
  - DCS reverse: 1710–1785 MHz
  - DCS forward: 1805–1880 MHz
- AmberJack-W (Wideband)
  - iDEN reverse: 806–825 MHz
  - iDEN forward: 851–870 MHz
  - Cellular reverse: 824–849 MHz
  - Cellular forward: 869–894 MHz
  - PCS reverse: 1850–1910 MHz
  - PCS forward: 1930–1990 MHz
  - EGSM reverse: 880–915 MHz
  - EGSM forward: 925–960 MHz
  - DCS reverse: 1710–1785 MHz
  - DCS forward: 1805–1880 MHz
  - UMTS IV reverse: 1710–1755 MHz
  - UMTS IV forward: 2110–2155 MHz
  - UMTS I reverse: 1920–1980 MHz
  - UMTS I forward: 2110–2170 MHz

External Control

- Laptop PC (Windows® XP Professional)

Power source

- 12 Vdc at 0.5 A

Physical Characteristics

- Size: D = 17", H = 4.2"
- Weight: <14 lbs

Required Accessories *(sold separately)*

Gossamer with PC Controller, StingRay system, StingRay II, or KingFish with PC Controller

Optional Accessories

Harpoon™ for DF range extension

Catalog Part Number

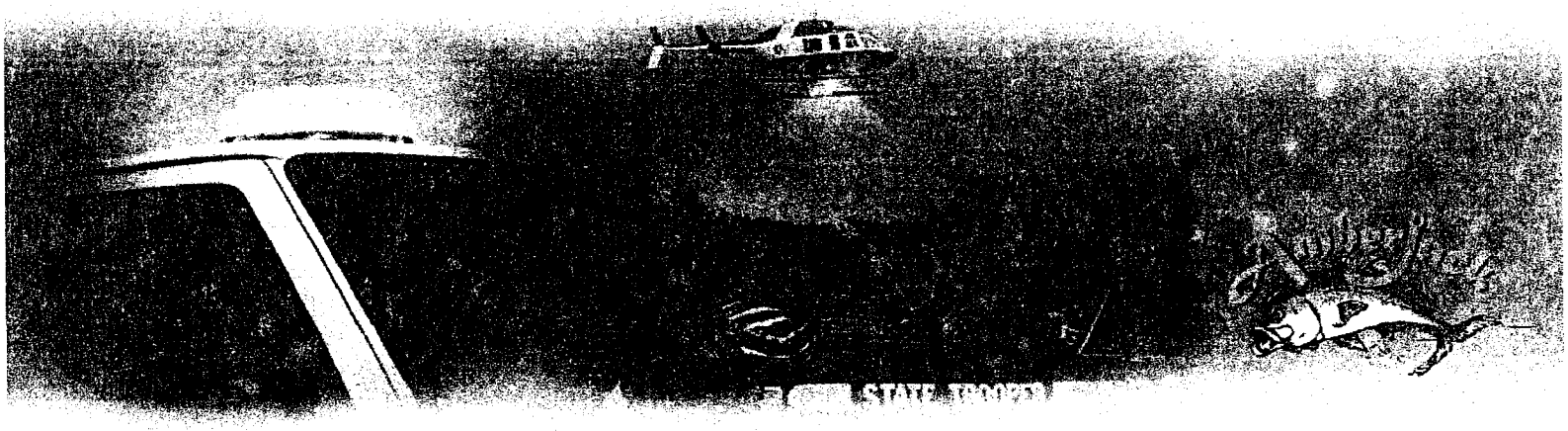
- AJ-X (AmberJack-X)
- AJ-G (AmberJack-G)
- AJ-W (AmberJack-W)

Authorized Federal Supply Service Information Technology Schedule

- SIN: 132-8 Purchase of Equipment
- SIN: 132-12 Maintenance, Repair Services and Repair Parts/Spare Parts

GSA Contract Number: GS-35F-0293J

General Services Administration Federal Supply Service products and ordering information in this Authorized FSS Information Technology Schedule Pricelist are also available on the GSA *Advantage!* System. Agencies can browse GSA *Advantage!* by accessing the GSA's home page via the Internet at *www.gsa.gov*.



Specifications are subject to change without notice. Harris is a registered trademark of Harris Corporation. AmberJack, KingFish, Gossamer, StingRay, and StingRay II are registered trademarks of Harris Corporation. Harpoon is a trademark of Harris Corporation. Windows XP Professional is a registered trademark of Microsoft Corporation. iDEN is a trademark of Motorola, Inc.

This product is a restricted use item and can be sold only to authorized law enforcement and government agencies. Its use shall comply with all local, state, and federal laws and regulations. Harris Corporation assumes no liability for any misuse or improper use of the product and makes no warranty or representation whatsoever as to its suitability for any specific application.

DISTRIBUTION WARNING

This brochure may be provided only to persons eligible under 18 USC 2512 (Government law enforcement agencies or communications service providers).

HARRIS assuredcommunications®

Government Communications Systems | P.O. Box 9800 | Melbourne, FL USA 32902-9800
1-800-358-5297 or wpg@harris.com | www.wpg.harris.com | **www.harris.com**

Copyright © 2008 Harris Corporation 07/08 514176k VPB d0105

EXHIBIT 012
EXHIBIT 012
EXHIBIT 012
EXHIBIT 012
EXHIBIT 012
EXHIBIT 012
EXHIBIT 012
EXHIBIT 012
EXHIBIT 012
EXHIBIT 012
EXHIBIT 012
EXHIBIT 012
EXHIBIT 012
EXHIBIT 012
EXHIBIT 012
EXHIBIT 012
EXHIBIT 012
EXHIBIT 012
EXHIBIT 012
EXHIBIT 012
EXHIBIT 012
EXHIBIT 012
EXHIBIT 012
EXHIBIT 012
EXHIBIT 012
EXHIBIT 012
EXHIBIT 012
EXHIBIT 012
EXHIBIT 012
EXHIBIT 012
EXHIBIT 012
EXHIBIT 012

Harris, Government Communications Systems Division, *Phased Array Antennas Brochure* (2004), *available at* http://download.harris.com/app/public_download.asp?fid=450 (last accessed: Sept. 22, 2010);

ATTACHED EXHIBITS
SECOND SUBMISSION OF CONSOLIDATED EXHIBITS RELATING TO DISCOVERY AND SUPPRESSION ISSUES
CR08-814-PHX-DGC

HARRIS®

Government Communications Systems

Phased Array Antennas

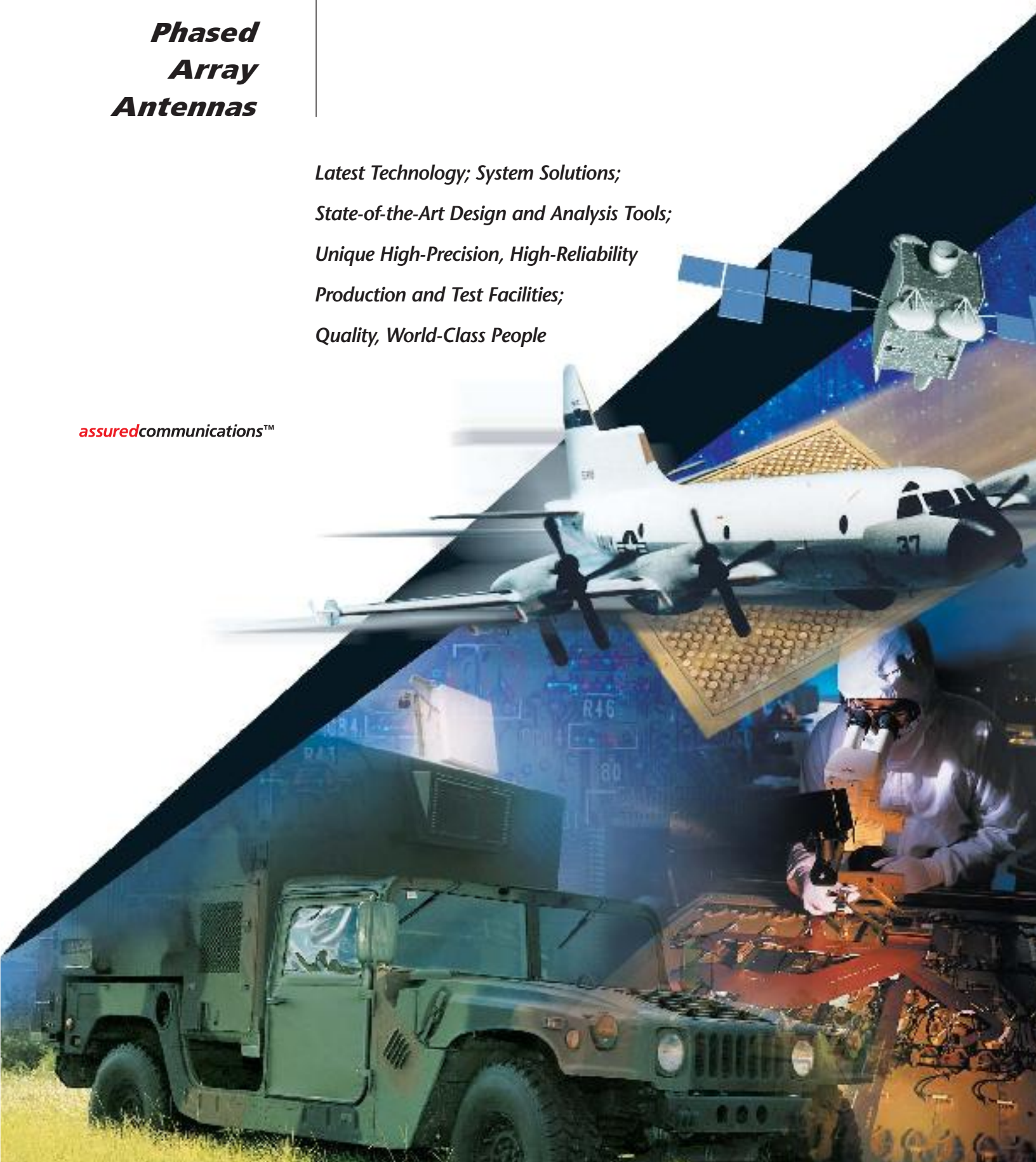
Latest Technology; System Solutions;

State-of-the-Art Design and Analysis Tools;

Unique High-Precision, High-Reliability

Production and Test Facilities;

Quality, World-Class People



assuredcommunications™

PHASED ARRAYS AT HARRIS

Harris invites you to join us as we bring the new-millennium technology of phased arrays into sharp focus for a broad range of communications and remote sensing applications. Harris specializes in providing high-performance, high-density phased array antennas.

And our investment in technology, people, design tools, and manufacturing facilities improves reliability while saving you time and money.

Harris' phased array expertise extends back to the 1960's. Today, we design and produce our phased arrays to meet the exacting requirements demanded by the harsh environments of space, airborne, ground, mobile and shipboard platforms. Where practical, we employ our commercial processes and technologies to reduce overall schedule and cost.

Our phased array experience covers a broad range of frequency bands including:

- UHF
- L-band
- S-band
- C-band
- X-band
- Ku-band
- Ka-band
- V-band

Our experience also includes many types of architectures, topologies and techniques which are available to solve your communication or remote sensing needs:

- Broadband
- Narrowband
- Conformal
- Wide or narrow scan
- Single or multiple beam
- Simplex or half/full duplex
- Spatial combining
- Adaptive nulling
- Block or tile
- Thinned

Harris has a proven track record of solving tough system problems.

From design through manufacturing and into test, we provide the expertise and the dedication to create the best system possible.

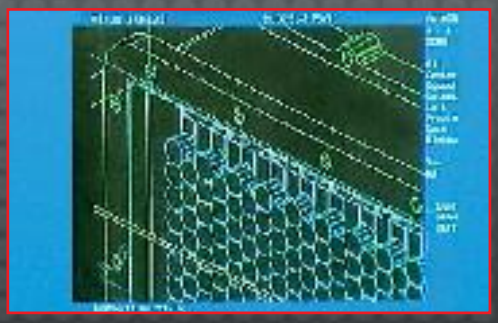
We provided the first large-scale communications phased array antenna system, with over 7,000 MMIC chips.

We have flight-demonstrated electronically steerable widescan arrays, hemispherical coverage arrays for direct data dissemination, and ruggedized phased arrays for comm-on-the-move.

We put our decades of expertise to work providing high-quality, high-performance systems at the lowest possible cost per unit of performance.

We lead the way from design through test; solving your complex problems; meeting your schedule and budget.

Systems



Design

Manufacture

Test

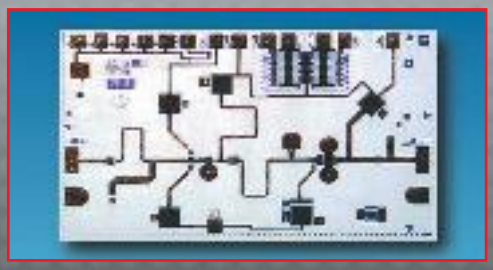
ENABLING TECHNOLOGY

Harris Corporation has been developing phased array antennas since the 1960's. We have simulation, design, test and production experience of phased arrays for surface, airborne, and space applications.

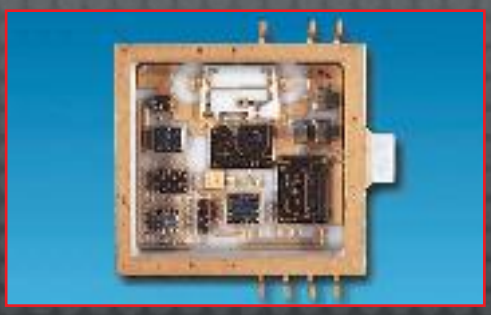
Harris has developed and employed numerous technologies to support phased array antenna design and production. These enabling technologies lead to the advanced, successful products that solve your communications and sensor needs.

Our enabling technologies include advanced packaging, adaptive algorithms, MMIC components, hybrid modules, special materials and automated panel assembly. In the space and avionics arenas, our integrated, lightweight packaging, embedded processors, thermal control and deployment mechanisms have also played a major part in our success.

Utilizing surface mount components, embedded microwave circuitry in high-density multilayer printed wiring boards and other advanced packaging techniques enables very low cost arrays.



Our use of highly efficient MMIC components improves reliability, reduces size and dc power and lowers cost.



Multilayered ceramic packages, high-density multichip modules and integrated digital, RF and power modules enable more advanced, lighter, smaller phased array antennas.

The Harris RH3000 family delivers modern 32-bit RISC processor performance for space and rad-hard applications.

Advanced packaging and design for automated manufacturing are the key technologies that Harris brings to enable affordable phased array solutions.

Our people combine their collective expertise with our expert tools to design creative phased array solutions.

We communicate the necessary feedback to help you assess the impact of your requirements on performance, schedule, and cost.

Our design and analysis tools are the best mix of commercial and custom, including: moment method, finite element, and hybrid finite element, GO/GTD, FDTD, and Physical Optics.

We precisely model the performance advantages of our phased array antennas. Three-dimensional modeling and simulation suites help ensure first pass success.

Harris calls on its people and vast resources to solve the most complex problems while meeting your budget and schedule requirements.

PHASED ARRAY ANTENNAS

Harris provides high-performance phased array antennas for space applications. Communications and remote-sensing phased array antennas are our specialty. Our antennas are designed for a wide variety of environments and applications.

Space Applications

X-Band Communications Array

- Multibeam Tx/Rx array
- Autonomous, self-contained building block
- 2.5 lbs./sq. ft. aperture

GEO MILSATCOM Ka-Band Transmit Array

- Singlebeam scans ±9°
- High data rate
- Highly efficient antenna elements and RF modules

NASA Ka-Band Transmit Array

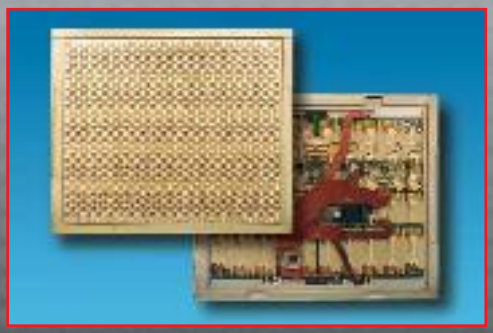
- Single beam scans ±60°
- NASA high data rate user phased array (155 Mb/s)

Multibeam Direct Downlink Array

- X-band (10 GHz)
- ±70° conical scan
- Variable EIRP
- Multiple beams (1–10)

Multibeam Ka-Band Array

- Multiple beams (10) scan ±60°
- Separate Tx/Rx apertures
- Tx optimized for NPR with multiple carriers

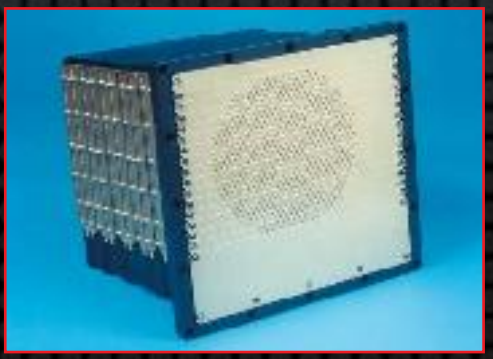


X-band communications array

GEO MILSATCOM Ka-band transmit array

NASA Ka-band transmit array

Multibeam direct downlink array



Multibeam Ka-band array

Harris phased array systems also support numerous avionics applications, both commercial and military. Entertainment systems, secure data dissemination, and airborne telemetry systems are some of our applications.

Airborne Applications

S-Band SATCOM Array

- Voice, imagery, and data reception through TDRSS S-band link
- Three panels provide hemispherical coverage

S-band SATCOM array

Airborne Telemetry System

- Ten simultaneous beams
- ± 60° Az, ± 40° El scan
- Used to track multiple high-speed targets

Airborne telemetry system

Airborne LiveTV

- Receives all available direct broadcast channels
- Simultaneous dual polarization
- Near hemispherical coverage
- Enables LiveTV to every airliner seat

Airborne LiveTV

Ground Applications

OceanNet™ C-Band SATCOM Array

- Intelsat certified
- Low transmit sidelobes
- Low profile
- Highly dynamic buoy applications
- Full acquisition, tracking, and calibration

OceanNet™

Comm-On-The-Move Array

- DSCS SATCOM or UAV link
- Supports 45 Mb/s
- Hemispherical coverage
- Adaptive null-steering (option)
- Two Rx/two Tx beams
- Full acquisition, tracking, and calibration

Comm-On-The-Move Array

PHASED ARRAY MANUFACTURING EXPERTISE

Millions of dollars have been invested to make Harris' Phased Array Antenna Manufacturing facilities the best in the world. These production facilities employ one-of-a-kind fully automated robotic systems to produce high-quality phased array antenna systems.

Phased Array Antenna Manufacturing Facility

- Over 4,000-square-feet of Class 10,000 clean room
- Space qualified automated phased array panel assembly
- Electronic paperless workflow
- High repeatability and reliability
- Shorter schedule and lower cost results

Pick and Place Tool

- Automated robotics
- Vision assisted
- High-speed, precise, reliable parts placement

These characteristics result in the lowest cost per unit of performance.

Our manufacturing facility provides the automation and the environment to produce space qualified antenna systems.

The automatic assembler provides precision controlled pick and place of microwave components, digital electronics and antenna elements.

The precision offered by our automated processes enables high-speed, reliable adhesive dispensing, parts placement and ribbon bonding provide high-density

Ribbon Bonder

- Over 200 bonds/minute
- Automated robotics
- Low temperature ribbon bonding
- Precise, repeatable interconnects

Bond Pull Tester

- 100% bond pull-testing
- Large area
- Integration with other equipment enables quick, simple repairs

Additional Manufacturing Facilities

Harris' numerous manufacturing facilities range from high-precision R&D to our large scale ISO 9002 manufacturing plant. Capabilities include:

- 300,000-square-foot high-volume manufacturing facility
- Functional and ESS screening
- ISO 9000 certified facilities
- 20,000-square-foot Advanced Space Manufacturing facility
- Class 100,000 clean room
- State-of-the-art assembly
- Advanced technology processing for space

The custom large area bonder provides fully automated, high-reliability RF interconnects.

The Harris Malabar Manufacturing Facility is a complete turnkey operation, fully capable of producing all types of electronic systems.

production of phased arrays across the frequency spectrum. Precise, repeatable packaging. The result is superior RF performance at lower production costs.

ADAPTIVE CAPABILITY

Harris' unique adaptive array processing techniques provide for automatic signal optimizing, interference suppression, and custom beam shaping.

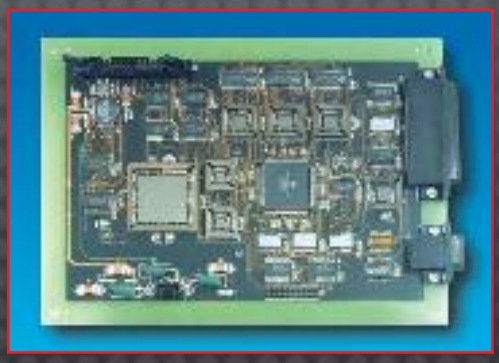
Combining multiple signal inputs into an optimized output, using our proprietary approaches and algorithms, permits enhancement of sensitivity on a desired signal while nulling interfering signals. Also, our approach enables highly accurate Angle of Arrival (AOA) estimates.

Harris uses the latest developments in digital microprocessors, DSP, digital and GaAs ASICs and optical processing techniques in combination with our perturbational algorithm approach to enhance the desired signal while minimizing the interferer.

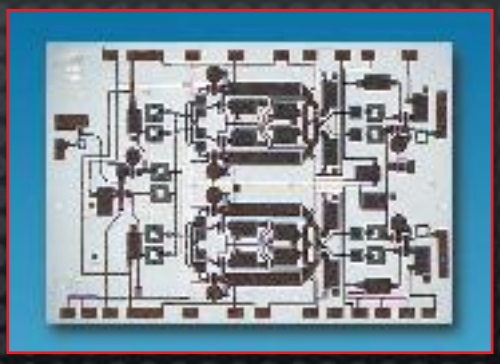
Our program experience spans nearly 20 years and over 20 programs and studies. Harris has invested in the tools, equipment, technologists and facilities to become the preeminent adaptive technology experts.

Our capabilities combine two separate processes, classical antenna array design and antenna array signal processing, to significantly improve signal-to-noise, geolocation accuracy and Angle of Arrival estimates.

Four-channel adaptive processing module . . . RF electronics.



Four-channel adaptive processing module . . . control electronics.

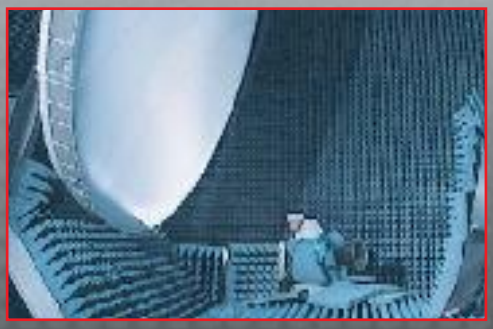


The complex weight MMIC forms the basis of our interference nulling suites.

Harris has unsurpassed facilities and capabilities for fully automated, comprehensive testing of phased array antennas.

Our compact ranges provide far field antenna pattern testing capability in a small chamber. Center frequencies up to 60 GHz are covered by automatic testing in these ranges. Also, our custom-built environmental shrouds provide temperature testing capability over wide ranges.

Harris' phased array test facility is the first of its kind to use the sophisticated Automated Antenna Measurement System which achieves high-speed, precision frequency, time, phase and pulse profiling results.



The phased array antenna testing is performed via a centralized control room.

Compact range shroud

"Harris has taken a state-of-the-art antenna test system one step further."

Copyright© 2004 Harris Corporation
01/04 508419 VPS d0038

EXHIBIT 013

Maricopa County, FL, USA – **Harris Price List** (Feb 24, 2010), *available at* http://www.maricopa.gov/materials/Awarded_Contracts/PDF/09041-c.pdf (last accessed Mar. 9, 2011), p. 21-25;

This information is provided for your convenience. Please call your Account Manager for most current pricing and availability.

WPG Product Pricing

Version S&L 2010

Effective Date: 12/7/09
Update: 2/24/10

Product Description	Part #	Domestic Pricing 1 - 15	Domestic Pricing 16+	GSA Pricing 1 - 15	GSA Pricing 16+
StingRay					
StingRay	STINGRAY	75,100	71,300	68,479	
StingRay GSM Software	SRAY-GSM-SW	22,000	20,900		
StingRay CDMA Software	SRAY-CDMA-SW	22,000	20,900		
StingRay iDEN Software	SRAY-IDEN-SW	22,000	20,900		
StingRay 2100 MHz B1 Down Converter w/ By Pass (OCONUS)	CONV-2100/1900-W/BP	19,800	18,800	18,054	
StingRay 2100 MHz B4 Down Converter w/ By Pass (CONUS)	CONV-2100/1700-W/BP	19,800	18,800	18,054	
StingRay Accessories					
StingRay Replacement Kit	SR-REPLACEMENT KIT	500			
Cable Assembly PC/USB - 6' Cable	3092524-102	196			
Cable Assembly PC/USB - 12' Cable	3092524-103	220			
Cable DC Power	3092525-101	171			
StingRay Carrying Case	RE1017HA	925			
115V Power Cord	17250	8			
Laptop PC Controller (Dell Latitude)	2009523-101	3,500			
Panasonic Toughbook Computer	2009525-101	6,500			
Adapter, DC (Laptop) (non- Charging)	DE2035-803	226			
Mouse, CMPTR (Micro Trac)	2009523-003	50			
Auto Power Adapter (8500 & D600)	2009523-002	128			
Mobile Mast 20'	OSMM-SA-20	2,990			
12' Extension Cable (TNC to N)	PE3665-144	80			
12' Extension Cable (TNC to TNC)	PE3414-144	85			
N-F to TNC-F Adapter	PE9131	48			
TNC-F to TNC-F Adapter	PE9099	28			
N-M to TNC-F Adapter	PE9090	30			
N-F to TNC-M Adapter	PE9089	28			
Directional Antenna, Yagi (GSM) Pole Mount	Y2287A-66	100			
SDR Radio Slice	3092527-201	15,000			
DC-DC Power Supply Module (SR & KF)	3092577-101	1,400			
Duplex Filter (AMPS/PCS) Stand Alone	WSA-00045	1,970			
Duplex Filter (EGSM/DCS) Stand Alone	WSA-00100	2,310			
Quad Band Mag Mount Antenex Antenna (TNC)	3174173-101	125			
15' TNC-M to TNC-F Extension Cable	CA-400UF-TMTF-15	60			
Sting Ray II					
StingRay II	STINGRAY II	148,000	140,600	134,952	
StingRay II Upgrade	STINGRAY II-UP	71,300	67,700	65,014	
StingRay II GSM Software	SRAY-II-GSM-SW	22,000	20,900		
StingRay II CDMA Software	SRAY-II-CDMA-SW	22,000	20,900		
StingRay II iDEN Software	SRAY-II-IDEN-SW	22,000	20,900		
StingRay II Accessories					
Cable Assembly PC/USB - 6' Cable	3092524-102	196			
Cable Assembly PC/USB - 12' Cable	3092524-103	220			
Laptop PC Controller (Dell Latitude)	2009523-101	3,500			
Adapter, DC (Laptop) (non- Charging)	DE2035-803	226			
Panasonic Toughbook Computer	2009525-101	6,500			
Mouse, CMPTR (Micro Trac)	2009523-003	50			
Quad Band Mag Mount Antenex Antenna (TNC)	3174173-101	125			
15' TNC-M to TNC-F Extension Cable	CA-400UF-TMTF-15	60			
Quad Band Yagi (Wedge) including 6ft cable (PE 3076-72)	3118694-201	1,300			
Cable Assembly, RF (SMA-M to RTANGM-M) 6'	PE3076-72	104			
Cable Assembly, RF (SMA-M to RTANGM-M) 12'	PE3076-144	108			
GPS Antenna	ANT-GPS-SH-SMA	50			
AC/DC Converter	ACHA1224-1936	800			
Volt Converter (Universal Plug Kit)	3142757-101	100			
StingRay II Case	RE041908HA	750			
SDR Radio Slice	3092527-201	15,000			

This information is provided for your convenience. Please call your Account Manager for most current pricing and availability.

WPG Product Pricing

Effective Date: 12/7/09
Update: 2/24/10

Version S&L 2010

KingFish				
KingFish	KINGFISH	27,800	26,400	25,349
KingFish N-Connector Upgrade	KF-N-UP	2,800	2,700	
KingFish GSM Software	KF-GSM-SW	18,100	17,200	
KingFish CDMA Software	KF-CDMA-SW	18,100	17,200	
KingFish iDEN Software	KF-IDEN-SW	18,100	17,200	
KingFish Accessories				
Kingfish Replacement Kit	KF-REPLACEMENT KIT	1,678		
Tote Bag Assembly	3100242-101	570		
Carrying Case, KingFish	RE0513HA	950		
Cable Assembly, W102 (PC USB Type A) 6' cable	3092524-102	196		
Cable DC Power	3092525-101	171		
Battery Pack (11.1V)	2014068-101	256		
Lithium-Ion Battery Charger	2014068-102	426		
Battery, Adapter, Lighter (24V, 1.5A)	VA2524	140		
Power Supply (12V, 5A)	ACHA-12501	190		
Quad Band Yagi (Wedge) including 6ft cable (PE 3076-72)	3118694-201	1,300		
Cable Assembly, RF (SMA-M to RTANGM-M) 6'	PE3076-72	104		
Cable Assembly, RF (SMA-M to RTANGM-M) 12'	PE3076-144	108		
Antenna Device, Wave, PCS/Cell (Green)	2014620-001	22		
Antenna Device, Wave, GSM (Orange)	2014620-002	22		
Antenna, ¼ Wave (2.4 GHZ) (Bluetooth)	2014628-001	18		
Backpack Carrying Case Custom (Blue)	3100242-103	450		
Backpack Carrying Case Custom (Army Digi-Camo)	3100242-104	450		
Quad Band Mag Mount Antenex Antenna (SMA)	3174173-102	125		
AmberJack				
AmberJack G	AJ-G	24,300	23,100	22,158
AmberJack X	AJ-X	24,300	23,100	22,158
AmberJack W	AJ-W	38,400	36,500	35,015
AmberJack Legacy to W Upgrade	AJL-W-UP	19,750	18,800	18,009
AmberJack X & G to W Upgrade	AJXG-W-UP	21,650	20,600	19,741
AmberJack Accessories				
Cable Assembly, DBDF Antenna, Loggerhead (12')	3088596-101	650		
Cable Assembly, DBDF Antenna, LH/Gossamer (12') (To be used in place of the	3120038-101	650		
Carrying Case	RE0512HA-2	890		
Cable Assembly, 3-Way Splitter	DC15A-3J1	170		
Eyebolt, Swivel	47621	54		
Power Cable Internal	3087877-101	73		
Tool, Eyebolt	47641/94882	15		
Webbing Assembly, 12ft.	8834T535	35		
Radome Assembly	3087882-101	1,800		
Cable Assembly, DBDF Antenna, StingRay (12')- (old PN: 3099547-101) Three	KCII/1660	800		
Cable Assembly, (35')	KCII/1672-1	1,200		
Cable Assembly, DBDF Antenna, StingRay (25')	KCII/1672	975		
Cable Assembly, DBDF Antenna, StingRay (5 meters or 16' 4") - (old PN:	KCII/1684	825		
Cable Assembly, DBDF Antenna, StingRay (50') - (old PN: 3099547-102)	KCII/1696	1,300		
CASE,CARRYING;AMBERJACK-W	RE022608HA	1,020		
4 Watt PA Kit				
Power Amp Kit	PA-KIT	3,500	3,300	
4 Watt PA Kit Accessories				
Power Amp	SM0520-36HH	2,150		
Carrying Case	RE0602HA	700		
Adapter Cable - SMA Male to SMA Male (12")	PE3377-12	58		
3 Way DC Splitter	DC15A-3J1	170		
DC Power Cable	CBLIO-00390	100		
Right Angle SMA Coax Adapter	PE9068	32		
Mounting Plate	3102393-101	52		
Adapter Cable - SMA Male to SMA Male (72")	PE3377-72	60		
Quad Band Mag Mount Antenex Antenna (SMA)	3174173-102	125		

This information is provided for your convenience. Please call your Account Manager for most current pricing and availability.

WPG Product Pricing

Effective Date: 12/7/09
Update: 2/24/10

Version S&L 2010

10 Watt PA Kit				
Power Amp Kit - 10 Watt	PA-KIT-10W	4,500	4,300	
10 Watt PA Kit Accessories				
Amplifier 10Watt	SM0822-3906	2,390		
Carrying Case	RE0118HA	700		
Adapter Cable - SMA / TNC (18") w/ Attenuator	3147080-101	108		
3 Way DC Splitter	DC15A-3J1	170		
Adapter Cable - SMA / TNC (72") w/ Attenuator	3147080-102	110		
DC Power Cable for 10-Watt PA	180-8045-66	62		
AC to DC Power Supply for 10 Watt PA	ACHA1270-1465	218		
AC to DC Power Supply for 10 Watt PA - 25 feet	CBLMS-F00416	120		
Quad Band Mag Mount Antenex Antenna (TNC)	3174173-101	125		
15' TNC-M to TNC-F Extension Cable	CA-400UF-TMTF-15	60		
Attenuator, FXD; 5DB (SMA to SMA)	BW-S5W2	50		
25 Watt PA Kits				
High Power Filtered 25W PA Kit - (800/850/1900/2100 B4)	PA-KIT-25W CONUS	11,500	10,900	10,486
High Power Filtered 25W PA Kit - (9001800/2100 B1)	PA-KIT-25W OCONUS	11,500	10,900	10,486
25 Watt PA Kit Accessories				
High Power antenna	VBC-822-M-1	800		
DC Powr Cable (CLA)	3092525-101	120		
AC/DC Power Converter	ACHA1224-2651	1,000		
DC / DC Power Cable	CBLIO-00640	200		
RF Cable	920-10027-012	250		
Carry Case	RE052809HA	900		
30 Watt PA Kits - Harpoons				
High Power Filtered 30W PA Kit- Single Band iDEN 800	PA-KIT-30W iDEN 800	16,400	15,600	14,954
High Power Filtered 30W PA Kit- Single Band 2100	PA-KIT-30W 2100	18,550	17,600	16,915
High Power Filtered 30W PA Kit- Dual Band 850/1900	PA-KIT-30W Dual-Band CONUS	20,200	19,200	18,419
High Power Filtered 30W PA Kit- Dual Band 900/1800	PA-KIT-30W Dual-Band OCONUS	20,200	19,200	18,419
30 Watt PA Kits - Harpoons Accessories				
Harpoon AC/DC Converter	ACHA2816-2597	1,200		
USB Cable Assembly	3092524-102	196		
USB to AUX Cable Assembly (Beige)	3181099-101	210		
RF Cable Assembly (Blue)	920-10027-012	210		
Harpoon Mounting Tray Assembly	3182503-101	700		
Antenna: 806-2200 MHZ Magnetic Mount	VBC-822-M-1	800		
Coax Adapter; SMA Male to TNC Female	PE9078	60		
Aux to Primary (Harpoon to SR) Cable Assy	3186799-101	210		
Aux to Primary (Harpoon to SR II) Cable Assy	3186800-101	180		
OCTOPUS				
Tactical Power Kit	OCTOPUS	20,000	19,000	18,237
OCTOPUS Accessories				
Directional Antenna, Quad Band w/Handle - *Requires P/N PE3377-72 &PE9070	SWAN80183G1W3V3	740		
Quad Band Mag Mount Antenex Antenna (TNC)	3174173-101	125		
15' TNC-M to TNC-F Extension Cable	CA-400UF-TMTF-15	60		
Quad Band Mag Mount Antenex Antenna (SMA)	3174173-102	125		
Antenna; 806-2200MHZ Magnetic Mount	VBC-822-M-1	800		
Directional Antenna, Yagi (Cell)	3084617-101	300		
Directional Antenna, Yagi (DCS/PCS)	3084618-101	300		
Directional Antenna, Yagi (GSM)	3084619-101	300		
Directional Antenna, Quad Band w/Handle w/ Attenuator - Requires P/N PE3377-	3120062-101	1,100		
Directional Antenna, Yagi (DCS/PCS) - Pole Mount	Y421812	100		
Directional Antenna, Yagi (GSM) Pole Mount	Y2287A-66	100		
Quad Band Yagi (Wedge) 6ft Cable included (PE3662-72)	3118694-101	1,300		

This information is provided for your convenience. Please call your Account Manager for most current pricing and availability.

WPG Product Pricing

Effective Date: 12/7/09
Update: 2/24/10

Version S&L 2010

Converters				
StingRay 2100 MHz B1 Down Converter w/ By Pass (OCONUS)	CONV-2100/1900-W/BP	19,800	18,800	18,054
StingRay 2100 MHz B4 Down Converter w/ By Pass (CONUS)	CONV-2100/1700-W/BP	19,800	18,800	18,054
Converter Accessories				
HA1225-1937	Adapter	210		
Controller Descriptions				
Laptop PC	2009523	3,500		
Toughbook PC	2009525	6,500		
Rugged Mini-PC	2014069	5,500		
Optional Antenna				
Directional Antenna, Quad Band w/Handle - *Requires P/N PE3377-72 &PE9070	SWAN80183G1W3V3	740		
Quad Band Mag Mount Antenex Antenna (TNC)	3174173-101	125		
15' TNC-M to TNC-F Extension Cable	CA-400UF-TMTF-15	60		
Quad Band Mag Mount Antenex Antenna (SMA)	3174173-102	125		
Antenna; 806-2200MHZ Magnetic Mount	VBC-822-M-1	800		
Directional Antenna, Yagi (Cell)	3084617-101	300		
Directional Antenna, Yagi (DCS/PCS)	3084618-101	300		
Directional Antenna, Yagi (GSM)	3084619-101	300		
Directional Antenna, Quad Band w/Handle w/ Attenuator - Requires P/N PE3377-	3120062-101	1,100		
Directional Antenna, Yagi (DCS/PCS) - Pole Mount	Y421812	100		
Directional Antenna, Yagi (GSM) Pole Mount	Y2287A-66	100		
Quad Band Yagi (Wedge) 6ft Cable included (PE3662-72)	3118694-101	1,300		
Repairs				
Repair for all WPG products not covered by warranty. Charges are $85.00/hr plus	REPAIR	TBD		
Maintenance Descriptions	**Part #**	**Domestic & Int'l**		**GSA**
Maintenance 4W PA Kit	MT-4W	500		
Maintenance 10W PA Kit	MT-10W	500		
Maintenance 25W PA Kit CONUS	MT-25WC	1,500		1,436
Maintenance 25W PA Kit OCONUS	MT-25WO	1,500		1,436
Maintenance AmberJack X	MT-AJX	3,000		2,872
Maintenance AmberJack G	MT-AJG	3,000		2,872
Maintenance AmberJack W	MT-AJW	5,000		4,786
Maintenance Converter Band 1 OCONUS w/ BP	MT-CONV1O	2,700		2,584
Maintenance Converter Band 4 CONUS w/ BP	MT-CONV4C	2,700		2,584
Maintenance Harpoon 2100	MT-HARP21	2,000		1,914
Maintenance Harpoon CONUS	MT-HARPC	2,000		1,914
Maintenance Harpoon iDEN	MT-HARPI	2,000		1,914
Maintenance Harpoon OCONUS	MT-HARPO	2,000		1,914
Maintenance KingFish	MT-KF	4,000		3,829
Maintenance Octopus	MT-OCT	2,700		2,584
Maintenance StingRay	MT-SR	11,000		10,529
Maintenance StingRay II	MT-SRII	22,000		21,058
Training Descriptions	**Part #**	**Per Description**		
Training - Melbourne	TRAIN-MLB	4,000		
Training - Melbourne 1-Day Course	TRAIN-MLB-1	2,500		
Training - Florida	TRAIN-FL	4,300		
Training - East Coast	TRAIN-EC	6,000		
Training - East Coast 1-Day Course	TRAIN-EC-1	3,750		
Training - West Coast	TRAIN-WC	9,000		
Training - West Coast 1-Day Ciurse	TRAIN-WC-1	6,000		

This information is provided for your convenience. Please call your Account Manager for most current pricing and availability.

WPG Product Pricing

Version S&L 2010

Effective Date: 12/7/09
Update: 2/24/10

WPG Contact Information:

Michael Dillon
Federal, State and Local Law Enforcement
(571) 246-7450
michael.dillon@harris.com

Rich Roosa
DoD, SOCOM, International, Federal Intelligence
Ph: (321) 309-7430
Cell: (321) 223-9551
richard.roosa@harris.com

Lin Vinson
ARMY, National Security, Federal Intelligence
(321) 258-2583
lin.vinson@harris.com

Susan McCreery
Sales/Support
321-309-7459 (Office)
321-258-9631 (BlkBry)
321-409-6975 (fax)
www.wpg.harris.com
www.premier.harris.com/wpg
susan.mccreery@harris.com

EXHIBIT 014

Miami, FL, USA – Legislative Files, **Harris GCSD Price List** (Sep. 2008) (Nov. 29, 2006), *available at* http://egov.ci.miami.fl.us/Legistarweb/Attachments/48000.pdf (last accessed: Mar. 9, 2011), p. 4;

HARRIS GCSD
PRICE LIST
Effective September 2008
All price quotes are in USD ($)

****This price list supersedes all previous price lists. Prices and products are subject to change without notice. Products are subject to discontinuation without notice.****

HARRIS Wireless Products Group
PO Box 9800
Melbourne, Florida 32902
1-800-FL8-LAWS (1-800-358-5297) Fax: 321-309-7437

HARRIS Wireless Products Group
PO Box 9800
Melbourne, Florida 32902
1-800-FL8-LAWS (1-800-358-5297) Fax: 321-309-7437

AmberJack®

MODEL NUMBER	DESCRIPTION	PRICE 1 to 15 Units	PRICE 16+ Units
AJ-G	**The AmberJack-G DF Antenna** is a phased array direction-finding (DF) antenna system capable of tracking and locating mobile phone users and base stations Forward and Reverse in the GSM 900 and 1800 MHz Bands.*	$ 24,300	$ 23,100
AJ-X	**The AmberJack-X DF Antenna** is a phased array direction-finding (DF) antenna system capable of tracking and locating mobile phone users and base stations Forward and Reverse in the GSM 800 and 1900 MHz Bands.*	$ 24,300	$ 23,100
AJ-W	**The AmberJack-W DF Antenna** is a wideband phased array direction-finding (DF) antenna system capable of tracking and locating mobile phone users and base stations Forward and Reverse in the frequency bands from 800MHz to 2100 MHz*	$ 38,400	$ 36,500
AJ-GUP	**AmberJack-G DF Antenna Upgrade.** Upgrades the legacy AJ-DF antenna to the AJ-G antenna.	$ 13,000	$ 12,400
AJ-XUP	**AmberJack-X DF Antenna Upgrade.** Upgrades the legacy AJ-DF antenna to the AJ-X antenna.	$ 9,000	$ 8,600
AJ-WUG	**AmberJack-W DF Antenna Upgrade.** Upgrades the legacy AJ-DF antenna, AJ-X or AJ-G antenna to the AJ-W antenna.	$ 18,000	$ 17,100
	** Requires PC Controller Software for Gossamer Operations.*		

AmberJack Accessories		PRICE
3088596-101	Cable Assembly, DBDF Antenna, Loggerhead (12')	$ 650
3120038-101	Cable Assembly, DBDF Antenna, LH/Gossamer (12') (To be used in place of the 3088596-101 for both LH and Gossamer)	$ 650
KCII/1660	Cable Assembly, DBDF Antenna, StingRay (12')- (old PN: 3099547-101)	$ 800
RE0512HA-2	Carrying Case	$ 890
DC15A-3J1	Cable Assembly, 3-Way Splitter	$ 170
47621	Eyebolt, Swivel	$ 54
3087877-101	Power Cable Internal	$ 73
47641/94882	Tool, Eyebolt	$ 15
8834T561	Webbing Assembly, 12ft.	$ 35
3087882-101	Radome Assembly	$ 1,800
KCII/1672	Cable Assembly, DBDF Antenna, StingRay (25')	$ 975
KCII/1684	Cable Assembly, DBDF Antenna, StingRay (5 meters or 16' 4") - (old PN: 3099547-103)	$ 825
KCII/1696	Cable Assembly, DBDF Antenna, StingRay (50') - (old PN: 3099547-102)	$ 1,000

HARRIS Wireless Products Group
PO Box 9800
Melbourne, Florida 32902
1-800-FL8-LAWS (1-800-358-5297) Fax: 321-309-7437

HARRIS

EFFECTIVE: SEPTEMBER, 2008
HARRIS PROPRIETARY INFORMATION
DO NOT DISTRIBUTE

StingRay®			
MODEL NUMBER	DESCRIPTION	PRICE 1 to 15 Units	PRICE 16+ Units
STINGRAY	**StingRay (4 module)** – 1-CH Xmit Interrogation and Direction Finding Transportable Unit.	$ 75,100	$ 71,300
SRAY-GSM-SW	**StingRay – GSM Software Package**	$ 22,000	$ 20,900
SRAY-CDMA-SW	**StingRay – CDMA Software Package**	$ 22,000	$ 20,900
SRAY-IDEN-SW	**StingRay – iDEN Software Package**	$ 22,000	$ 20,900
SRAY-UMTS-SW	**StingRay – UMTS Software Package**	N/C	N/C
SRAY-GSM-SW-INTCP	**StingRay -- GSM Intercept Software Package without S/C**	$ 27,400	$ 26,000
SRAY-GSM-SW-INTCP-SC	**StingRay -- GSM Intercept Software Package with S/C** (Restricted Sales only Federal Customer)	$ 50,000	$ 25,000
UMTS-B1-CONV	**StingRay 2100/1900MHz Down Converter**	$ 16,000	$ 15,200
UMTS-B4-CONV	**StingRay 2100/1700MHz Down Converter**	$ 16,000	$ 15,200
AIRBRN-KIT-CONUS	**Airborne DF Kit CONUS**	$ 9,000	$ 8,550
StingRay II®			
STINGRAY II	**StingRay II** – 4-CH Multi-Xmit Interrogattion and Direction Finding Transportable Unit.	$ 148,000	$ 140,600
STINGRAY II-UP	**StingRay II** – StingRay to StingRay II Upgrade	$ 65,000	$ 61,800
SRAY II-GSM-SW	**StingRay – GSM Software Package**	$ 22,000	$ 20,900
SRAY II-CDMA-SW	**StingRay – CDMA Software Package**	$ 22,000	$ 20,900
SRAY II-IDEN-SW	**StingRay – iDEN Software Package**	$ 22,000	$ 20,900
SRAY II-GSM-SW-INTCP	**StingRay -- GSM Intercept Software Package**	$ 27,400	$ 26,000
SRAY II-GSM-SW-INTCP-SC	**StingRay -- GSM Intercept Software Package with S/C** (Restricted Sales only Federal Customer)	$ 50,000	$ 25,000
SRAY II-UMTS-SW	**StingRay – UMTS Software Package**	N/C	N/C

StingRay Accessories		PRICE
3092524-102	Cable Assembly PC/USB - 6' Cable	$ 196
3092524-103	Cable Assembly PC/USB - 12' Cable	$ 220
3092525-101	Cable DC Power	$ 171
RE1017HA	Carrying Case	$ 925
17250	115V Power Cord	$ 8
2009523-101	Laptop PC Controller (Dell Latitude D630)	$ 3,500
2009525-101	Panasonic Toughbook Computer	$ 6,500
DE2035-803	Adapter, DC (Laptop) (non- Charging)	$ 226
2009523-003	Mouse, CMPTR (Micro Trac)	$ 50
2009523-002	Auto Power Adapter (8500 & D600)	$ 128
OSMM-SA-20	Mobile Mast 20'	$ 2,990
PE3665-144	12' Extension Cable (TNC to N)	$ 80
PE3414-144	12' Extension Cable (TNC to TNC)	$ 85
PE9131	N-F to TNC-F Adapter	$ 48
PE9099	TNC-F to TNC-F Adapter	$ 28
PE9090	N-M to TNC-F Adapter	$ 30
PE9089	N-F to TNC-M Adapter	$ 28

HARRIS Wireless Products Group
PO Box 9800
Melbourne, Florida 32902
1-800-FL8-LAWS (1-800-358-5297) Fax: 321-309-7437

StingRay Accessories continued…			**PRICE**
Y2287A-66	Directional Antenna, Yagi (GSM) Pole Mount	$	100
FPPA-400	Field Portable Power Adapter (Military Vehicles)	$	2,900
FPPS-375	Field Portable Power Source (Battery Pack)	$	1,700
FPACPS	Field Portable AC Power Source	$	900
3092527-201	SDR Radio Slice	$	15,000
3092577-101	DC-DC Power Supply Module (SR & KF)	$	1,400
WSA-00045	Duplex Filter (AMPS/PCS) Stand Alone	$	1,970
WSA-00100	Duplex Filter (EGSM/DCS) Stand Alone	$	2,310
3174173-101	Quad Band Mag Mount Antenex Antenna (TNC)	$	125

HARRIS

KingFish®			
MODEL NUMBER	**DESCRIPTION**	**PRICE** 1 to 15 Units	16+ Units
KINGFISH	**KingFish** – Man Portable Interrogation and Direction Finding Unit for the CDMA waveform	$ 27,800	$ 26,400
KF-GSM-SW	**KingFish** – GSM Software Package	$ 18,100	$ 17,200
KF-CDMA-SW	**KingFish** – CDMA Software Package	$ 18,100	$ 17,200
KF-IDEN-SW	**KingFish** – iDEN Software Package	$ 18,100	$ 17,200
KF-UMTS-SW	**KingFish** – UMTS Software Package	N/C	N/C
KingFish Accessories		**PRICE**	
3100242-101	Tote Bag Assembly	$ 570	
RE0513HA	Carrying Case, KingFish	$ 950	
3092524-102	Cable Assembly, W102 (PC USB Type A) 6' cable	$ 196	
3092525-101	Cable DC Power	$ 171	
2014068-101	Battery Pack (11.1V)	$ 256	
2014068-102	Lithium-Ion Battery Charger	$ 426	
VA2524	Battery, Adapter, Lighter (24V, 1.5A)	$ 140	
ACHA-12501	Power Supply (12V, 5A)	$ 190	
3118694-201	Quad Band Yagi (Wedge) including 6ft cable (PE 3076-72)	$ 1,300	
PE3076-72	Cable Assembly, RF (SMA-M to RTANGM-M) 6'	$ 104	
PE3076-144	Cable Assembly, RF (SMA-M to RTANGM-M) 12'	$ 108	
2014620-001	Antenna Device, Wave, PCS/Cell (Green)	$ 22	
2014628-001	Antenna, ¼ Wave (2.4 GHZ) (Bluetooth)	$ 18	
2014629-002	Antenna Device, Wave, GSM (Orange)	$ 22	
3100242-103	Backpack Carrying Case Custom (Blue)	$ 660	
3100242-104	Backpack Carrying Case Custom (Army Digi-Camo)	$ 660	
3174173-102	Quad Band Mag Mount Antenex Antenna (SMA)	$ 125	

HARRIS

PC Controllers

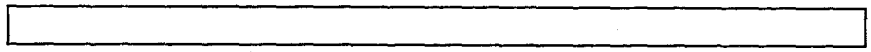
MODEL NUMBER	DESCRIPTION	PRICE
2009523-101	Laptop PC Controller (Dell Latitude D630)	$ 3,500
2015651-101	Mini PC Controller (OQO)	$ 3,200
2014069-101	Rugged Mini PC Controller (GD Go Book)	$ 4,900
3084625-101	Laptop Computer, Lightweight, Low Power, 12" Screen	$ 3,000
2009525-101	Panasonic Toughbook Computer	$ 6,500
PC Controller Accessories		**PRICE**
3058870-101	Serial Cable	$ 40
2009523-003	Mouse, CMPTR (Micro Trac)	$ 50
2009523-002	Auto Power Adapter (8500 & D600)	$ 128

Harpoon High Powered Amp 30 Watt Filtered

MODEL NUMBER	DESCRIPTION	PRICE	
		1 to 15 Units	16+ Units
PA-KIT-30W iDEN 800	High Powered Filtered 30W PA Kit - Single Band iDEN 800	$ 14,000	$ 13,300
PA-KIT-30W 2100	High Powered Filtered 30W PA Kit - Single Band UMTS 2100	$ 16,000	$ 15,200
PA-KIT-30W Dual-Band CONUS	High Powered Filtered 30W PA Kit - Dual Band 850/1900	$ 17,500	$ 16,600
PA-KIT-30W Dual-Band OCONUS	High Powered Filtered 30W PA Kit - Dual Band 900/1800	$ 17,500	$ 16,600
3184472-101	Harpoon Diplexer Kit (Use w/SR I)	$ 650	$ 650
	Need Mag Mount Antenna Specified		

UMTS Band Converters

MODEL NUMBER	DESCRIPTION	PRICE	
		1 to 15 Units	16+ Units
CONV-2100/1700	UMTS Band IV -AWS Converter	$ 16,000	$ 15,200
CONV-2100/1900	UMTS Band I Converter	$ 16,000	$ 15,200



HARRIS Wireless Products Group
PO Box 9800
Melbourne, Florida 32902
1-800-FL8-LAWS (1-800-358-5297) Fax: 321-309-7437

EXHIBIT 015

Durham, NC, USA - City Council Agenda No. 7503, **Harris Sole Source Vendor Letter** (Sept. 29, 2010), *available at* http://www.durhamnc.gov/agendas/2010/cws20110103/251951_7503_342363.pdf (last accessed Mar. 9, 2011);

HARRIS

HARRIS CORPORATION

Government Communications Systems Division
Wireless Products Group
4100 Lafayette Center Drive
Chantilly, VA USA 20151
phone 1-571-246-7450
e-mail: michael.dillon@harris.com
www.harris.com

September 29, 2010

Kisha Ethridge
Grants Manager
Durham Police Department
505 West Chapel Hill St.
Durham, NC 27701

RE: RayFish® Sole Source Justification

Harris Government Communications Systems Division, via its Wireless Products Group (WPG) in Melbourne, FL, offers a comprehensive line of wireless surveillance and tracking equipment, plus training and maintenance, for exclusive utilization by Government and Law Enforcement Agencies. Harris WPG developed and owns the equipment designs, but does sub-contract the electronic board assemblies, functional testing of those assemblies, and chassis integration. Harris WPG adds application specific, proprietary software, and conducts final testing on the chassis prior to shipment to the customer. Harris WPG has also developed specialized training courses for the operation and use of the RayFish equipment.

The Harris RayFish® product line includes the StingRay II, StingRay, and KingFish systems, which are compatible with the CDMA2000, GSM, and iDEN (Nextel) protocols. The Harris StingRay and KingFish systems are the only cooperative portable/man-portable standard +12VDC powered/battery powered multi-protocol surveillance systems currently available. When interfaced with the optional Harris AmberJack DF antenna, supported mapping software, laptop PC controller, and the Harris 25-Watt power amplifier kit, the StingRay can perform vehicular-based operations. The transportability and standard +12VDC vehicular power features of the Harris StingRay and AmberJack, and the battery-powered features of the KingFish are unique for tactical mission needs.

The StingRay and KingFish are quoted with software and accessories that are required in order to perform missions. These include the cable assemblies, power supplies, antennas, laptop PC controller, power amplifiers, handheld DF antenna, AmberJack DF antenna, and protocol software.

Harris also sells training on the use of the RayFish product line and accessories. Standard training sessions are 2 days per class with a maximum class size of 4 students. One-year maintenance agreements are included with all Harris WPG Products. Maintenance agreements include the following:

- Customer telephone support (8AM – 6PM EST)
- Hardware warranty
- Notification and access to software upgrades as they are released

Harris WPG is your only source and distributor for the StingRay II, StingRay and AmberJack vehicular-based systems, and the KingFish man-portable and dual-mode systems, and compatible accessories, authorized training and maintenance. Harris may provide equipment through a designated vehicle integrator when needed and arranged.

If you require any additional information, please don't hesitate to call me at (571) 246-7450.

Sincerely,

Michael E. Dillon
Major Account Manager Wireless Products Group
Harris Corporation

EXHIBIT 016

Miami, FL, USA – Legislative Files, **Harris Sole Source Vendor Letter** (Nov. 29, 2006), *available at* http://egov.ci.miami.fl.us/Legistarweb/Attachments/34768.pdf (last accessed: Mar. 9, 2011), p. 1;

HARRIS

HARRIS CORPORATION

Government Communications
Systems Division
Wireless Products Group
Post Office Box 9800
Melbourne, FL USA 32902-9800
phone 1-800-358-5297
fax 1-321-309-7437

www.harris.com

Date: 29 November 2006

To: City of Miami PD – Manuel Diaz

From: Harris Wireless Products Group

REF: KingFish, KingFish GSM S/W, Pocket PC GSM S/W & Training Sole Source Justification

Harris Government Communications Systems Division, via its Wireless Products Group (WPG) in Melbourne, FL, offers a comprehensive line of cellular surveillance and tracking equipment for exclusive utilization by Government and Law Enforcement Agencies. Harris WPG developed and owns the design, but does sub-contract the electronic board assemblies, the functional testing of those assemblies, and the integration into the final equipment chassis. Harris WPG adds application specific S/W and conducts final testing on this chassis prior to shipping to the end-item customer.

The KingFish system is the only man-portable battery powered CDMA & GSM Interrogation, Active Location, and Signal Information Collection system currently available. KingFish is compatible with CDMA commercial standards IS-95A, IS-95-B, TSB74, and J-STD-008 in the U.S. 800 and 1900 MHz bands. A GSM S/W upgrade package (for the KingFish and its Pocket PC) is available for purchase that will allow operation against the GSM standard in the U.S. 800 and 1900 MHz bands (as well as the overseas 900 MHz E-GSM and DCS 1800 MHz bands). KingFish can also be powered via standard automotive +12V DC or standard 110VAC. The man-portability and battery power features of the Harris KingFish product are unique for tactical mission needs, allowing the user to perform passive collection, active interrogation and active location while on foot (i.e., inside a multi-story building, or outside in rough terrain).

The KingFish is delivered with all the accessories necessary to perform man-portable active location, interrogation and passive collection technical investigations on the CDMA & GSM cellular formats. Harris also sells training on the use of the KingFish. Training sessions are 2 days per class with a maximum class size of 4 students. One training class is required per product, and per cellular protocol.

Harris WPG is your only source for the KingFish, KingFish GSM S/W, KingFish Pocket PC GSM S/W and associated training.

One-year maintenance agreements are included with all Harris WPG Products. A Maintenance Agreement includes:

- Customer Telephone Support (8AM – 6PM EST) @ 1-800-358-5297
- Warranty on hardware
- Notification of and free access to S/W upgrades as they are released (applies to purchased protocols only)

Upon expiration of the first-year Maintenance Agreement, customers may extend their coverage another 12 months by purchasing an Extended Annual Maintenance Agreement at 15% of the original purchase price of their cellular product. These can then be renewed annually thereafter for the same 15% fee.

If you require any additional information, please feel free to contact our office at (800) 358-5297 or you can call my direct line at (321) 309-7430.

Sincerely,

Richard F. Roosa
Manager Advanced Programs
Harris Corporation
Wireless Products Group

ATTACHED EXHIBITS
SECOND SUBMISSION OF CONSOLIDATED EXHIBITS
RELATING TO DISCOVERY AND SUPPRESSION ISSUES
CR08-814-PHX-DGC

EXHIBIT 017

EXHIBIT 017
EXHIBIT 017
EXHIBIT 017
EXHIBIT 017
EXHIBIT 017
EXHIBIT 017
EXHIBIT 017
EXHIBIT 017
EXHIBIT 017
EXHIBIT 017
EXHIBIT 017
EXHIBIT 017
EXHIBIT 017
EXHIBIT 017
EXHIBIT 017
EXHIBIT 017
EXHIBIT 017
EXHIBIT 017
EXHIBIT 017
EXHIBIT 017
EXHIBIT 017
EXHIBIT 017
EXHIBIT 017
EXHIBIT 017
EXHIBIT 017
EXHIBIT 017
EXHIBIT 017
EXHIBIT 017
EXHIBIT 017
EXHIBIT 017
EXHIBIT 017

Miami, FL, USA – Legislative Files, **Harris Sole Source Letter** (Aug. 25, 2008), *available at* http://egov.ci.miami.fl.us/Legistarweb/Attachments/40003.pdf (last accessed: Mar. 9, 2011), p. 2;

HARRIS

HARRIS CORPORATION

Government Communications
Systems Division
Wireless Products Group
P.O. Box 9800
Melbourne, FL USA 32902-9800
phone 1-321-309-7773

www.harris.com

August 25, 2008

To: Raul Perez, City of Miami PD

RE: StingRay and KingFish Sole Source Justification

Harris Government Communications Systems Division, via its Wireless Products Group (WPG) in Melbourne, FL, offers a comprehensive line of cellular surveillance and tracking equipment, plus training and maintenance, for exclusive utilization by Government and Law Enforcement Agencies. Harris WPG developed and owns the equipment designs, but does sub-contract the electronic board assemblies, functional testing of those assemblies, and chassis integration. Harris WPG adds application specific, proprietary software, and conducts final testing on the chassis prior to shipment to the customer. Harris WPG has also developed specialized training courses for the operation and use of the StingRay and KingFish equipment.

The Harris StingRay and KingFish systems are compatible with the CDMA standard in the 800 MHz and 1900 MHz frequency bands, the GSM standard in the 800 MHz, 900 MHz, 1800 MHz, and 1900MHz frequency bands, the iDEN (Nextel) standard in the 800 MHz and 850 MHz frequency bands, the UMTS standard in the 800 MHz and 1900 MHz frequency bands, and, with optional converter equipment, the UMTS standard in the 2100 MHz frequency band.

The Harris StingRay and KingFish vehicular-based systems are the only portable standard +12VDC powered CDMA, GSM, UMTS, and iDEN interrogation, tracking and location, and signal information collection system currently available. When interfaced with the optional Harris AmberJack direction-finding (DF) antenna(s) (or handheld DF antenna for iDEN and UMTS), Tarpon software, laptop PC controller, and Harpoon amplifier kits, the StingRay can perform vehicular-based DF operations on the CDMA, GSM, UMTS, and iDEN cellular formats. The transportability and standard +12VDC vehicular power features of the Harris StingRay and KingFish products are unique for tactical mission needs.

The StingRay and KingFish are quoted with software and accessories that are required in order to perform missions on the CDMA, GSM, UMTS, and iDEN cellular formats. These include the cable assemblies, power supplies, antennas, laptop PC controller, power amplifiers, handheld DF antenna, AmberJack DF antenna, and cellular format software (CDMA, GSM, UMTS, and iDEN).

Harris also sells training on the use of the StingRay, KingFish and its accessories. Standard training sessions are 2 days per class with a maximum class size of 4 students. One-year maintenance agreements are included with all Harris WPG Products. Maintenance agreements include the following:

- Customer telephone support (8AM – 6PM EST)
- Hardware warranty
- Notification and access to software upgrades as they are released

Harris WPG is your only source and distributor of the StingRay vehicular-based and KingFish man-portable systems plus compatible accessories, training and maintenance.

If you require any additional information, please feel free to my direct line at 321-309-7773 or my mobile at 321-258-2583.

Sincerely,

Lin Vinson 8/25/08

Lin Vinson
Major Account Manager, Wireless Products Group
Harris Corporation

EXHIBIT 018

Maricopa County, FL, USA – **Harris Contract**, Serial No. 09041-SS (May 27, 2010), *available at* http://www.maricopa.gov/materials/Awarded_Contracts/PDF/09041-c.pdf (last accessed Mar. 9, 2011), p. 1, 13-14;

SERIAL 09041 SS KING FISH DUAL-MODE SYSTEM

DATE OF LAST REVISION: May 27, 2010 CONTRACT END DATE: May 19, 2011

CONTRACT PERIOD BEGINNING MAY 20, 2009
ENDING MAY 19, ~~2010~~ 2011

TO: All Departments

FROM: Department of Materials Management

SUBJECT: Contract for **KING FISH DUAL-MODE SYSTEM**

Attached to this letter is a listing of vendors available to Maricopa County Agencies utilizing the Sheriff's Office Contract C-50-09-073-3-00. The using agency and other interested parties may access and electronic version of this contract from the Materials Management Web site at: http://www.maricopa.gov/materials/Awarded_Contracts/search.asp.

Please note: Price Agreement Purchase Orders (PG documents) may be generated using the information from this list. Use NIGP CODE 6808701.

All purchases of product(s) listed on the attached pages of this letter are to be obtained from the listed contractor(s).

EXHIBIT A
PRICING

SERIAL 09041-SS
NIGP CODE: 72500

RESPONDENT NAME:	Lin Vinson
VENDOR NUMBER :	
ADDRESS:	Harris Corporation, GCSD Attn: Mailstop R5/11A PO Box 9800 Melbourne, FL 32902
P.O. ADDRESS:	Harris Corporation, GCSD Attn: Mailstop R5/11A PO Box 9800 Melbourne, FL 32902
TELEPHONE NUMBER:	321-309-7333
FACSIMILY NUMBER:	321-309-7437
WEB SITE:	
REPRESENTATIVE:	Lin Vinson
REPRESENTATIVE E-MAIL:	wvinson@harris.com

	YES	NO	REBATE
WILL ALLOW OTHER GOVERNMENTAL ENTITIES TO PURCHASE FROM THIS CONTRACT:	[ ]	[X]	
WILL ACCEPT PROCUREMENT CARD FOR PAYMENT:	[X]	[]	
WILL OFFER REBATE (CASH OR CREDIT) FOR UTILIZING PROCUREMENT CARD: (Payment shall be made within 48 hours of utilizing the Purchasing Card)	[ ]	[]	0%

PAYMENT TERMS: RESPONDENT IS REQUIRED TO PICK ONE OF THE FOLLOWING. PAYMENT TERMS WILL BE CONSIDERED IN DETERMINING LOW BID. FAILURE TO CHOOSE PAYMENT TERMS WILL RESULT IN A DEFAULT TO NET 30 DAYS.

[] NET 10 DAYS	[ ] NET 45 DAYS	[ ] 1% 10 DAYS NET 30 DAYS
[ ] NET 15 DAYS	[ ] NET 60 DAYS	[ ] 2% 30 DAYS NET 31 DAYS
[ ] NET 20 DAYS	[ ] NET 90 DAYS	[ ] 1% 30 DAYS NET 31 DAYS
[X] NET 30 DAYS	[ ] 2% 10 DAYS NET 30 DAYS	[ ] 5% 30 DAYS NET 31 DAYS

KingFish Dual-Mode System
Vehicular/Man-Portable Configuration
CDMA, GSM, & iDEN

Technology	Part Number	Description	Unit Price	Qty (ea.)	Total Price
KingFish Dual-Mode System:	KINGFISH	KingFish System	$ 27,800	1	$ 27,800
Vehicular and Man-Portable Operation	KF-CDMA-SW	CDMA Controller Software	$ 18,100	1	$ 18,100
CDMA/GSM/iDEN	KF-GSM-SW	GSM Controller Software	$ 18,100	1	$ 18,100
Interrogation, Direction Finding, Denial of Service & Passive Collection	KF-iDEN-SW	iDEN Controller Software	$ 18,100	1	$ 18,100
	MINI PC (2015657)	OQO Mini-PC Controller	$ 3,200	1	$ 3,200
			KingFish Price		**$ 85,300**
Training Classes	TRAIN-MLB	Training-Melbourne, FL (KingFish)	$ 4,000	1	$ 4,000
KingFish System			**Training Price**		**$ 4,000**
			Total System Price		**$ 89,300**

NOTES

Standard Delivery is 90 Days ARO

StingRay and KingFish Hardware platform comes standard without Software. Protocol Software (CDMA, GSM, or iDEN) must be purchased separately (includes SDR and Controller Software)

StingRay and KingFish Hardware platform comes standard without a controller computer. A Laptop or Mini PC must be purchased separately

StingRay and Kingfish support 3 technologies simultaneously, additional technologies can be swapped through a hardware flash process (software provided).

The unit prices above include 1 year Hardware warranty and 1 year access to Software upgrades for the protocol(s) purchased

1 Year extended Maintenance Agreements are available for 15% of the line item prices for the KingFish or AmberJack systems

Maintenance Agreements provide for an additional 12 months of extended Hardware warranty and Software upgrades

Training classes are 12 hours (2 days) per product per protocol (unless stated otherwise) with 4 students maximum per class

EXHIBIT 019
EXHIBIT 019
EXHIBIT 019
EXHIBIT 019
EXHIBIT 019
EXHIBIT 019
EXHIBIT 019
EXHIBIT 019
EXHIBIT 019
EXHIBIT 019
EXHIBIT 019
EXHIBIT 019
EXHIBIT 019
EXHIBIT 019
EXHIBIT 019
EXHIBIT 019
EXHIBIT 019
EXHIBIT 019
EXHIBIT 019
EXHIBIT 019
EXHIBIT 019
EXHIBIT 019
EXHIBIT 019
EXHIBIT 019
EXHIBIT 019
EXHIBIT 019
EXHIBIT 019
EXHIBIT 019
EXHIBIT 019
EXHIBIT 019
EXHIBIT 019
EXHIBIT 019
EXHIBIT 019

ATTACHED EXHIBITS
SECOND SUBMISSION OF CONSOLIDATED EXHIBITS RELATING TO DISCOVERY AND SUPPRESSION ISSUES
CR08-814-PHX-DGC

Valentino-DeVries, Jennifer, *'Stingray' Phone Tracker Fuels Constitutional Clash*, The Wall Street Journal, p. A1 (Sept. 22, 2011) (original article addressing CR08-814-PHX-DGC) *available at* http://online.wsj.com/article/SB10001424053111904194604576583112723197574.html (last accessed: Sept. 22, 2011);

Dow Jones Reprints: This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers, use the Order Reprints tool at the bottom of any article or visit www.djreprints.com

See a sample reprint in PDF format. Order a reprint of this article now

THE WALL STREET JOURNAL.
WSJ.com

TECHNOLOGY | SEPTEMBER 22, 2011

'Stingray' Phone Tracker Fuels Constitutional Clash

By JENNIFER VALENTINO-DEVRIES

For more than a year, federal authorities pursued a man they called simply "the Hacker." Only after using a little known cellphone-tracking device—a stingray—were they able to zero in on a California home and make the arrest.

U.S. Patent and Trademark Office

A Harris StingRay II, one of several devices dubbed 'stingrays.'

Stingrays are designed to locate a mobile phone even when it's not being used to make a call. The Federal Bureau of Investigation considers the devices to be so critical that it has a policy of deleting the data gathered in their use, mainly to keep suspects in the dark about their capabilities, an FBI official told The Wall Street Journal in response to inquiries.

A stingray's role in nabbing the alleged "Hacker"—Daniel David Rigmaiden—is shaping up as a possible test of the legal standards for using these devices in investigations. The FBI says it obtains appropriate court approval to use the device.

Stingrays are one of several new technologies used by law enforcement to track people's locations, often without a search warrant. These techniques are driving a constitutional debate about whether the Fourth Amendment, which prohibits unreasonable searches and seizures, but which was written before the digital age, is keeping pace with the times.

On Nov. 8, the Supreme Court will hear arguments over whether or not police need a warrant before secretly installing a GPS device on a suspect's car and tracking him for an extended period. In both the Senate and House, new bills would require a warrant before tracking a cellphone's location.

More

- **Key Documents in 'Stingray' Case**
- **Digits:** How 'Stingray' Devices Work
- **Digits:** How Technology Is Testing the Fourth Amendment

And on Thursday in U.S. District Court of Arizona, Judge David G. Campbell is set to hear a request by Mr. Rigmaiden, who is facing fraud charges, to have information about the government's secret techniques disclosed to him so he can use it in his defense. Mr. Rigmaiden maintains his innocence and says that using stingrays to locate devices in homes without a valid warrant "disregards the United States Constitution" and is illegal.

His argument has caught the judge's attention. In a February hearing, according to a transcript, Judge Campbell asked the prosecutor, "Were there warrants obtained in connection with the use of this device?"

The prosecutor, Frederick A. Battista, said the government obtained a "court order that satisfied [the] language" in the federal law on warrants. The judge then asked how an order or warrant could have been obtained without telling the judge what technology was being used. Mr. Battista said: "It was a standard practice, your honor."

Judge Campbell responded that it "can be litigated whether those orders were appropriate."

On Thursday the government will argue it should be able to withhold details about the tool used to locate Mr. Rigmaiden, according to documents filed by the prosecution. In a statement to the Journal, Sherry Sabol, Chief of the Science & Technology Office for the FBI's Office of General Counsel, says that information about stingrays and related technology is "considered Law Enforcement Sensitive, since its public release could harm law enforcement efforts by compromising future use of the equipment."

The prosecutor, Mr. Battista, told the judge that the government worries that disclosure would make the gear "subject to being defeated or avoided or detected."

A stingray works by mimicking a cellphone tower, getting a phone to connect to it and measuring signals from the phone. It lets the stingray operator "ping," or send a signal to, a phone and locate it as long as it is powered on, according to documents reviewed by the Journal. The device has various uses, including helping police locate suspects and aiding search-and-rescue teams in finding people lost in remote areas or buried in rubble after an accident.

The government says "stingray" is a generic term. In Mr. Rigmaiden's case it remains unclear which device or devices were actually used.

The best known stingray maker is Florida-based defense contractor Harris Corp. A spokesman for Harris declined to comment.

Harris holds trademarks registered between 2002 and 2008 on several devices, including the StingRay, StingRay II, AmberJack, KingFish, TriggerFish and LoggerHead. Similar devices are available from other manufacturers. According to a Harris document, its devices are sold only to law-enforcement and government agencies.

Some of the gadgets look surprisingly old-fashioned, with a smattering of switches and lights scattered across a panel roughly the size of a shoebox, according to photos of a Harris-made StingRay reviewed by the Journal. The devices can be carried by hand or mounted in cars, allowing investigators to move around quickly.

A rare public reference to this type of technology appeared this summer in the television crime drama "The Closer." In the episode, law-enforcement officers use a gadget they called a "catfish" to track cellphones without a court order.

The U.S. armed forces also use stingrays or similar devices, according to public contract notices. Local law enforcement in Minnesota, Arizona, Miami and Durham, N.C., also either possess the devices or have considered buying them, according to interviews and published requests for funding.

The sheriff's department in Maricopa County, Ariz., uses the equipment "about on a monthly basis," says Sgt. Jesse Spurgin. "This is for location only. We can't listen in on conversations," he says.

Sgt. Spurgin says officers often obtain court orders, but not necessarily search warrants, when using the device. To obtain a search warrant from a court, officers as a rule need to show "probable cause," which is generally defined as a reasonable belief, based on factual evidence, that a crime was committed. Lesser standards apply to other court orders.

A spokeswoman with the Bureau of Criminal Apprehension in Minnesota says officers don't need to seek search warrants in that state to use a mobile tracking device because it "does not intercept communication, so no wiretap laws would apply."

FBI and Department of Justice officials have also said that investigators don't need search warrants. Associate Deputy Attorney General James A. Baker and FBI General Counsel Valerie E. Caproni both said at a panel at the Brookings Institution in May that devices like these fall into a category of tools called "pen registers," which require a lesser order than a warrant. Pen registers gather signals from phones, such as phone numbers dialed, but don't receive the content of the communications.

To get a pen-register order, investigators don't have to show probable cause. The Supreme Court has ruled that use of a pen register doesn't require a search warrant because it doesn't involve interception of conversations.

But with cellphones, data sent includes location information, making the situation more complicated because some judges have found that location information is more intrusive than details about phone numbers dialed. Some courts have required a slightly higher standard for location information, but not a warrant, while others have held that a search warrant is necessary.

The prosecution in the Rigmaiden case says in court documents that the "decisions are made on a case-by-case basis" by magistrate and district judges. Court records in other cases indicate that decisions are mixed, and cases are only now moving through appellate courts.

The FBI advises agents to work with federal prosecutors locally to meet the requirements of their particular district or judge, the FBI's Ms. Sabol says. She also says it is FBI policy to obtain a search warrant if the FBI believes the technology "may provide information on an individual while that person is in a location where he or she would have a reasonable expectation of privacy."

Experts say lawmakers and the courts haven't yet settled under what circumstances locating a person or device constitutes a search requiring a warrant. Tracking people when they are home is particularly sensitive because the Fourth Amendment specifies that people have a right to be secure against unreasonable searches in their "houses."

"The law is uncertain," says Orin Kerr, a professor at George Washington University Law School and former computer-crime attorney at the Department of Justice. Mr. Kerr, who has argued that warrants should be required for some, but not all, types of location data, says that the legality "should depend on the technology."

In the case of Mr. Rigmaiden, the government alleges that as early as 2005, he began filing fraudulent tax returns online. Overall, investigators say, Mr. Rigmaiden electronically filed more than 1,900 fraudulent tax returns as part of a $4 million plot.

Federal investigators say they pursued Mr. Rigmaiden "through a virtual labyrinth of twists and turns." Eventually, they say they linked Mr. Rigmaiden to use of a mobile-broadband card, a device that lets a computer connect to the Internet through a cellphone network.

Investigators obtained court orders to track the broadband card. Both orders remain sealed, but portions of them have been quoted by the defense and the prosecution.

These two documents are central to the clash in the Arizona courtroom. One authorizes a "pen register" and clearly isn't a search warrant. The other document is more complex. The prosecution says it is a type of search warrant and that a finding of probable cause was made.

But the defense argues that it can't be a proper search warrant, because among other things it allowed investigators to delete all the tracking data collected, rather than reporting back to the judge.

Legal experts who spoke with the Journal say it is difficult to evaluate the order, since it remains sealed. In general, for purposes of the Fourth Amendment, the finding of probable cause is most important in determining

whether a search is reasonable because that requirement is specified in the Constitution itself, rather than in legal statutes, says Mr. Kerr.

But it is "odd" for a search warrant to allow deletion of evidence before a case goes to trial, says Paul Ohm, a professor at the University of Colorado Law School and a former computer-crime attorney at the Department of Justice. The law governing search warrants specifies how the warrants are to be executed and generally requires information to be returned to the judge.

Even if the court finds the government's actions acceptable under the Fourth Amendment, deleting the data is "still something we might not want the FBI doing," Mr. Ohm says.

The government says the data from the use of the stingray has been deleted and isn't available to the defendant. In a statement, the FBI told the Journal that "our policy since the 1990s has been to purge or 'expunge' all information obtained during a location operation" when using stingray-type gear.

As a general matter, Ms. Sabol says, court orders related to stingray technology "will include a directive to expunge information at the end of the location operation."

Ms. Sabol says the FBI follows this policy because its intent isn't to use the data as evidence in court, but rather to simply find the "general location of their subject" in order to start collecting other information that can be used to justify a physical search of the premises.

In the Rigmaiden example, investigators used the stingray to narrow down the location of the broadband card. Then they went to the apartment complex's office and learned that one resident had used a false ID and a fake tax return on the renter's application, according to court documents.

Based on that evidence, they obtained a search warrant for the apartment. They found the broadband card connected to a computer.

Mr. Rigmaiden, who doesn't confirm or deny ownership of the broadband card, is arguing he should be given information about the device and about other aspects of the mission that located him.

In the February hearing, Judge Campbell said he might need to weigh the government's claim of privilege against the defendant's Fourth Amendment rights, and asked the prosecution, "How can we litigate in this case whether this technology that was used in this case violates the Fourth Amendment without knowing precisely what it can do?"

Write to Jennifer Valentino-DeVries at Jennifer.Valentino-DeVries@wsj.com

Copyright 2011 Dow Jones & Company, Inc. All Rights Reserved
This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by our Subscriber Agreement and by copyright law. For non-personal use or to order multiple copies, please contact Dow Jones Reprints at 1-800-843-0008 or visit www.djreprints.com

EXHIBIT 020

Valentino-DeVries, Jennifer, *Feds Shift Tracking Defense: Prosecutors in Arizona Case Drop Position That 'Stingray' Use Didn't Require Warrant*, The Wall Street Journal, (Nov. 3, 2011) *available at* http://online.wsj.com/article/SB10001424052970204621904577014363024341028.html (last accessed: Nov. 15, 2011);

Dow Jones Reprints: This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers, use the Order Reprints tool at the bottom of any article or visit www.djreprints.com

See a sample reprint in PDF format. Order a reprint of this article now

THE WALL STREET JOURNAL.
WSJ.com

TECHNOLOGY | NOVEMBER 3, 2011

Feds Shift Tracking Defense

Prosecutors in Arizona Case Drop Position That 'Stingray' Use Didn't Require Warrant

By JENNIFER VALENTINO-DEVRIES

The U.S. Department of Justice now says its use of a cellphone-tracking device in a controversial Arizona case could be considered a "search" under the Fourth Amendment, a tactical move legal experts say is designed to protect the secrecy of the gadgets known as "stingrays."

For more than a year, federal prosecutors have argued in U.S. District Court that the use of the stingray device—which can locate a mobile phone even when it's not being used to make a call—wasn't a search, in part because the user had no reasonable expectation of privacy while using Verizon Wireless cellphone service. Under that argument, authorities wouldn't need to obtain a search warrant before using one of the devices.

The defendant in the case, Daniel David Rigmaiden, is facing fraud charges. His quest to force the government to provide information about the device used to locate him was the subject of front-page article in The Wall Street Journal in September.

Legal experts say the government's move fits into its strategy of keeping information about the devices under wraps, and the government continues to maintain that, in general, search warrants aren't required.

The government said it is willing to make these concessions in this case alone in an attempt to "avoid unnecessary disclosure" of information about its stingray devices. The judge in the case, David G. Campbell, had indicated he might want to know more about the technical details of the devices before ruling on whether their use constituted a search.

The government's move comes amid renewed questions about how the use of new technologies by law enforcement is challenging interpretations of the Fourth Amendment, which prohibits unreasonable searches and seizures.

The Supreme Court is set to hear oral arguments next week in a case in which federal agents used a GPS device to track a suspect's car for a month without a search warrant. The government argues that people driving on public roads don't have a reasonable expectation of privacy in their public movements.

In the Arizona case, Mr. Rigmaiden was found after federal agents used a stingray to track a mobile device to an apartment building. He has argued that using stingrays to locate devices in homes without a valid warrant "disregards the United States Constitution" and is illegal.

U.S. Patent and Trademark Office

Harris Corp. is the best-known maker of stingrays, like the one above.

In a memo filed with the court last week, the prosecution said it will agree that in this case, the "tracking operation was a Fourth Amendment search and seizure." It also will agree with some of the defendant's other assertions, including that the stingray caused a "disruption of service."

But the government's concessions don't represent a shift in policy. In the same memo, the government says its "position continues to be that, as a factual matter, the operation did not involve a search or seizure under the Fourth Amendment."

The latest filing means that in the Arizona case the government could stake its case on the argument that it did have a valid search warrant.

The defense has asserted the order wasn't, in fact, a proper search warrant, in part because it allowed investigators to delete all the tracking data collected, rather than reporting back to the judge.

The defense didn't immediately respond to a request for comment. The U.S. Attorney's Office declined to comment beyond what was in the memorandum.

Earlier

Phone Tracker Fuels Constitutional Clash
9/22/2011

More on Internet Privacy

Using Credit Cards to Target Web Ads

Secret Orders Target Email

Heading Off Privacy Problems

Latest in Web Tracking: Stealthy 'Supercookies'

Facebook Adds New Privacy Controls

In September, a Federal Bureau of Investigation representative told the Journal the policy of deletion "is intended to protect law enforcement capabilities so that subjects of law enforcement investigations do not learn how to evade or defeat lawfully authorized investigative activity."

Along with its memorandum, the government submitted an affidavit from an FBI special agent expanding on the agency's reasons for deleting data associated with stingray devices.

In the latest memo, the FBI says all data from stingrays are deleted because the devices may tend to pick up information on innocent people in addition to suspects. To ensure "that the privacy rights of those innocent third parties are maintained" after their data has been captured, all the information is deleted, including that pertaining to the subject. The defense indicated that it plans to file a response to the memorandum this week.

Copyright 2011 Dow Jones & Company, Inc. All Rights Reserved
This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by our Subscriber Agreement and by copyright law. For non-personal use or to order multiple copies, please contact Dow Jones Reprints at 1-800-843-0008 or visit
www.djreprints.com

EXHIBIT 021	USDOJ [M.D.La.] Aug. 12, 2008, Response to ACLU FOIA Request No. 07-4130, *available at* http://www.aclu.org/pdfs/freespeech/cellfoia_release_074130_20080812.pdf (last accessed: Jan. 11, 2011); Note: only relevant pages are included with footers added containing the page numbers from the full PDF available at the above URL;
EXHIBIT 021	
EXHIBIT 021	
EXHIBIT 021	
EXHIBIT 021	
EXHIBIT 021	
EXHIBIT 021	
EXHIBIT 021	
EXHIBIT 021	
EXHIBIT 021	
EXHIBIT 021	
EXHIBIT 021	
EXHIBIT 021	
EXHIBIT 021	
EXHIBIT 021	
EXHIBIT 021	
EXHIBIT 021	
EXHIBIT 021	
EXHIBIT 021	
EXHIBIT 021	
EXHIBIT 021	
EXHIBIT 021	
EXHIBIT 021	
EXHIBIT 021	
EXHIBIT 021	
EXHIBIT 021	
EXHIBIT 021	
EXHIBIT 021	
EXHIBIT 021	
EXHIBIT 021	
EXHIBIT 021	

U.S. Department of Justice

Executive Office for United States Attorneys
Freedom of Information/Privacy Act Staff
600 E Street, N.W., Room 7300
Washington, D.C. 20530
202-616-6757 Fax 202-616-6478

Requester: Catherine Crump Request Number: 07-4130

Subject of Request: Mobile Phone Tracking (Item 1-4) AUG 12 2008

Dear Requester:

Your request for records under the Freedom of Information Act/Privacy Act has been processed. This letter constitutes an interim reply from the Executive Office for United States Attorneys, the official record-keeper for all records located in this office and the various United States Attorneys' Offices. To provide you the greatest degree of access authorized by the Freedom of Information Act and the Privacy Act, we have considered your request in light of the provisions of both statutes.

The records you seek are located in a Privacy Act system of records that, in accordance with regulations promulgated by the Attorney General, is exempt from the access provisions of the Privacy Act, 28 C.F.R. § 16.81. We have also processed your request under the Freedom of Information Act and are making all records required to be released, or considered appropriate for release as a matter of discretion, available to you. This letter is a [**X**] partial [ ] full denial.

Enclosed please find:

37 page(s) are being released in full (RIF);
2 page(s) are being released in part (RIP);
_____ page(s) are withheld in full (WIF). **The redacted/withheld documents were reviewed to determine if any information could be segregated for release.**

The exemption(s) cited for withholding records or portions of records are marked below. An enclosure to this letter explains the exemptions in more detail.

Section 552			Section 552a
[ ] (b)(1)	[ ] (b)(4)	[ ] (b)(7)(B)	[**X**] (j)(2)
[ ] (b)(2)	[**X**] (b)(5)	[ ] (b)(7)(C)	[ ] (k)(2)
[ ] (b)(3)	[ ] (b)(6)	[ ] (b)(7)(D)	[ ] (k)(5)
_____	[ ] (b)(7)(A)	[**X**] (b)(7)(E)	[ ] _____
_____		[ ] (b)(7)(F)	

USDOJ [M.D.La.] Response to ACLU FOIA Request No. 07-4130 [Aug. 12, 2008]; Page # 1 of 42;
Download at <http://www.aclu.org/pdfs/freespeech/cellfoia_release_074130_20080812.pdf>
[last accessed Jan. 11, 2011];

[**X**] 47 additional page(s) originated with another government component. **These records were found in the U.S. Attorney's Office files and may or may not be responsive to your request.** These records will be referred to the following component for review and direct response to you: Department of Justice, Criminal Division.

[**X**] 4 additional page(s) originated with another government component. **These records were found in the U.S. Attorney's Office files and may or may not be responsive to your request.** These records will be referred to the following component for consultation and our office will respond to you after their review: U.S. Marshals Service .

[**X**] See additional information attached.

Although I am aware that this request is the subject of ongoing litigation and that appeals are not ordinarily acted on in such situations, I am required by statute and regulation to inform you that if you consider my response to be a denial of your request, you have the right to file an administrative appeal by writing within 60 days from the date of this letter to the **Office of Information and Privacy, United States Department of Justice, 1425 New York Avenue, Suite 11050, Washington, D.C. 20530-0001**. In light of the fact that this is an interim response, I would ask that you wait until the EOUSA has issued its final response in this request before you file an appeal.

Sincerely,

Karen M. Finnegan for

William G. Stewart II
Assistant Director

Enclosure(s)

USDOJ [M.D.La.] Response to ACLU FOIA Request No. 07-4130 [Aug. 12, 2008]; Page # 2 of 42;
Download at <http://www.aclu.org/pdfs/freespeech/cellfoia_release_074130_20080812.pdf>
[last accessed Jan. 11, 2011];

EXPLANATION OF EXEMPTIONS

FOIA: TITLE 5, UNITED STATES CODE, SECTION 552

(b) (1)	(A) specifically authorized under criteria established by and Executive order to be kept secret in the in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order;
(b)(2)	related solely to the internal personnel rules and practices of an agency;
(b)(3)	specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;
(b)(4)	trade secrets and commercial or financial information obtained from a person and privileged or confidential;
(b)(5)	inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;
(b)(6)	personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;
(b)(7)	records or information compiled for law enforcement purposes, but only the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual.
(b)(8)	contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or
(b)(9)	geological and geophysical information and data, including maps, concerning wells.

PRIVACY ACT: TITLE 5, UNITED STATES CODE, SECTION 552a

(d)(5)	information complied in reasonable anticipation of a civil action proceeding;
(j)(2)	material reporting investigative efforts pertaining to the enforcement of criminal law including efforts to prevent, control, or reduce crime or apprehend criminals;
(k)(1)	information which is currently and properly classified pursuant to Executive Order 12356 in the interest of the national defense or foreign policy, for example, information involving intelligence sources or methods;
(k)(2)	investigatory material complied for law enforcement purposes, other than criminal, which did not result in loss of a right, benefit or privilege under Federal programs, or which would identify a source who furnished information pursuant to a promise that his/her identity would be held in confidence;
(k)(3)	material maintained in connection with providing protective services to the President of the United States or any other individual pursuant to the authority of Title 18, United States Code, Section 3056;
(k)(4)	required by statute to be maintained and used solely as statistical records;
(k)(5)	investigatory material compiled solely for the purpose of determining suitability eligibility, or qualification for Federal civilian employment or for access to classified information, the disclosure of which would reveal the identity of the person who furnished information pursuant to a promise that his identity would be held in confidence;
(k)(6)	testing or examination material used to determine individual qualifications for appointment or promotion in Federal Government service the release of which would compromise the testing or examination process;
(k)(7)	material used to determine potential for promotion in the armed services, the disclosure of which would reveal the identity of the person who furnished the material pursuant to a promise that his identity would be held in confidence.

FBI/DOJ
1/06

USDOJ [M.D.La.] Response to ACLU FOIA Request No. 07-4130 [Aug. 12, 2008]; Page # 3 of 42;
Download at <http://www.aclu.org/pdfs/freespeech/cellfoia_release_074130_20080812.pdf>
[last accessed Jan. 11, 2011];

A cell site simulator (sometimes called a digital analyzer, cell site locator, triggerfish, ESN reader, or swamp box) is a mobile device that can electronically force a cell phone to register its telephone number (MIN), electronic serial number (ESN), and information about its location, when the phone is turned on. This can be done without the user knowing about it, and without involving the cell phone provider.

Section 216 of the Patriot Act altered the definition of a pen register in 18 U.S.C. § 3127 (3) so that it includes these devices. Consequently, a pen register/trap and trace order must be obtained by the government before it uses such a device.

The use of a triggerfish to locate cellular telephones is an issue of some controversy. The Office of Enforcement Operations (OEO) encourages AUSAs to contact Mark Eckenwiler at (202) 616-0435 if they have questions or concerns.

Note. It may also be possible to flash the firmware of a cell phone so that you can intercept conversations using a suspect's cell phone as the bug. You don't even have to have possession of the phone to modify it; the "firmware" is modified wirelessly. This law enforcement tool was recently discussed in a Memorandum Opinion from SDNY, and has been getting a bit of news coverage lately. The authority for doing this can be found in 18 U.S. C. § 2518(11), but it sounds like something that you would not want to do without checking with OEO first.

See also:

- *Electronic Surveillance Manual* Chapter XIV
- Electronic Surveillance Issues
- *Federal Narcotics Prosecutions* § 3.16
- 76 ALR4th 536 ("Search and Seizure of Telephone Company Records Pertaining to Subscriber as Violation of Subscriber's Constitutional Rights")
- USABook topic pages: Electronic Surveillance; Pen Registers

updated 02/23/07

USDOJ [M.D.La.] Response to ACLU FOIA Request No. 07-4130 [Aug. 12, 2008]; Page # 18 of 42;
Download at <http://www.aclu.org/pdfs/freespeech/cellfoia_release_074130_20080812.pdf>
[last accessed Jan. 11, 2011];

Altron, *GSM/UMTS Grabber: Deploying local mobile networks and secret grabbing of identification information in GSM and UMTS bands*, PDF provided at ISS World Europe 2008, *available at* http://wikileaks.org/spyfiles/files/0/87_ALTRON-GRABBER.pdf (last accessed: Apr. 10, 2012);

ALTRON
DEVELOPMENT AND PRODUCTION

GSM/UMTS Grabber

Deploying local mobile networks and secret grabbing of identification information in GSM and UMTS bands

Current tasks:

- Deployment of local GSM network
- Grabbing of IMSI and IMEI identifiers
- Searching and determining of the target phone's location

Product features:

- Emulation of any base station work in the coverage (based on NetMonitor data)
- Defining the identifiers (IMSI, IMEI) and saving them to the database
- Turning off the target phone from real GSM network and the restriction of certain mobile stations to obtain services (voice calls, SMS, data transfer)
- Searching and determining the location of the target phone
- Sending SMS and making calls from the operator of the GSM GRABBER to the target (within the local GSM network)
- Checking the presence of certain mobile stations in the coverage of the complex

GSM GRABBER can be made in different configurations. Design, size and functionality depend on the configuration of the complex.

GSM Grabber Handheld

It is a portable, handheld device made in the body that fits in a bag for 13″ laptop. The complex is designed for the secret grabbing of International Mobile Equipment Identify (IMEI) and International Mobile Subscriber Identify (IMSI). The system has built-in PC, antenna, and battery.

Due to its small size, the ability to hide the system to a laptop bag, as well as operation using wireless channel with the help of iPod Touch, you can secretly grab the identifiers of mobile stations anywhere: in restaurants, offices, and shops. The system has built-in omnidirectional antenna. The built-in rechargeable high capacity battery allows you to operate continuously at least 2 hours.

GSM Grabber Base

This complex made in a watertight, crashproof and dust proof case equipped with high performance secure series notebook as well as set of all the necessary components designed to perform tasks of grabbing the identifiers and searching for GSM mobile stations.

GSM Grabber Vehicle

The complex made in a special radiolucent AirBox case intended for installation on the car roof. Base stations unit of GSM 900 / 1800 band is equipped with a rotation antenna system. Operation of base station and antenna position control unit are controlled remotely (from the car).

UMTS Grabber

The UMTS Grabber allows you to grab identification information circulating in UMTS networks and to move UMTS phones to GSM network. It is an addition for any of GSM Grabbers which allows determining UMTS target phones location.

CJSC Altron
6, Kostomarovskaya str.
61002 Kharkov, Ukraine
Tel./Fax: +38 (057) 766-13-63
e-mail: post@altron.ua
http://www.altron.ua

EXHIBIT 023

EXHIBIT 023
EXHIBIT 023
EXHIBIT 023
EXHIBIT 023
EXHIBIT 023
EXHIBIT 023
EXHIBIT 023
EXHIBIT 023
EXHIBIT 023
EXHIBIT 023
EXHIBIT 023
EXHIBIT 023
EXHIBIT 023
EXHIBIT 023
EXHIBIT 023
EXHIBIT 023
EXHIBIT 023
EXHIBIT 023
EXHIBIT 023
EXHIBIT 023
EXHIBIT 023
EXHIBIT 023
EXHIBIT 023
EXHIBIT 023
EXHIBIT 023
EXHIBIT 023
EXHIBIT 023
EXHIBIT 023
EXHIBIT 023
EXHIBIT 023
EXHIBIT 023
EXHIBIT 023
EXHIBIT 023
EXHIBIT 023
EXHIBIT 023
EXHIBIT 023
EXHIBIT 023
EXHIBIT 023
EXHIBIT 023
EXHIBIT 023
EXHIBIT 023
EXHIBIT 023
EXHIBIT 023
EXHIBIT 023
EXHIBIT 023

NeoSoft [website], *Portable IMSI/IMEI GSM catcher NS-17-1*, http://www.neosoft.ch/products/emerg_tracking/detail.php?ID=1017&IBLOCK_ID=39 (last accessed: Feb. 1, 2012);

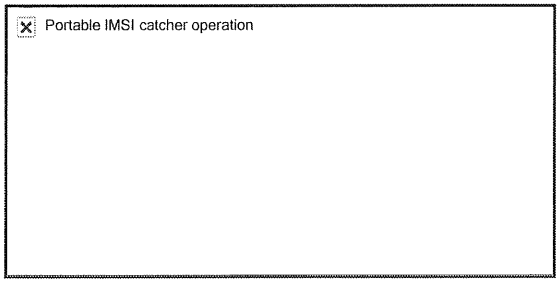
Back to HTML view

Portable IMSI/IMEI GSM catcher NS-17-1

System overview

- Our specialized GSM catcher is intended for government agencies and law enforcement groups in order to collect basic GSM information (IMSI, IMEI) about handsets in the local area (airport terminals, prisons etc).
- By utilizing our special GSM Base unit it is possible to create a special outlook system that can detect the presence of the group of handsets in the place of interest.

Functional diagram of the "IMSI/IMEI catcher" by NeoSoft is represented below:



Operational overview

The Compact GSM Base unit forces GSM phones in its vicinity to register with it. Unlike others IMSI/IMEI catchers NS-17-1 does not need to transmit very powerful signals in order to force GSM phones to make the handover from the real GSM network into this micro network.

There are two basic selection modes of control for GSM catcher NS-17-1:

1. Random (all handsets);
2. IMSI or/and IMEI (only targets).

The system ensures selection of subscribers (targets) according to known IMSI or/and IMEI identifications. Also, it has the means of detection of such identifications according to the results of statistical processing of a list of registered subscribers.

The system operates invisibly, so that the mobile station subscriber is unable to detect it. The system does not interfere with the external mobile GSM networks.

Once the compact GSM Base Unit of gsm catcher NS-17-1 requests mobile phones to introduce themselves, i.e. to send their identities – IMSI and IMEI.

The Basic operational applications for IMSI/IMEI NS-17-1 are:

- « IMSI/IMEI catching » mode

  This mode is intrinsic to the system and a part of all other modes. The Software of the system initiates operation of the base station. A cell is created (further – internal network) where the MCC, MNC and arfcn correspond to the parameters of one of the real cellular network operators that operates in this area (further – external network), the LAC differs from the same used in the real network. Mobile phones located within its operational area (further - subscribers) will detect activation of a strong channel and start the registration procedure. They provide the system with their IMSI, IMEI, TMSI (received in the real GSM network), classmark, KCN. In the "BTS control" program window a list of registered subscribers appears. For the subscribers there is no difference between registration in this micro internal network or the real external network.

- «IMSI or/and IMEI» mode

  This operational mode is intended to select targets of interest (according to IMSI/IMEI identifications) from the total number of subscribers located within operational area of the system. This mode allows registration in the internal network only for subscribers listed in the target-list. The rest of subscribers will get refusal in registering in the internal network and go back to the EN. So, all resources of the system will be redistributed solely for escorting of sessions of the subscribers of interest. The system operates with these subscribers in the same way as it operates in « IMSI/IMEI catching » mode.

- «Targets correlation» mode

  This mode allows the system to search for identifications of subscribers of interest according to information (IMSI, IMEI and their combinations) accumulated during operation of the system.

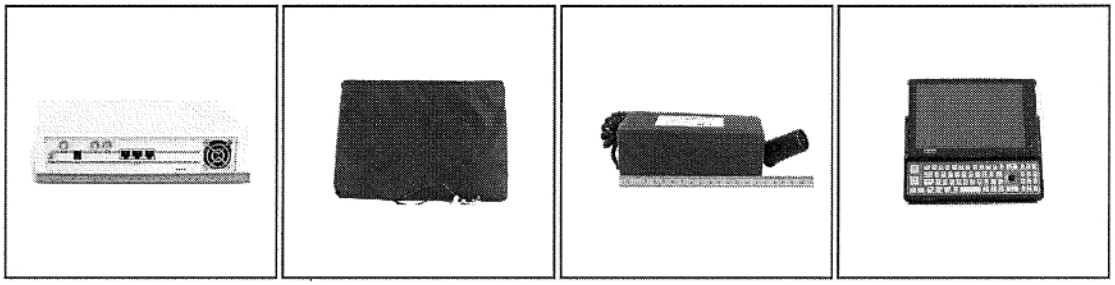
Some of the additional applications for IMSI/IMEI GSM catcher NS-17-1 are:

- Jamming of communication;
- Presence verification;
- Data Analysis;

- Direction Finding Support.

What is in the package?

- Compact GSM base unit of IMSI/IMEI catcher with three planar Directional Aeirials, battery and gateway Portable computer (OQO);



- Notebook Computer with pre-installed software;

- Carrying Case;

- User's Manual.

Technical Specifications of GSM IMSI/IMEI catcher

Frequency Range	850, 900, 1800, 1900 MHz
Output power	0.1-10 Watts
Operation Range	50..1500 m
Dimensions portable	290x260x75 mm
Equipment	Notebook PC with GM software, Portable GSM Base unit (Base unit, Battery,3xGSM Aerials, Portable PC (OQO))

Download Technical Description (zip)

EXHIBIT 024

MMI Research Trading as Cobham Surveillance, *Tactical Lawful Intercept*, PDF presentation provided at ISS World Europe 2008, *available at* http://wikileaks.org/spyfiles/files/0/43_200906-ISS-PRG-COBHAM.pdf (last accessed: Apr. 5, 2012);

COBHAM

May 2009

AVIONICS AND SURVEILLANCE DIVISION

End to end avionics and covert surveillance solutions

DEFENCE SYSTEMS DIVISION

Critical technology for network centric operations

MISSION SYSTEMS DIVISION

Complete 'nose to tail' refuelling and 'wingtip to wingtip' mission systems capability

AVIATION SERVICES DIVISION

Operates, modifies and maintains more than 150 fixed and rotary wing aircraft around the world

Tactical Lawful Intercept

Agenda

- Introductions
- Why do we need Tactical Systems?
- How do Tactical Active Systems work?
- What do Active Tactical Systems provide?
- Examples of Tactical Solutions
- Questions

Cobham Surveillance (MMI Research Products)

- Duncan Askew
  - Responsible for sales in Europe and Middle East
  - Chartered Engineer
  - 15 years in communications industry

- Cobham Surveillance (MMI Research Products) UK owned market leading company which provides off-air cell-phone:
  - Target identification
  - Target geo-locating
  - Voice/SMS interception
  - Target control

COBHAM

AVIONICS AND SURVEILLANCE DIVISION

End to end avionics and covert surveillance solutions

DEFENCE SYSTEMS DIVISION

Critical technology for network centric operations

MISSION SYSTEMS DIVISION

Complete 'nose to tail' refuelling and 'wingtip to wingtip' mission systems capability

AVIATION SERVICES DIVISION

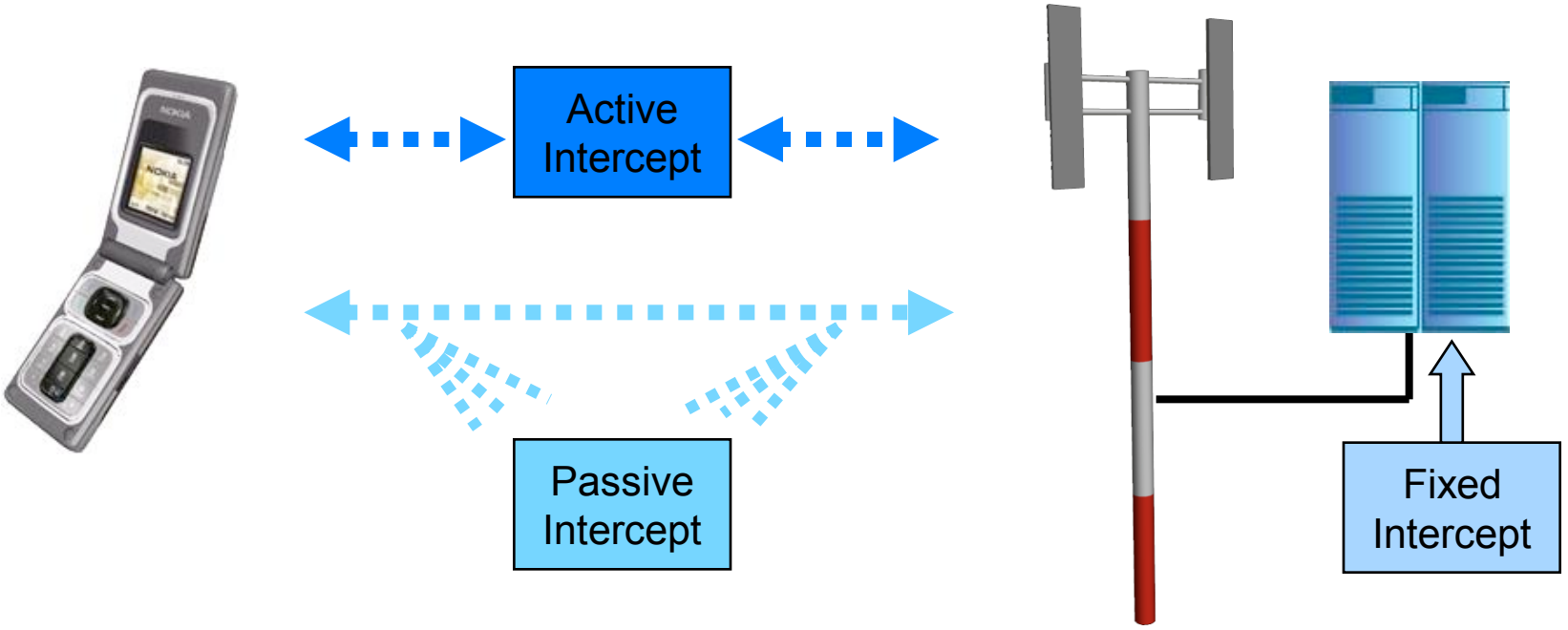
Operates, modifies and maintains more than 150 fixed and rotary wing aircraft around the world

Why do we need Tactical Systems?

Benefits of Tactical Systems

- Deployed without the cooperation of the Network Provider
- Can be used for overseas deployment
- Can be used where strategic fixed line intercept systems are NOT installed
- Allows intelligence picture to remain on target
- Complement fixed line strategic systems
- Offers location finding capabilities
- Ability to create controlled areas of network access

Complete intercept picture



Air interface
- Off-Air/Tactical Intercept
- Can operate independent to Network Provider

Core Network
- Fixed/Strategic Intercept
- Must be connected to Network

COBHAM

AVIONICS AND SURVEILLANCE DIVISION

End to end avionics and covert surveillance solutions

DEFENCE SYSTEMS DIVISION

Critical technology for network centric operations

MISSION SYSTEMS DIVISION

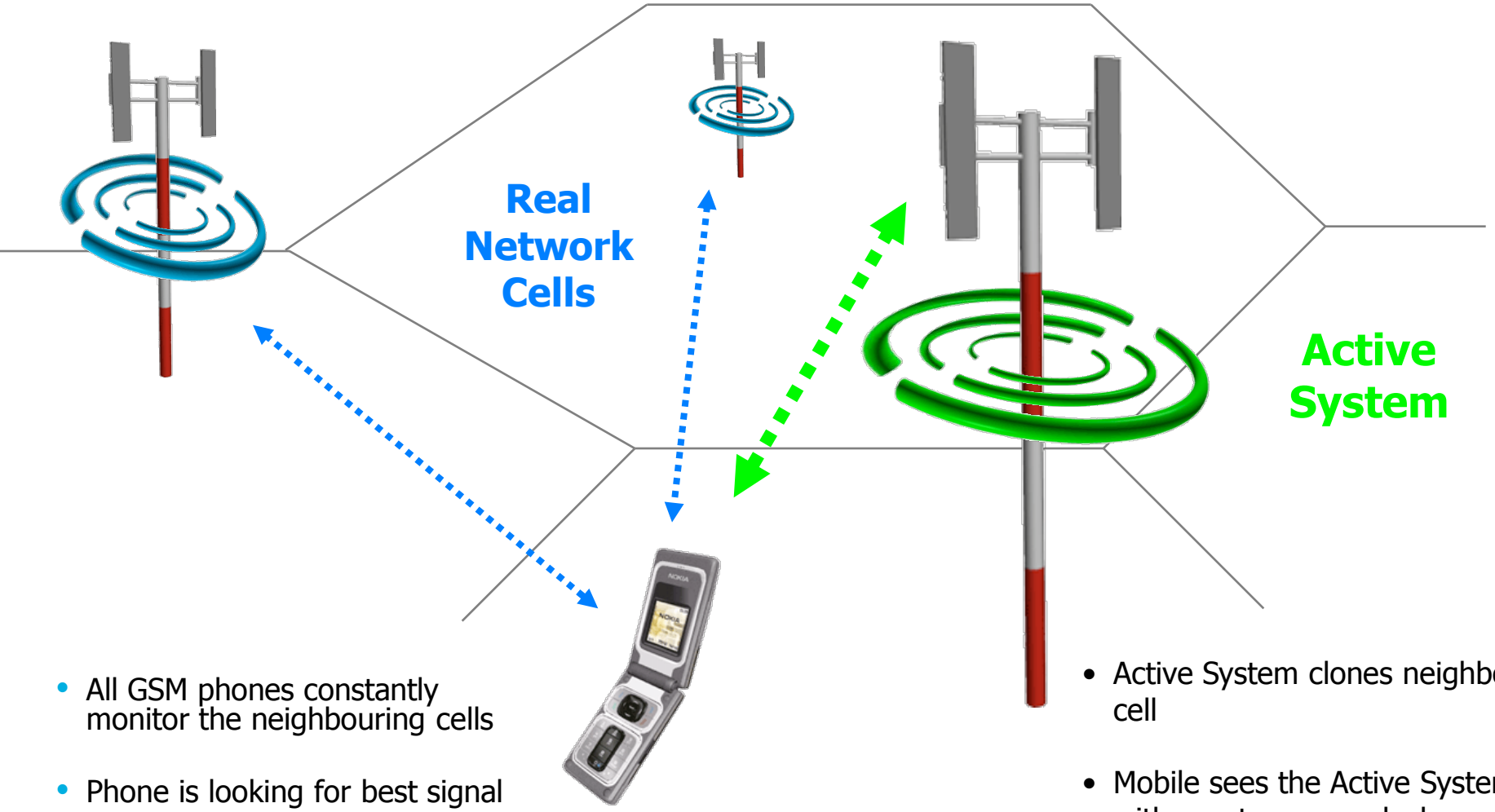
Complete 'nose to tail' refuelling and 'wingtip to wingtip' mission systems capability

AVIATION SERVICES DIVISION

Operates, modifies and maintains more than 150 fixed and rotary wing aircraft around the world

How do Tactical Active Systems Work?

How does it work?

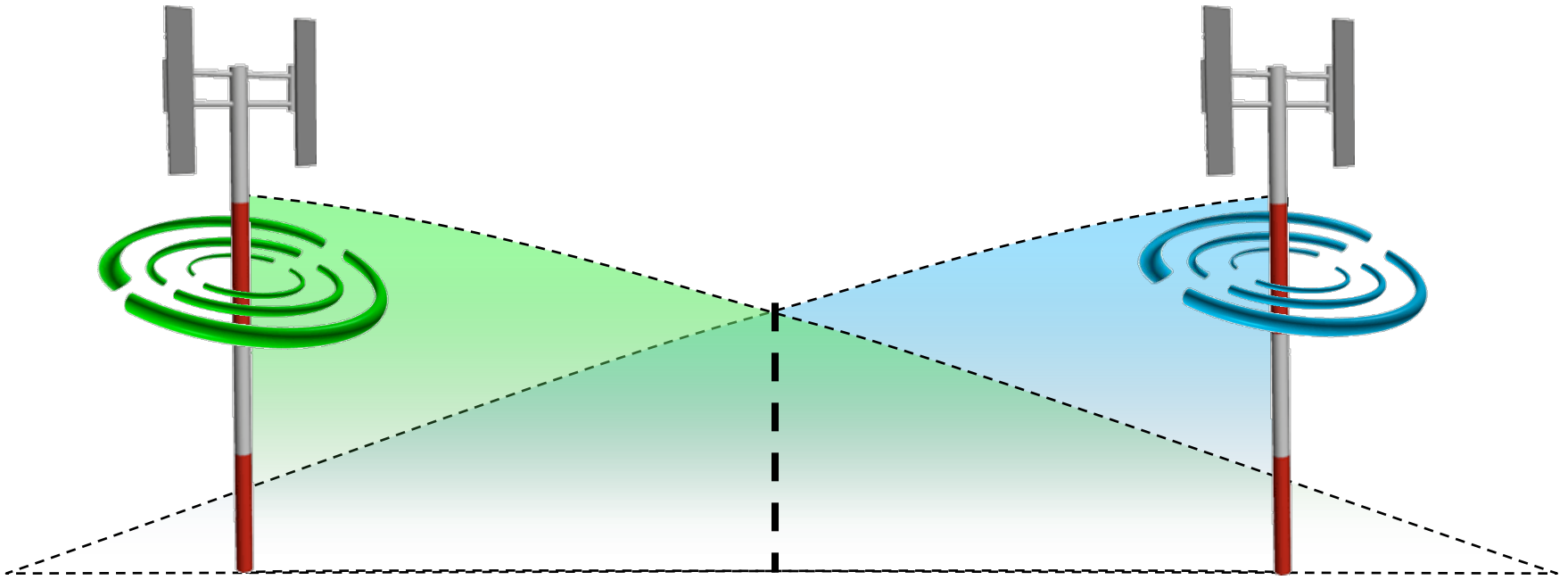


- All GSM phones constantly monitor the neighbouring cells
- Phone is looking for best signal

- Active System clones neighbour cell
- Mobile sees the Active System with greater power, locks on and gives up IMSI & IMEI data

Active system range

- The effective range is the point at which the real network signal is greater than that of the Active System
- Range can be increased by manipulation of the broadcast parameters or by increasing Active System output power
- Typical ranges: 50m dense urban, 1km urban, 5km rural



COBHAM

AVIONICS AND SURVEILLANCE DIVISION

End to end avionics and covert surveillance solutions

DEFENCE SYSTEMS DIVISION

Critical technology for network centric operations

MISSION SYSTEMS DIVISION

Complete 'nose to tail' refuelling and 'wingtip to wingtip' mission systems capability

AVIATION SERVICES DIVISION

Operates, modifies and maintains more than 150 fixed and rotary wing aircraft around the world

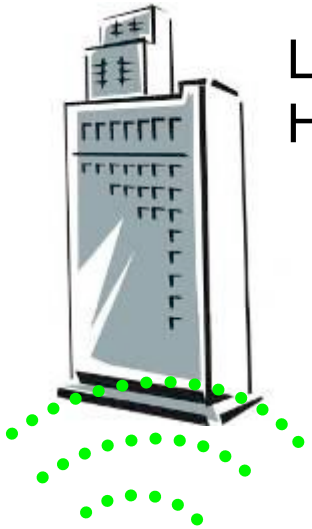
Target Identification

Phase 1 – Target Identification

- Some criminals are smart, they constantly change handsets and swap SIM cards
- They use both GSM and for greater security 3G handsets
- How do we start to build a telecoms intelligence picture if we cannot identify the targets current handset/SIM card?
- We need a tool that can capture GSM and 3G handset and SIM card identities – The Active Tactical System!

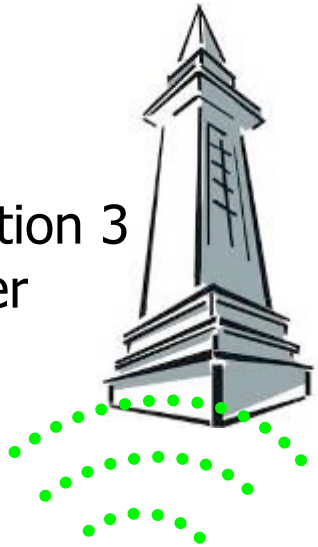
Identify a mobile at known location

Location 1
Home



Location 2
Hotel

Location 3
Tower



Last loc	IMSI	IMEI	Hits	Loc
Tower	234..	350..	12	3 *****
Hotel	234..	498..	8	2
Home	234..	520..	2	1
Hotel	234..	359..	1	1

Target Intelligence

- Once we have obtained the identity of our targets handsets and SIM card we can:
  - Establish 'Pattern of Life' through network provider cell IDs
  - Track targets handset changes and SIM swaps
  - Derive other associates through call records
  - Capture handset and SIM identities for associates in the same vicinity
  - Provide details for fixed line strategic intercept systems

COBHAM

AVIONICS AND SURVEILLANCE DIVISION

End to end avionics and covert surveillance solutions

DEFENCE SYSTEMS DIVISION

Critical technology for network centric operations

MISSION SYSTEMS DIVISION

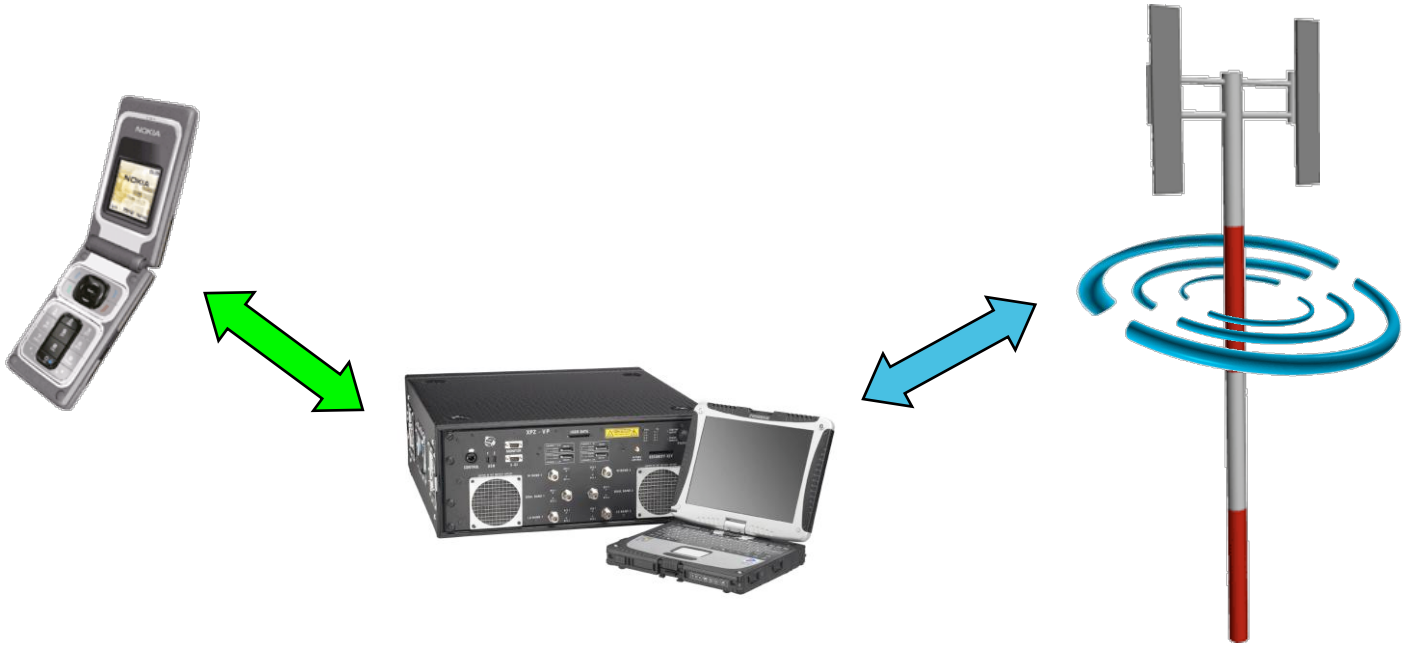
Complete 'nose to tail' refuelling and 'wingtip to wingtip' mission systems capability

AVIATION SERVICES DIVISION

Operates, modifies and maintains more than 150 fixed and rotary wing aircraft around the world

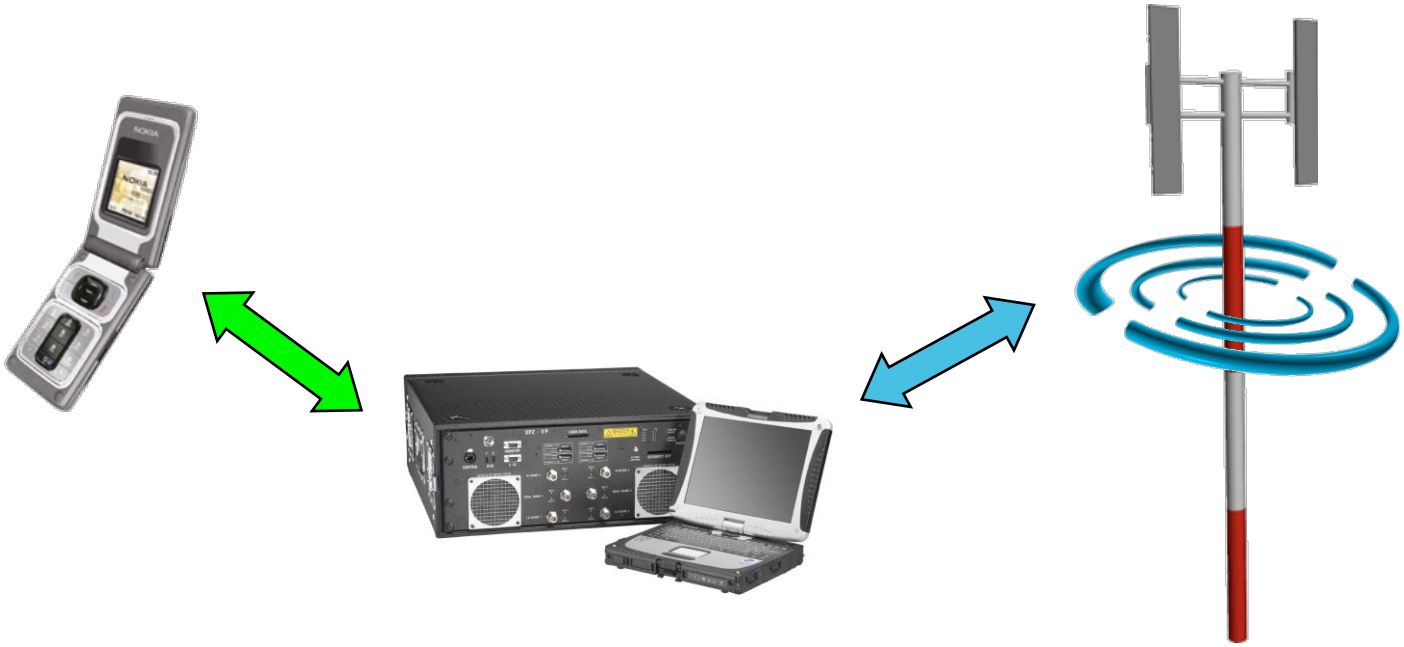
Voice/SMS Intercept

Man in the middle allows Voice/SMS intercept



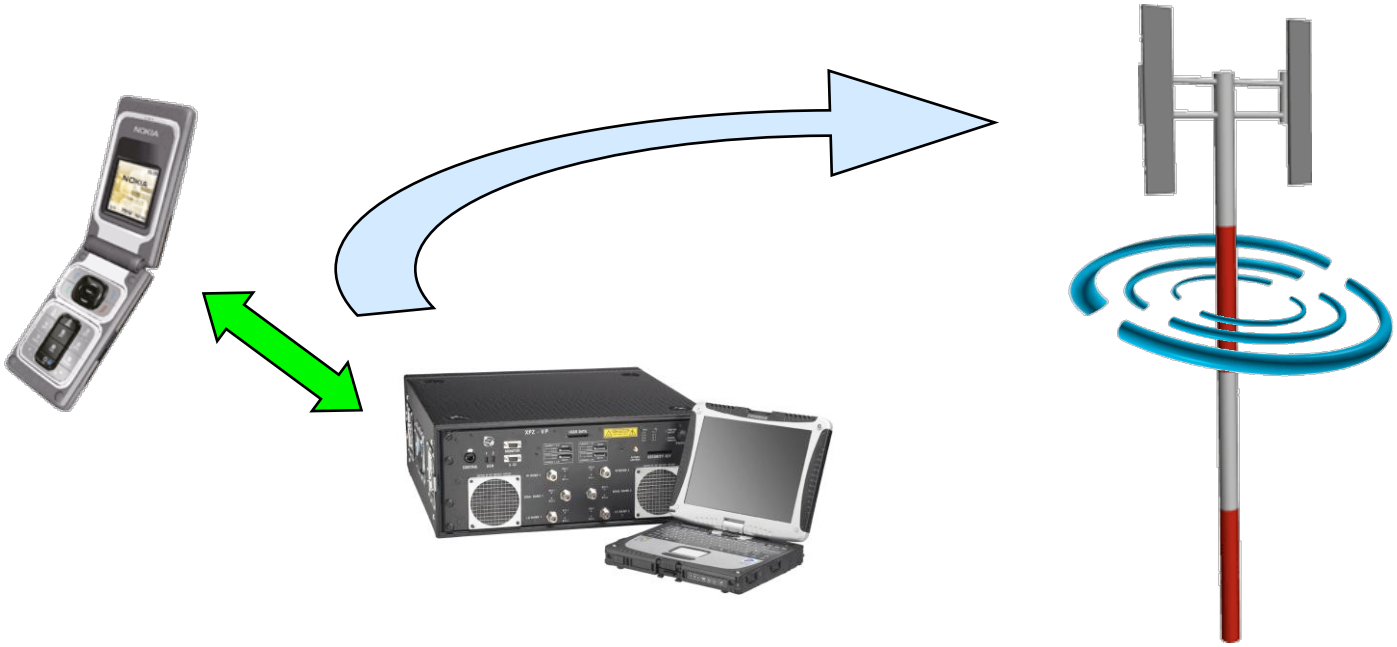
- Active system appears to be the real network
- Target phones register and will stay locked to the system
- Target phone is now off the real network and under Active System control for e.g. direction finding or hostage control situation
- Incoming and outgoing target calls/SMS can be intercepted and will be automatically recorded

Voice Intercept



- With a cloned target an Active System is able to intercept incoming and outgoing voice calls
- The system can override the call destination and redirect to a predefined number without the target knowing (e.g for hostage scenarios)
- Active System is able to record simultaneous calls. The operator can listen in in real time
- The records are stored as GSM speech frames, which yields in-build tamper protection

SMS Intercept



- Active System is able to intercept SMS calls
- Active System can send spoofed SMS to the target for misinformation purposes

COBHAM

AVIONICS AND SURVEILLANCE DIVISION

End to end avionics and covert surveillance solutions

DEFENCE SYSTEMS DIVISION

Critical technology for network centric operations

MISSION SYSTEMS DIVISION

Complete 'nose to tail' refuelling and 'wingtip to wingtip' mission systems capability

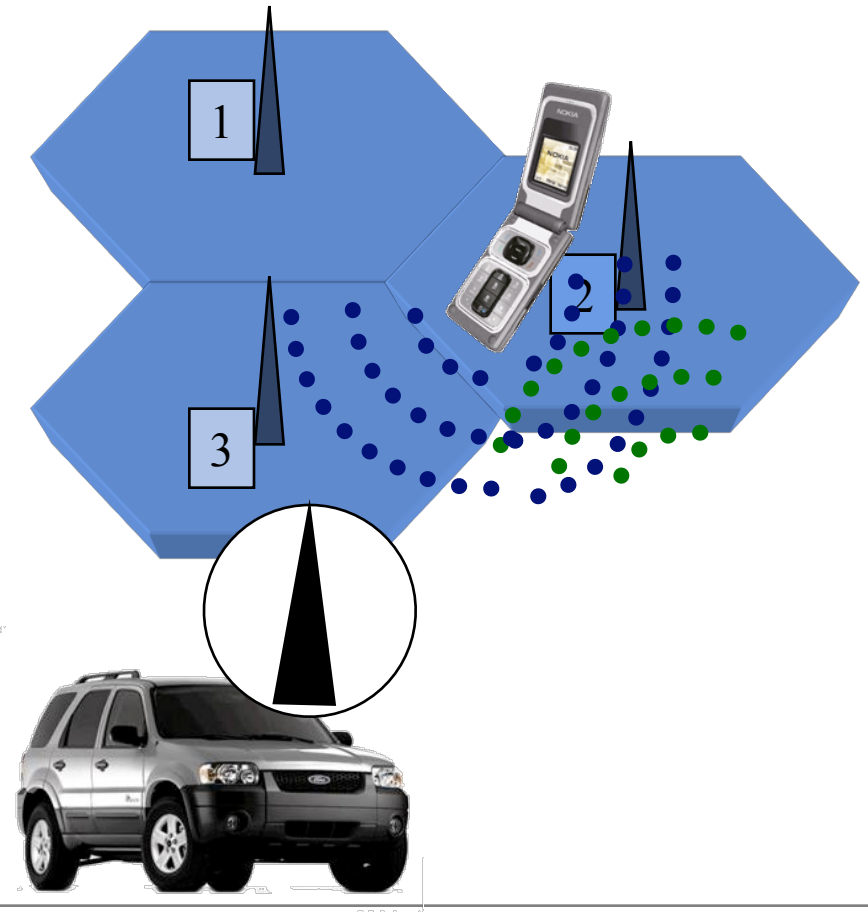
AVIATION SERVICES DIVISION

Operates, modifies and maintains more than 150 fixed and rotary wing aircraft around the world

Direction Finding

COBHAM

Geo-locate a known GSM/3G Target Mobile



- IMSI traced to GSM cell through network supplied information/call records
- Active System team deployed to cell
  - Optionally cell survey performed to determine boundary
- Once target can hear GSM signal he will be locked to the Active System
- Target is now under our control
- We initiate a 'Blind' (Silent) call
  - Target phone does not ring or vibrate
- Target phone is now transmitting on a frequency we control

- DF team move in for tracking
  - Normal to use separate vehicle
  - Vehicle system will bring you to the building
  - Handheld systems to within 1m of the phone
- DF'ing can also used to confirm target presence in suspected area/building

COBHAM

AVIONICS AND SURVEILLANCE DIVISION

End to end avionics and covert surveillance solutions

DEFENCE SYSTEMS DIVISION

Critical technology for network centric operations

MISSION SYSTEMS DIVISION

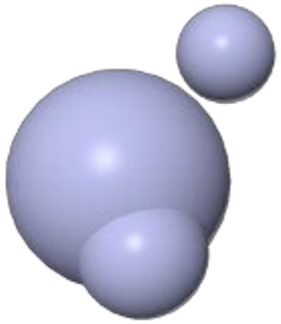
Complete 'nose to tail' refuelling and 'wingtip to wingtip' mission systems capability

AVIATION SERVICES DIVISION

Operates, modifies and maintains more than 150 fixed and rotary wing aircraft around the world

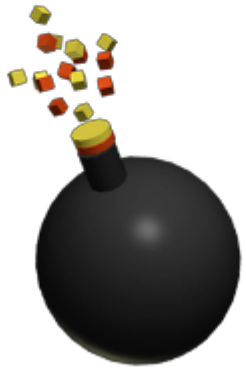
Situation Control

Controlled Zones



- We need to provide an area of controlled network access. This may be for VIP protection purposes or perhaps to prevent the use of mobile phones in prisons for example
- For VIP protection we need to ensure that our agents can still gain access to the real network allowing them to carry a regular mobile phone
- For prevention in prisons, standard jamming prevents phone use but it doesn't allow any intelligence to be gathered
- Deploy Active System Bubble Mode
  - Soft denial
  - Locks all phones in the surrounding area
  - Network coverage appears normal but mimics network congestion for non-agent mobiles
  - Temporary cover. All mobiles are returned to the real network when the system stops transmitting or moves away from the area

Controlled Zones



- A bomb threat is received and it is anticipated that the device may be triggered by a mobile phone
- We need a way to disable the trigger handset and prevent it from rejoining the real network after we have stopped transmitting or have moved away from the area
- Deploy Active System Service Denial Mode
  - Hard denial. Results in disabling of SIM card
  - Handset cannot rejoin the network until its power is turned off and on again
  - Blanket denial or target specific

Private Network

- Your own network in a box!
- Allows communications between agents independently of the real network
  - Secure comms between agents, cannot be intercepted on a strategic intercept system
  - Comms via standard GSM handset
  - Free calls!
- Can be deployed where no real network exists
- Can be deployed when the real network is off air or congested in crisis scenarios ensuring agent communication is maintained

COBHAM

AVIONICS AND SURVEILLANCE DIVISION

End to end avionics and covert surveillance solutions

DEFENCE SYSTEMS DIVISION

Critical technology for network centric operations

MISSION SYSTEMS DIVISION

Complete 'nose to tail' refuelling and 'wingtip to wingtip' mission systems capability

AVIATION SERVICES DIVISION

Operates, modifies and maintains more than 150 fixed and rotary wing aircraft around the world

Examples of Tactical Solutions

Company history

- Owned by Cobham Plc
  - Member of Cobham Surveillance division, which includes:
    - Orion
    - Spectronic
    - Domo
    - Micromill
    - DTC
    - GMS
- 14 years experience in digital communications surveillance
  - Current GSM family is 3rd generation offered by MMI
  - Equipment deployed in over 88 countries
- All development is customer lead
- In house design, development and production
- Regional sales/support offices in Singapore, Washington D.C. and Dubai

Cobham Surveillance (MMI Research Products) Tactical Solutions Product Portfolio

3G/UMTS

GSM

Direction Finding

MMI is able to supply the complete Active surveillance solution

Complete Solution

- Start to end solution, includes
  - full analysis of customer requirements
  - tailored training package
  - complete end of life support.

- All design, development, build and support is done from our UK headquarters.
  - System designed using advanced CAD.
  - Latest technology employed in products. Hardware standards constantly evolving
  - Good engineering practice
    - Designed to meet the relevant European EMC directives

- Regional offices in Singapore, Washington D.C. and Dubai for immediate support response

Summary

- Tactical Active Systems can operate on a standalone basis or complement a strategic system
- Allow the intelligence picture to remain on the target even when they are swapping handsets and SIM cards
- Provide extended capability such as direction finding capability
- Provide control over network access
- Provide a network in a box for crisis scenarios

Any questions?

Thank you

Duncan Askew
Account Manager (EME)
Cobham Surveillance
(MMI Research Products)
T: +44 (0) 1252 848300
M: +44 (0) 7811 382315
E: Duncan.Askew@Cobham.com

EXHIBIT 025

Elaman, *Active Off-Air System 3GN UMTS*, Product Brochure, *available at* http://wikileaks.org/spyfiles/files/0/124_ELAMAN-200805-CATALOGUE-P1.zip (last accessed: May 14, 2012) [Active Off-Air System 3GN UMTS Technical Specification.pdf];

elaman
GERMAN SECURITY SOLUTIONS

GOVERNMENTAL SECURITY SOLUTIONS

Active Off-Air System
3GN UMTS

CONFIDENTIAL – Subject to change without prior notice!

Active Off-Air System: 3GN UMTS

General Overview

The 3GN is a state-of-the-art multi-channel UMTS (WCDMA or 3G) tactical off-air cell phone identity collection system. Using the 3GN, it is possible for the first time to simultaneously collect the identities of UMTS (3G) mobile phones on 2 different UMTS networks or 2 different channels of the same network.

Building on the impressive capabilities of the current product range, the 3GN is capable of working co-operatively with GSM-XPZ. Control is streamlined to allow operation of both systems from a single interface. Users can simultaneously acquire the identities of GSM and 3G phones and display this and other information in a real-time converged database.

When working in tandem with a GSM-XPZ, it is possible to acquire a target phone on UMTS and then 'push' the target onto the GSM-XPZ cell and into a Blind Call for geolocating and tracking purposes.

The native 3G technology is unique in the marketplace in that it has no detrimental effect on 3G phones within its zone of influence. The technology enables control of target mobile phones and normal rejection of non-target mobile phones on 3G. Unlike a jamming solution, non-target 3G mobile phones are caught on 3G and then allowed to continue to use their normal 3G network with no impedance to service.

Main Features

- UMTS Band 1 (2100MHz) operation
- Transmits 2x3GPP configured UMTS cells simultaneously to a maximum of 5W each
- Adjustable Node B transmission power, ranging from 1mW to a maximum of 20W on a single Node B
- Integrated Antenna Switch for up to 3 antennas
- 3G Identify Grabbing using protocol message exchanges rather than 'Jamming'
- Advanced Node B configuration for emulation of any UMTS network
- Fast UMTS cell configuration using optional 3G Spectrum Scanner
- Integrated 2G/3G system operation when connected to a GSM-XPZ system
- User friendly Graphical User Interface (GUI)
- Single combined database for 2G & 3G operation
- Identification whether mobile phone is caught on 2G or 3G
- Powerful database search facility for quick target identification
- 'Push to 2G' function allows specific target mobiles to be assigned to the GSM-XPZ and instantly placed in Blind Call for geo-locating purposes

3GN Specifications

Function	Acquire the identity parameters (IMSI, IMEI & TMSI) of UMTS cell phones off-air from two different UMTS networks simultaneously. 'Push' target cell phones to GSM in a controlled manner for geo-locating. Correctly interact with non-target cell phones to preserve 3G network service in the operational zone.
Channels	Two (2)
Channel Range	UMTS Band 1 (2110-2170MHz)
RF Output Power	2 x 5W max or 1 x 20W max
RF Output Connector	3 x N Type
Size	W 324mm x H 180mm x D 398mm
Weight	16,5kg (20kg including carry case)
Operating Temperature	-5°C to + 45°C
Storage Temperature	-10°C to + 70°C
Power Supply	*12Vdc – 24 Vdc*
Power Consumption	*25A, 600W maximum @ 24 Vdc*

If you would like further Information about ELAMAN,
or would like to discuss a specific requirement or project, please contact us at:

Elaman GmbH
German Security Solutions
Seitzstr. 23
80538 Munich
Germany

Tel: +49-89-24 20 91 80
Fax: +49-89-24 20 91 81
info@elaman.de
www.elaman.de

GOVERNMENTAL SECURITY SOLUTIONS

EXHIBIT 026
EXHIBIT 026 (repeated 32 times down the left side of the page)

ATTACHED EXHIBITS
SECOND SUBMISSION OF CONSOLIDATED EXHIBITS RELATING TO DISCOVERY AND SUPPRESSION ISSUES
CR08-814-PHX-DGC

Elaman, *GSM Vehicle Direction Finder (VDF)*, Product Brochure, *available at* http://wikileaks.org/spyfiles/files/0/124_ELAMAN-200805-CATALOGUE-P1.zip (last accessed: May 14, 2012) [GSM Vehicle Direction Finder-VDF.pdf];

elaman
GERMAN SECURITY SOLUTIONS

GSM Vehicle Direction Finder (VDF)

Technical Specifications

GOVERNMENTAL SECURITY SOLUTIONS

GSM Vehicle Direction Finder (VDF)
Overview

The VDF a complementary product to the GSM-XPZ, is a key element of the MMI solution deployed to locate targets.

Based on the latest military technology, the DFV is a vehicle based direction finding system that significantly addresses the weakness of current direction finding systems. This significantly increases the operational benefit to the customer:

- direction find targets to within a few metres
- azimuth and elevation target resolution
- direction finding on specific GSM timeslots
- multi-antenna array for accurate target resolution
- map overlay of target position data
- covert antenna fit

GSM-VDF Features
The VDF is designed to work in conjunction with the GSM-XPZ product family. Available in 2 options, supporting either the Euro or US bands, location finding of a radiating target mobile can be performed from a vehicle.

Comprising of a multi-antenna array, system unit and laptop the system can be either permanently or temporarily mounted in a vehicle using either an external vehicle antenna or a highly covert internal antenna.

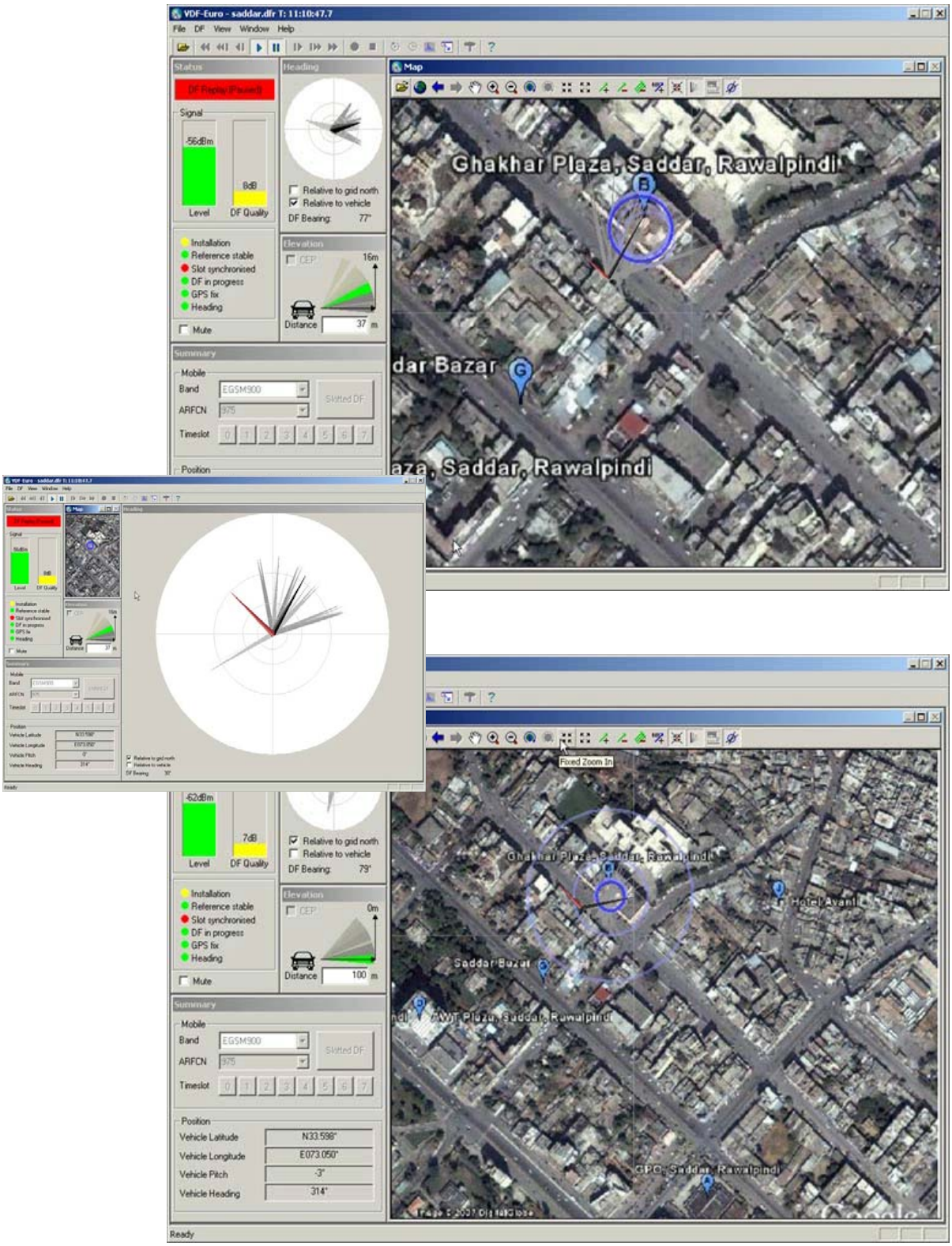
The antennas are very simply calibrated before the start of the mission using a supplied hand-held calibration unit. The key features of the VDF are:

- Direction find to a preset GSM frequency and timeslot.
- Direction find to a preset GSM frequency (for GSM XPZ accurate DF mode)
- Direction find simultaneously in Azimuth and Elevation
- Covert antenna mounted within vehicle or optional roof mount antenna
- Simple GUI display of direction in Azimuth and Elevation
- Display of historic vehicle and direction track
- Map overlay
- Capability for remote interface to other DF and XPZ devices
- Direction given in relation to North and vehicle direction
- Integrated GPS and compass

VDF Specifications

Function

Function:	Provides RF signal strength indication on a selectable RF channel
Channel Range:	Euro: ARFCN 975-1023 , 0-124 , 512-885 US: ARFCN 128-251, 512-810
Direction Finding Axis	Simultaneous in Azimuth and Elevation
Resolution:	Better than 5o
Accuracy	Better than 5o
Power Supply:	12V , 40W
Antenna (covert) :	Azimuth 360o Elevation (as per vehicle aperture)
Antenna (rooftop)	Azimuth 360o Elevation 90o
Mapping Formats	Combined Vector and Raster data ESRI shape file (SHP) Raster data in Band Interleaved by Line (BIL) Bitmap (BMP) Multiresolution Seamless Image Database (MrSID) Portable Network Graphics (PNG) ERDAS Joint Picture Expert Group (JPEG) TIFF and GeoTIFF


VDF-Euro - saddar.dfr T: 11:10:47.7
File DF View Window Help
Status
Signal
-56dBm
Level
8dB
DF Quality
Heading
Relative to grid north
Relative to vehicle
DF Bearing 77°
Elevation
CEP 16m
Distance 37 m
Installation
Reference stable
Slot synchronised
DF in progress
GPS fix
Heading
Mute
Summary
Mobile
Band EGSM900
ARFCN 975
Timeslot 0 1 2 3 4 5 6 7
Position
Map
Ghakhar Plaza, Saddar, Rawalpindi
dar Bazar
aza, Saddar, Rawalpindi
-62dBm
Level
7dB
DF Quality
Relative to grid north
Relative to vehicle
DF Bearing 79°
Elevation
CEP 0m
Distance 100 m
Installation
Reference stable
Slot synchronised
DF in progress
GPS fix
Heading
Mute
Summary
Mobile
Band EGSM900
ARFCN 975
Timeslot 0 1 2 3 4 5 6 7
Position
Vehicle Latitude N33.598°
Vehicle Longitude E073.050°
Vehicle Pitch -3°
Vehicle Heading 314°
Fixed Zoom In
Ghakhar Plaza, Saddar, Rawalpindi
Hotel Avani
Saddar Bazar
GPO, Saddar, Rawalpindi
Ready

GOVERNMENTAL SECURITY SOLUTIONS

If you would like further Information about ELAMAN,
or would like to discuss a specific requirement or project, please contact us at:

Elaman GmbH
German Security Solutions
Seitzstr. 23
80538 Munich
Germany

Tel: +49-89-24 20 91 80
Fax: +49-89-24 20 91 81
info@elaman.de
www.elaman.de

EXHIBIT 027

Ability, *3G Interception & Advanced GSM Active Solution*, PDF provided at ISS World Europe 2008, *available at* http://wikileaks.org/spyfiles/files/0/80_ABILITY-GSM_3G_Intercept.pdf (last accessed: Apr. 10, 2012);

ability

3G Interception

3G-CAT

Interception, Localization and Selective Jamming of 3G (UMTS, WCDMA) Phones

Number of 3G subscribers in the world is growing up rapidly. Defense and security market demands from producers of off-the-air interception systems solutions for 3G phones and their call remains unanswered.

Most popular method used for interception of 3G communications is by using 3G JAMMERS combined with GSM interception systems. The jammers block the 3G channels and 3G phones are forced to migrate to 2G-mode where they can be intercepted.
However, this method has suffers from disadvantages:

1. High power 3G jammers disrupt normal work of 3G networks and it can be easily detected.
2. For interception of a single target, all "innocent" 3G phones in the vicinity of the target are pushed to change into 2G mode.
3. 3G jammer has to be used continually; if it stops operating, 3G phones will return to 3G mode and interception will be eliminated.

Those limitations make usage of such method undesirable and in many cases impossible. The 3G-CAT introduced by Ability is a unique, advanced, state of the art device that overcomes the above limitations with additional meaningful capabilities.

ABILITY COMPUTERS & SOFTWARE INDUSTRIES LTD
17 Hatzefira St, Tel Aviv, Israel 67779 | Tel +972 3 687 9777 | Fax +972 3 537 6483

ability

3G Interception

System main capabilities:

- Multi Network Coverage - automatic detection of 3G networks in all frequency bands.
- IMSI/IMEI/TMSI Catching - detection of all 3G phones and their identities (IMSI, IMEI and TMSI) for the networks of interest.
- Extended Mobile Parameters - detection of additional parameters such as model of mobile phones and country of origin.
- Mobile location - distance to 3G phones is presented with accuracy of less than 30m.
- Force into 2G-Mode - 3G-Cat forces only selected 3G phones into 2G-mode for interception by other 2G systems. Once forced 3G Phones will remain in 2G-mode forever until reboot. This unique feature makes possible and convenient interception of 3G phones by passive and active 2G interception systems.
- Selective "Blocking" - 3G-Cat can completely block selected 3G phones. Such phones will not be able to communicate in all networks including 3G and 2G.
- Selective "Jamming" - 3G-Cat can efficiently work as an intellectual 3G jammer and jam all 3G phones in only selected networks.

3G-CAT can be used either as a stand-alone device or integrated with Ability's IBIS, GTReS of AGIS systems. It can also be integrated with GSM interception systems of other vendors.

Main specifications:

• Number of received networks	Not Limited
• Number of received mobiles	Not Limited
• Operating frequency	3 frequency bands
• Modes of operation	Random / Target
• Jamming capability	Specific targets or specific network
• Maximum Output power	Typical up to 10w
• Power supply	115/230 V AC or 12 V DC

- Optional built in batteries for transportable / man-pack operation

ABILITY COMPUTERS & SOFTWARE INDUSTRIES LTD
17 Hatzefira St, Tel Aviv, Israel 67779 | Tel +972 3 687 9777 | Fax +972 3 537 6483

ability

Advance **GSM** **A**ctive **S**olution

IBIS - II

In Between Interception System
2nd Generation

The IBIS–II is the most advanced and newest GSM interception system in the market. The system was designed and developed according to the vast experience gathered in the last 10 years, while deploying worldwide hundreds of GSM interception systems, listening to customer's feedback and analyzing customer's operational requirements.

The IBIS-II is an advanced integrated active solution that includes all relevant sub systems in a single unit, allows the user to scan, analyze, intercept, monitor, record and track GSM mobiles, regardless if they are encrypted by A5.1 or A5.2 encryption (monitoring is not done by forcing the mobile to use A5.0 or A5.2 but rather by an integrated deciphering capability).

The IBIS–II is a stand-alone solution for off the air interrogation / interception / monitoring / deception of tactical GSM communication, in a seamless way, without any cooperation with the network provider.

The IBIS-II is restricted for Law Enforcement Agencies and Authorized Governmental Agencies and it offers them a powerful tool to intercept and track GSM communication of all types.

ABILITY COMPUTERS & SOFTWARE INDUSTRIES LTD
17 Hatzefira St, Tel Aviv, Israel 67779 | Tel +972 3 687 9777 | Fax +972 3 537 6483

ability

Advance GSM Active Solution

The IBIS-II extracts easily and in short time the mobiles ID's such as IMEI, IMSI & TMSI and allows the user in no time to identify his target mobiles and to monitor them. The IBIS-II offers a complete set of capabilities and advance features to allow the user to control the GSM environment and GSM communication. The user can control the level of service to the target mobiles, selectively Jam specific mobiles, perform silent calls, call or SMS on behalf of target mobile, change SMS messages "on the fly", detect change of SIM card or change of handset, and support Direction Finding system and many additional operational features.

The IBIS-II main capabilities:

- **All GSM in One Single Unit** – the IBIS-II includes all required modules for dual band simultaneous interception in A5.2 and A5.1 environment. No need for any additional hardware.
- **Instant Set Up Time** – without need for external modules, setup is within few minutes only.
- **Dual Band Solution** – any of the required frequencies 850, 900, 1800, 1900MHz.
- **Real Time Interception** – for voice and SMS, Incoming and Outgoing, in A5.1 and A5.2 networks.
- **Semi Passive** - Invisible & undetectable operation, no need for cooperation with network providers.
- **Data Extracting** – system detects mobile identities including IMSI, IMEI, TMSI, MSISDN (phone number), Kc etc.
- **Presence verification** – user can detect presence of specific target mobile.
- **Concurrent Calls** – system Intercepts up to 6 concurrent duplex calls by default.
- **Selective jamming of communication** – user can block communication of GSM phones defined as targets or specific network service (voice, SMS).
- **Direction Finding Support** – by using silent call, target mobile is activated and can be traced by external DF / Homing system.
- **Manipulation** – user can make fake calls and send fake SMS to / from target.
- **Remote Control** – IBIS-II can be operated locally by the system laptop, by LAN connection and remote laptop or via WiFi, by a remote laptop.

System can operate with variety of power sources such as AC supply, batteries, car supply etc and by that, it can be installed and operated in many types of applications and environments (fixed installation, remote control configuration, transportable, vehicular, man pack).

ABILITY COMPUTERS & SOFTWARE INDUSTRIES LTD
17 Hatzefira St, Tel Aviv, Israel 67779 | Tel +972 3 687 9777 | Fax +972 3 537 6483