The Big Black Book of Electronic Surveillance 5th Edition: 2017

Copyright 2017 by Insider Surveillance, Inc.

Contents

The Big Black Book of Electronic Surveillance: 5th Edition

Welcome to *The Big Black Book of Electronic Surveillance: 5th edition (3BES5)*. As a *Buyer's Guide to the Top ISS Vendors,* this is a special work, arguably "unique" in the true sense of the word. We are not aware of another source that endeavors to help customers of Intelligence Support Systems make better-informed decisions on their ISS investments. We believe that our members will find this guide invaluable.

The 5th edition is expanded to include an additional 11 ISS vendors: **Boeing**, **ComWorth**, **DESOMA**, **Elbit Systems CYBERBIT**, **Expert Team, Fifth Dimension**, **NSO Group**, **Ockham Solutions**, **Providence Group**, **Riverbed**, and **Ultra Electronics**. It is updated throughout to show new products and services by key vendors. We have removed companies that merely resell without innovating: the UK's **ComsTrac**, Germany's **PKI**, Ireland's **Accuris Networks** and India's **Fastech**, as well as niche players such as **Vocal** and **Zimbra** of the U.S. Finally, when a vendor is affiliated with a failed program yet touts it as a success, as **Modus Operandi** does re: the U.S. military's DCSG-A program – a boondoggle that cost American lives – they're out.

In our 4th edition we observed that the world has entered a new "Dark Age" of terrorism. According to the U.S. State Department "Country Reports on Terrorism 2015," 11,744 terrorist attacks occurred in that calendar year, leading to 28,328 deaths. While the State Department reported this as a decline of 13 percent over the prior year, the attacks in 2015 took a different, more sinister turn that no doubt escalated in 2016. As military pressure on ISIS condensed the geographic area it controlled, the Caliphate encouraged "home grown" Islamic fanatics to take the lead on terrorism. Mass immigration of civilians from conflicts throughout the Middle East and North Africa contributed to this trend. While the vast majority of immigrants into Western Europe and elsewhere were harmless, there is no question that some arrived with evil intent.

The combination of native and newcomer terrorists fueled an outbreak of "lone wolf" violence in France, Belgium, Germany, Canada, the United States and elsewhere. European nations were quick to respond.

Following the "Charlie Hebdo" attack in Paris in January 2015, France enacted laws that provide greater surveillance powers to police and government intelligence. Germany joined this movement n January 2016, implementing its own stricter surveillance law. Following July's gun attack in Munich and attempted suicide bombing in Ansbach, and the December 19 semi-truck rampage against Christmas shoppers in Berlin, German legislators have proposed new laws that will increase the deployment of surveillance cameras in all public places.

Across the Channel, the British Parliament in November 2016 passed The Investigatory Powers Act. The Act significantly extends the powers of law enforcement, requiring service providers to retain and provide "Internet Call Records" on demand for any and all Web communications including social media. The law also empowers LEAs to collect bulk metadata and mandates "equipment interference," mandatory back doors that compromise end-to-end encryption and provide access to any network hardware or end user device.

Despite high profile terrorist attacks in San Bernardino, CA and Orlando Florida, the United States has undertaken no serious national security policy changes since enacting of The USA Freedom Act, which took a major step back from strong surveillance policy by discarding Section 215 of The Patriot Act – the provision allowing bulk metadata collection. Other U.S. surveillance laws such as The Communications Assistance for Law Enforcement Act (CALEA) are, in comparison to those of other nations, seriously antiquated. CALEA, now entering its 22nd year, has no provision for monitoring social media, and is not likely to be updated in the foreseeable future. The Edward Snowden overhang on national security policy remains strong nearly four years after the fact.

ISS vendors of necessity operate in secrecy. *Insider Surveillance* endeavors to bring them out of the shadows for the benefit of their customers, reviewing ISS vendors and their products to help inform better purchase decisions. The best vendors are presented here in *3BES5*.

3BES5 is structured in 10 chapters, each dedicated to a specific type of vendor and its technology solutions: *Trusted Third Party* providers; makers of *Lawful Intercept Solutions; Packet Monitoring; Mobile Location; Biometric Identification; Ethical Malware; Advanced Analytics; Forensics solutions; OSINT and Social Media Monitoring;* and *Military Intelligence.*

Note that many ISS companies are multi-play vendors that operate in more than one niche. As in any marketplace, competition drives diversification. Cross-referencing in *3BES5* shows when a vendor offers more than one type of ISS solution.

3BES5 reflects the dynamism of the marketplace. Among the highlights since our 4th edition was released in June 2016:

- **Cisco** ventured into mobile location with its Hyperlocation solution for WiFi networks.
- Italian regulators suspended malware vendor **The Hacking Team's** export license.
- Through partnership with **Vencore**, real time threat analysis specialist **Recorded Future** now offers detailed geospatial intelligence on targets.
- **Nuance** acquired Spain's **AGNITIO**, creating a global powerhouse in voice biometrics.
- Germany's **PLATH Group** expanded from RF monitoring to enter the markets for cybersecurity and its opposite – ethical malware.
- **Verint** made major advances into advanced analytics, OSINT, social media monitoring, the Deep Web and the Dark Web.
- **46 Labs** of Austin, TX on Sept.16, 2016 purchased the tech assets of US-based lawful intercept vendor **SwitchRay** and SwitchRay parent company **MFI-Soft** – of Russia.
- **BrightPlanet** exited social media monitoring by dropping Blue Jay – a unique product with malware capability – but remains active in Deep Web Monitoring.

Because the surveillance business never stands still – nor do policymakers and terrorists – *3BES5* will continue to be a work in progress with regular updates. We hope you find this book helpful, and as always, we welcome your input.

Chapter 1: Lawful Intercept Providers – "Trusted Third Parties"

"Lawful intercept" (LI) is the process of obtaining signaling data, call records or full content of communications via court order or subpoena to support a criminal or terrorist investigation. With the rapid growth of technology, lawful intercept has leapt from the simple voice "wiretap" of yesteryear to include the capture of data, signaling and content from mobile networks, as well as from IP, broadband and "cloud" services.

Laws governing electronic surveillance are equally complex. In many nations there is no single law with oversight. Rather, like the technologies involved in lawful intercept, laws have evolved to have integrated functionality. United States surveillance law is a case in point.

In the United States, law enforcement agencies (LEAs) conduct lawful intercept via an interconnected framework of laws:

- Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("The Wiretap Act");
- The Foreign Intelligence Services Act (FISA) of 1978;
- The Electronic Communications Privacy Act (ECPA) of 1986;
- The Stored Communications Act (SCA), enacted as Title II of ECPA in 1986;
- The Communications Assistance for Law Enforcement Act (CALEA) of 1994;
- The Patriot Act of 2001, which amended FISA and ECPA;
- The 2005 FCC Order extending CALEA to apply to *facilities-based* providers of Internet, broadband and Voice over IP (VoIP) services that connect to the public switched telephone network (PSTN) – but exempting "over the top" services, i.e., those *not* connected to the PSTN;
- The FISA Amendments Act (FAA) of 2008, principally Section 702 on requirements for NSA surveillance of non-US targets within the U.S. under *PRISM* (downstream collection from ISP servers of Google, Apple, Yahoo, Facebook, Skype, etc.) and upstream (directly from cables and other network infrastructure).
- The USA Freedom Act of 2015, reauthorizing most aspects of the Patriot Act but eliminating Section 215, by and large ending bulk metadata collection by the NSA.

In the United States, LEAs use these laws to conduct lawful intercept over networks operated by communications service providers (CSPs), which in turn must have in place the technology solutions and expert staff to support court orders for lawful intercept. Court interpretation and administration of surveillance laws may vary state to state. For example, the use of mobile location technologies varies widely depending on jurisdiction and applicable case law.

Failure to comply with surveillance laws carries stiff penalties – in the case of CALEA, fines of up to US $10,000 per day. As yet, however, there is no known instance of a CSP being fined for non-compliance. With the emergence of broadband and over-the-top services, a growing number of service providers believe they are exempt from the law. Quite often they are wrong. The rule of thumb: If a carrier's service interconnects at any point with the public switched telephone network (PSTN), it is subject to the rules of CALEA and must have a technology solution in place to facilitate lawful intercept upon receipt of a valid court order. CALEA applies not only to wireline and wireless carriers, but to broadband and VoIP providers whose networks touch the PSTN. Social media services are exempt from CALEA compliance.

CSPs may either purchase, deploy and manage the technology solutions required for compliance themselves – as the largest tend to do – or hire a Trusted Third Party (TTP) to help. In either event, when a CSP has in place a solution that meets the technical standards of CALEA, it is considered to be in "safe harbor," i.e., in compliance with law.

Putting and keeping CSPs in "safe harbor" with CALEA is the principal mission of TTP LI vendors. Some TTPs operate as service bureaus that provide end-to-end CALEA compliance. "End-to-end" means they: (1) deploy, test and maintain the technology solution; (2) provide in-house legal counsel to review and confirm the accuracy of court orders received by a CSP; (3) implement the intercept as detailed in the court order; (4) ensure that the intercept follows the strict privacy protections outlined in CALEA; (5) employ former law enforcement officers to liaise with the LEA in charge of the investigation; and (6) shut down the intercept when the court order's time stamp expires. Other TTPs simply sell CALEA tech solutions.

New regulations add to the complexity and cost of lawful intercept. For example, in the U.S., federal authorities now require vendors and CSPs to partition LTE technology solutions so that they will not intercept Voice over LTE (VoLTE) and VoIP unless such communications are specifically targeted by a court order. The upshot: Vendors must now reconfigure LTE lawful intercept technology solutions to follow the rules.

CALEA is generally perceived as the principal law governing U.S. lawful intercept.
That said, the bulk of activities undertaken by TTPs often pertain to FISA and Wiretap Act court orders requested by the U.S. Federal Bureau of Investigation.

The companies shown in Table 1 are Trusted Third Parties that help service providers meet their legal compliance requirements in the United States and other nations.

Table 1: Lawful Intercept Providers – Trusted Third Parties

Company	Location	Solution	Function	Market	Of Note
Apogee	Austin, TX, USA.	**SIS (Secure Intercept Service).**	**SIS**: Service Bureau model. Provides full administration of court orders, liaison with LEAs and a technology platform that includes: raw data and command & control messaging; Apogee processing system; LEA mediation, verification, & intercept.	CSPs, LEAs, universities.	Partners with Cisco and SS8.
Subsentio	Centennial, CO, USA.	**Verint STAR-GATE.** **Safe Harbor Mediator.** **Safe Harbor 1GB Probe.** **Safe Harbor 10GB Probe.** **Safe Harbor Probe for LTE.** **Safe Harbor CALEA in the Cloud.**	**Verint STAR-GATE:** Mediation device connects with network hardware to collect evidence. **Safe Harbor Mediator** Mediation device. Currently applicable to SONUS network devices only. **Safe Harbor 1GB Probe:** Passive probe with 1GB throughput. **Safe Harbor 10GB Probe:** Passive probe with 10GB throughput. **Safe Harbor Probe for LTE:** Passive probe for LTE networks. **Safe Harbor CALEA in the Cloud.**	CSPs and FBI's NDCAC (National Domestic Communications Assistance Center).	Trusted third party (TTP) service bureau: Sells active and passive LI tech solutions + provides court order review, LEA liaison and warrant management. Acquired lawful intercept and Records Productions assets of Neustar, June 1, 2015. Resells Verint STAR-GATE. Other Safe Harbor products are made by a partner company. **See more on Verint STAR-GATE under "Lawful Intercept Solutions."**

Subsentio (continued)		**Safe Harbor sProbe.** **Records Production.**	Passive probe linked to Subsentio Network Operations Center. **Safe Harbor sProbe:** Low-cost subprobe remotely configured & managed. Target market: broadband & VoIP CSPs. **Records Production:** Warrant & subpoena requests management.		
Yaana Technologies	Milpitas, CA, USA.	**Request Management System.** **Data Retention System.** **Lawful Interception System.** **4G/LTE Lawful Interception System.**	**Request Management System:**Records Production. **Data Retention System:** Storage of intercepted data. **Lawful Interception System:** Mediation device. **4G/LTE Lawful Interception System:** Mediation device for for 4G/LTE.	CSPs, LEAs.	Relative newcomer to LI. Primary focus through 2013: data retention. Entered LI business (2014) with NetCompliance mediation & cloud-based solutions. Expanded to DPI & DPI analytics in 2015 via acquisition of IP Fabrics. Introduced Tunnelbox ethical malware, (May 2016). Company is active in global markets; recently appointed manager of UK operations. **Also see Yaana Technologies in "Packet Monitoring" and "Malware."**

Chapter 2: Lawful Intercept Solutions – "Active" versus "Passive"

This chapter covers vendors that offer devices and solutions that use either of the two principal technical approaches to lawful intercept: "active" and "passive." A third approach, "CALEA Compliance in the Cloud," typically involves a passive solution installed at the network edge and connected to a TTP's Network Operations center (NOC) or LEA monitoring center and are included in the "passive" category.

Active solutions consist of appliances and software that are deployed *within* a communications service provider network. Active solutions are two-part: (1) "lawful intercept modules" [software] installed in network hardware such as conventional or soft switches and routers; and (2) mediation devices.

In the case of an active solution: When a CSP or trusted third party acting on the CSP's behalf receives a court order for lawful intercept, an engineer activates the mediation device to program hardware-based software modules on specific traffic to track. These modules intercept the traffic and route it to the mediation device, which packages the data in the proper protocols before sending it to a designated LEA, or multiple ones engaged an investigation.

Passive LI solutions, known as probes, are network-independent, that is, they are deployed on the edge of the network, *not within* the network on existing hardware. When a communications operator receives a court order for surveillance, the carrier – or its designated trusted third party vendor – activates the probe to intercept communications traffic of the targeted suspect.

As a newer alternative to mediation devices, probes are made for capturing the dominant mode of modern communications, IP. Probes are provisioned to look for identifiers specified in a court order, such as telephone numbers, IP addresses and urls. They also use Deep Packet Inspection (DPI) capabilities to single out protocols of signaling such as Session Initiation Protocol (SIP) and then unobtrusively capture or "mirror" metadata and content. Probes may be used to intercept traditional circuit-switched voice and data. A probe may also be part of a hybrid system, intercepting data which is then routed to a mediation device for formatting and delivery to the LEA.

One drawback of probes: Many are less scalable than mediation devices. Probes are typically available in 1GB and 10GB models. A 1GB probe might "listen" to between one and four 1 GB streams simultaneously. A mediation device can scale to handle multiple networks, targets and concurrent sessions.

One plus for probes: lower cost. Active solutions often begin in the "low six figures" owing to the high cost of software, which escalates with the size of the network and the number of LI modules, traffic types and volumes to be intercepted. Passive solutions may be purchased for a fraction of that amount. Hosted cloud-based passive systems are even more economical.

Table 2: Lawful Intercept Solutions – "Active versus "Passive"

Company	Location	Solution	Function	Market	Of Note
46 Labs	Austin, TX,USA.	**Sormovich E1T Probe.** **SORM 2 Mediation.** **SORM Converters.** **Perimeter F Deep Packet Inspection.** **SORM 3 Metadata Retention.**	**Sormovich E1T**: Passive probe. **SORM 2 Mediation**: Active mediation device. **SORM Converters**: For using ETSI-compliant devices with Russian SORM products. **Perimeter F Deep Packet Inspection**: DPI hardware. **SORM3 Metadata Retention**: For data acquisition and processing. Includes a storage module with a control unit for handling searches.	CSPs.	46 Labs purchased tech assets of SwitchRay, U.S. arm of Russia's MFI-Soft (Sept. 2016). Previously MFI-Soft serviced Russia and CSI. SwitchRay serviced U.S., Canadian and LATAM customers. How product nomenclature, CALEA/ETSI compliance and intl. marketing will play out remains to be seen. Product names shown here are MFI-Soft. SORM is Russia's lawful intercept law.
Aculab	Milton Keynes, UK + offices in Germany & USA.	**ProsodyX.**	**ProsodyX:** Mediation device.	CSPs.	Acquired Prosody (2003). Partners with NSF Telecom. **Also see Aculab in "Mobile Location."**
Altron	Kharkov, Ukraine.	**AMUR-IP.**	**AMUR-IP:** IP Telephony intercept & recording.	CSPs, ISPs, LEAs.	
AQSAQOM	Paris, France. Melbourne, Australia. + Washington., D.C., USA.	**ALIS.**	**ALIS:** Mediation platform for PSTN, GSM, GPRS, 3G, LTE, CDMA, WCDMA, VoIP, xDSL and SATCOM networks.	CSPs, Govt.& Intel. agencies, LEAs.	**Also see AQSAQOM in "Mobile Location."**

AQSAQOM (continued)		**ALIS HP & VHP.** **ADRIS.**	**ALIS HP & VHP:** "High Performance" (HP) and "Very High Performance" (VHP) mediation platform for lawful interception at GB speeds. **ADRIS:** Data retention for intercepts from all network types. Provides ability to merge data from LI with OSINT.		
ATIS UHER	Bad Homburg, Germany.	**Klarios TKU Monitoring Centre.** **Klarios AIMS**. **Klarios Interception Controller.** **Klarios TLMS.** **Klarios IDEC.**	**Klarios TKU Monitoring Centre:** Centrally administered monitoring center for PSTN and IP network traffic intercepts. **Klarios AIMS**: Mediation device. **Klarios Interception Controller**: Configures LI in Klarios AIMS or other mediation devices. **Klarios TLMS:** Trunkline monitoring center uses multiple DPI devices to manage and mirror IP traffic. **Klarios IDEC:** Separate DPI unit for decoding encrypted traffic.	CSPs, Govt. agencies, LEAs, Military.	Acquired IP Fabrics (2011), then sold it to Yaana Technologies (2015). **Also see ATIS UHER in "Mobile Location," "Advanced Analytics," and "Military."**
BAE Systems Applied Intelligence	Guildford, UK.	**DataBridge Suite**.	**DataBridge Suite:** Mediation device and DPI probes. CALEA and ETSI compliant.	LEAs.	**Also see BAE Systems in "Advanced Analytics."**

ClearTrail Technologies	Indore, India.	**ComTrail Interception Suite.** **xGTrail.**	**ComTrail Interception Suite**: Passive probes. **xGTrail**: Passive probe for tactical DPI.	Wireless CSPs, LEAs	**Also see ClearTrail in “Mobile Location,” “Packet Monitoring,” “Malware” and “Advanced Analytics.”**
CommuniGate Systems (a Stalker Software Inc. company)	Larkspur, CA, USA.	**CommuniGate Pro Server.**	**CommuniGate Pro Server**. Monitors and records VoIP calls and messages and target’s login and usage data. Compiles and relays this data to external tools to translate recorded data.	ISPs, LEAs.	
CRYPTON-M	Kiev, Ukraine.	**TerraLIS.** **TerraNET 10G.**	**TerraLIS**: mediation device compatible with CALEA and ETSI + Russia’s SORM standards. **TerraNET 10G**: passive probe.	LEAs, Govt. & Intel. agencies.	**Also see CRYPTON-M in “Mobile Location” and “Military.”**
DigiVox	Rotterdam, Netherlands	**MAGNA Lawful Intercept Solution.**	**MAGNA:** DPI software built into commercial off the shelf hardware from XYLON. Can be outfitted with cards for active/passive intercept. Integrates with XYLON mediation hardware and monitoring center.	CSPs, LEAs.	Hardware-provider XYLON is based in Zabreb, Croatia.
Dreamlab Technologies	Bern, Switzerland. Schwindegg, Germany. Santiago, Chile.	**LI-IPS**.	**LI-IPS**: Mediation device.	CSPs, LEAs.	Formerly re-sold FinFisher malware but disavowed the relationship in 2013.

Group 2000	Almelo, Netherlands. Oslo, Norway. Freienbach, Switzerland. Wilmington, DE, USA.	**LIMA Lawful Interception.** **LIMA Disclosure Management.**	**Lima Lawful Interception**: Mediation device with data retention and analytics. Integrates with intelligence including financial records, social media, video surveillance, OSINT, location data from metadata and content. Suite includes DPI capability for 300+ applications. **LIMA Disclosure Management**: Records production.	CSPs, LEAs.	**Also see Group 2000 in "Mobile Location," "Biometric Identification," and "OSINT & Social Media Monitoring."**
HP Enterprise	Palo Alto, CA, USA.	**HP DRAGON Manager.** **HP Network Probe.** **HP DRAGON Blue.** **HP Autonomy.**	**HP Dragon Manager**: Warrant management. **HP Network Probe**: LI via DPI for traffic monitoring. **HP Dragon Blue**: DPI at Layer 7 of OSI stack for full packet payload. **HP Autonomy**: video surveillance & analytics.	CSPs, LEAs.	Effective March 2017 HP Enterprise Services Division (including ISS) is acquired by Computer Sciences Corp. **Also see HP Enterprise in "Advanced Analytics."**
INNOVA	Trieste, Italy.	**EGO.** **IP Probes.** **Micro IP.**	**EGO**: ETSI-compliant lawful intercept system for wireline, mobile & IP traffic; built-in analytics. **IP Probes**: For Web, email, SMS, IP video, social media. **Micro IP**: High quality audio	LEAs.	

INNOVA (continued)		**GPS Innova.** **RB800.**	interception device for vehicle tracking. **GPS Innova**: Real time tracking via tablet; can be sync’d with Micro IP audio. **RB800**: Miniature audio recording device.		
iPS	Aprilia, Italy.	**GENESI NIP.** **GENESI NIP Packet Switch Probe.**	**GENESI NIP**: Mediation device. **GENESI NIP**: Passive or in-line DPI probes.	CSPs, ISPs.	**Also see iPS in “Mobile Location,” “Malware,” “Advanced Analytics,” “Biometric Identification,” and “OSINT and Social Media.”**
Elbit Systems CYBERBIT	Ra’anana, Israel.	**Target 360°.**	**Target 360°:** Mediation devices and probes that integrate with the full range of end-to-end CYBERBIT solutions.	LEAs.	Acquired NICE Systems Cyber & Intel Division (May 2015). **Also see Elbit Systems CYBERBIT in “Advanced Analytics,” “Mobile Location,” “Biometric Identification,” “Malware,” “OSINT and Social Media” and “Military.”**
NORSI-TRANS	Moscow, Russia.	**Vitok-IMS.** **Vitok-TAP-8E1.** **Vitok IPTel.** **Vitok-SDH.**	**Vitok-IMS:** Probe monitors targets on IP Multimedia Subsystems networks. **Vitok-TAP-8E1:** Probe for non-intrusive signal tap for E1 streams. **Vitok IPTel:** Probe for VoIP. **Vitok-SDH:** Probe specific to	CSPs, LEAs, Govt. & Intl. agencies	NORSI-TRANS solutions are SORM AND ETSI compliant. **Also see NORSI-TRANS in “Packet Monitoring,” “Mobile Location,” Advanced Analytics” and “OSINT and Social Media.”**

NORSI-TRANS (continued)		**Vitok-E1.** **Vitok-Concentrator.** **Vitok-HUB.** **Yakhont-TLF.**	SONET/SDH traffic on fiber optic networks. **Vitok-E1:** Probe for multiplexed E1/PDH/PCM-30 digital lines. **Vitok-Concentrator:** “Hub” that retrieves intercept data from probes. **Vitok-HUB:** Mediation device that collects and formats intercept data for transmission to monitoring control center. **Yakhont-TLF:** Voice transaction data retention for smaller CSPs, offered in desktop format with small rack-space mounting requirements. Collects intercepted wireline, mobile, private network, radio or SATCOM.		
NSF Telecom	Westendintie (Helsinki) Finland.	**NSF IP traffic Monitor.** **NSF Melody.**	**NSF IP traffic Monitor**: DPI. Lightweight collectors can monitor several network devices and local area networks. Captures source destination address, ports, protocols. **NSF Melody**: Mediation device normalizes multiple data sources.	CSPs, LEAs.	Spun off from Ericsson in 2002. Partners with Aculab.

NSF Telecom (continued)		**NSF TTAnalyzer.**	**NSF TTAnalyzer**: Allows events to be examined independent of call data records.		
Packet Forensics	Tempe, AZ, USA.	**M1.** **M1S.** **5BG3.** **cQuery DNS Internet Directory Service.**	**M1:** Packet Forensics' lowest-cost carrier grade probe for Ethernet, IP and MPLS networks. Provides mediation functions and 8GB storage capacity. **M1S**: Mid-range probe for interception of Ethernet, IP and MPLS traffic. Includes Ethernet probe, integrated mediation server and accelerated cryptography. **5BG3**: Top-of-line probe for Ethernet, IP and MPLS. Triggers intercepts based on IP, MAC, keywords, RADIUS, DHCP, VoIP calls, behavior or other criteria. **cQuery DNS**: Makes DNS inquiries anonymous.	CSPs, LEAs, Govt. & Intel. agencies.	**Also see Packet Forensics in "Packet Monitoring."**
PALADION	Bangalore & Mumbai, India.	**Internet Monitoring Solutions.**	**Internet Monitoring Solutions**: DPI for tactical single operator, multi-operator and nationwide platforms.	CSPs, LEAs, Govt. & Intel. agencies.	450 customers in 15 countries. **Also see Paladion in "Mobile Location," "Malware," "Advanced Analytics," and "Forensics."**

PALADION (continued)		**Telecom Operator Interception System (TIS).**	**Telecom Operator Interception System**: Mediation device.		
Pen-Link	Lincoln, NE, USA.	**Pen-Link 8.** **LINCOLN Collection Systems.** **LINCOLN Collection Server.** **LINCOLN Access Points.** **Pen-Proxy.**	**Pen-Link 8**: Administration, reporting and analysis software for CALEA solutions. **LINCOLN Collection Systems**: LAN server for terminating intercepts from CSP. **LINCOLN Collection Server**: Terminates and stores intercepted content. **LINCOLN Access Points**: Pen register metadata collection. **Pen Proxy**: Real time alerts of changes in target activity. Interfaces with other services, mobile location.	CSPs. LEAs.	CALEA compliant.
Pine Digital Lawful Interception	The Hague, Netherlands.	**EVE.**	**EVE**: Modular Lawful intercept solution with “building blocks” for 1GB/10GB passive probe, or active mediation. Integrates to monitor any network including LTE & VoLTE. Supports all LEA protocols, and both CALEA and ETSI standards.	CSPs, LEAs.	

RCS Labs	Milan, Italy.	**MITO^3 Monitoring Center.**	**MITO^3 Monitoring Center**: Intercepts & records metadata and content. DPI function extracts metadata and content from IP communication. Includes module for analytics and visualization.	LEAs, Govt. & Intel. agencies.	**Also see RCS Labs in “Mobile Location,” “Malware,” “Advanced Analytics,” and “OSINT and Social Media.”**
Roke Manor Research (a Chemring Group company)	Romsey, Hampshire UK.	**Vanguard System.** **Pico Probe**. **Aquila Deep Packet Probe.** **Packet Capture and Analysis.**	**Vanguard System**: Provisions & manages mediation device. **Pico Probe**: Miniature passive probe. **Aquila Deep Packet Probe**: DPI for multiple channels. Scalable from 10GB to 100GB per channel. **Packet Capture and Analysis**: DPI software compatible with any hardware. Scalable from 100MB to 10GB.	CSPs, LEAs, Govt. & Intel agencies, Military.	Chemring Group: UK-based Military electronics contractor with worldwide offices. **Also see Roke Manor Research in “Advanced Analytics,” “Forensics,” and “Military.”**
Savvius	Walnut Creek, CA, USA.	**WildPackets Lawful Intercept Software Package (LISP).**	**WildPackets Lawful Intercept Software Package:** Captures and classifies packets. Uses DPI with specialized plug-ins for lawful intercept to capture, decrypt and analyze VoIP, SMS, FTP sessions, web surfing, Radius traffic. Performs man-in-the-	LEAs.	LISP is sold under the old WildPackets brand name. **Also see Savvius in “Packet Monitoring” and “Forensics.”**

Savvius (continued)			middle attack on SSH. Can also be used for pen registers to capture call and IP metadata.		
Septier	Petach Tikva, Israel.	**Septier Mediation.** **Septier Monitoring Center.**	**Septier Mediation**: Mediation platform targets, captures, processes and delivers metadata and content of mobile calls. **Septier Monitoring Center:** CALEA and ETSI-compliant. Includes LI provisioning, data capture, mediation and delivery.	CSPs, LEAs, Govt. & Intel. agencies.	**Also see Septier in “Mobile Location,” “Advanced Analytics” and “Military.”**
Shoghi Communica-tions	Himachal Pradesh, India.	**SCL-LISF.**	**SCL-LISF:** ETSI and CALEA compatible mediation device for PSTN, ISDN, wireless and VoIP. Scalable to multiple E-1s. Optional CDR analytics.	CSPs, ISPs. LEAs.	**Also see Shoghi in “Mobile Location” and “Military.”**
SIEMENS Convergence Creators, GMbH	Vienna, Austria.	**LIOS ONE**.	**LIOS ONE:** Mediation device and data retention system.	CSPs.	
SS8	Milpitas, CA, USA.	**Xcipio Platform.** **Xcipio Mediation Solution for VoIP**.	**Xcipio Platform:** Mediation device for PSTN, IP & mobile operators including LTE. **Xcipio Mediation Solution for VoIP:** VoIP interception.	CSPs, ISPs, LEAs.	**Also see SS8 in “Packet Monitoring,” “Malware” and “Advanced Analytics.”**

SSI Pacific	Melbourne. Australia. Wellington, New Zealand. Singapore.	**Monitoring Centre.** **LIMS.** **NIC (National Information Centre).** **Warrant Management System.**	**Monitoring Centre:** Overall management of lawful intercept. **LIMS:** Mediation device compliant with ETSI, 3GPP, ANSI/ATIS and CableLabs. **NIC:** Data retention. Real time access to all connected data sources, internal or external, in their original format. **Warrant Management System:** Electronic records production and management.	CSPs.	Partners with Trovicor and Utimaco. Claims 90 deployments worldwide.
Suntech – Verint Group	Florianópolis, Brazil.	**Vigia IP.** **Vigia Web Viewer.** **RELIANT.** **IP Decoding Studio.** **Verint STAR-GATE.**	**Vigia IP:** Passive probes capture metadata and content from PSTN, mobile and IP networks. **Vigia Web Viewer:** Real time access to lawful intercept data for LEAs. **RELIANT:** DPI captures and filters voice, internet, mobile and fixed satellite and cellular. Includes analytics module. **IP Decoding Studio:** Layer 7 DPI for apps and content. **Verint STAR-GATE:** active mediation system.	CSPs, LEAs, Govt. & Intel. agencies.	Suntech acquired by Verint (August, 2011). Partners with Cisco, Ericsson, Acme Packet (Oracle). Claims to own 90% of the LI market in Brazil. Clients include Embratel, Claro, TIVO. **Also see Suntech in "Mobile Location" and "Advanced Analytics."**

Syborg – Verint Group	Bexbach, Germany.	**Syborg Interception Center (SIC).** **Sgate.** **SIC for ISPs.** **SIC for Tactical.**	**Syborg Interception Center (SIC):** Captures, mediates and analyzes metadata & content. **Sgate**: Mediation device. **SIC for ISPs**: DPI probes. **SIC for Tactical**: Tactical solutions for ADSL, ISDN and WiFi.	CSPs, LEAs, Govt. & Intel. agencies.	Syborg acquired by Verint (August 2011). Swiss hired Verint in January 2014 to replace national *Interception System Schweiz* developed by Syborg, 2002. **Also see Syborg in “Mobile Location.”**
Thales	Neuilly-sur-Seine, France.	**SMART INT.**	**SMART INT:** Based on legacy product, **Cell Spyder**: Passive probe that collects calls/data. Includes management center that selects targets and processes data for LEAs.	LEAs, Govt. & Intel. agencies, Military.	Thales’ “Plateforme Nationale des Interceptions Judiciaires” (PNIJ), a national platform for lawful intercept and govt. intelligence, remains inoperative owing to inter-agency turf battles. The PNIJ was first proposed in 2010, and was to have launched in 2014, but has not progressed beyond testing. **Also see Thales under “Packet Monitoring” and “Military.”**
TraceSpan	Ra’anana, Israel.	**GPON Phantom.** **DSL Phantom.**	**GPON Phantom:** Passive interception of optical fiber in FTTx topology. **DSL Phantom:** Captures, stores	Cable MSOs, LEAs.	All TraceSpan units may be used standalone, or integrated with LI systems.

TraceSpan (continued)		**VDSL2 Phantom**	and records data from ADSL. **VDSL2 Phantom:** LI on VDSL2 lines.		
Trovicor	Munich, Germany.	**Fusion System.**	**Fusion System:** Monitoring suite for lawful intercept. Location, analytics and OSINT features, e.g., integrates with social media and financial data.	LEAs, Govt. & Intel. agencies.	**Also see Trovicor under “Mobile Location,” “Malware,” “Advanced Analytics” and “OSINT and Social Media.”**
Utimaco	Aachen, Germany. Palo Alto, CA, USA.	**Utimaco LIMS (Lawful Intercept Management System).** **LIMS Access Points**. **Data Retention Suite.**	**LIMS**: Centralized management of active and passive devices. **LIMS Access Points**: Carrier grade DPI probes ranging from 100/1000MB to 10GB. **Data Retention Suite:** Records product and warrant management.	CSPs – fixed & mobile.	Utimaco was acquired by UK security firm Sophos (2009). Utimaco partners with Safesoft (Budapest – biometrics) and SkyTECH Asia (Hong Kong – social analytics). Uses Procera DPI.
Verint	Melville, NY, USA.	**STAR-GATE.** **VANTAGE Monitoring Center.** **RELIANT Monitoring Center.**	**STAR-GATE**: Active mediation device. **VANTAGE Monitoring Center**: Mass and target interception. Intercepts, filters analyzes voice, Internet, mobile, fixed satellite. **RELIANT Monitoring Center:** stream**li**ned version of VANTAGE. Can target LTE/LTE-A, UMTS, GSM, xDSL, Cable, VoIP, IMS.	LEAs.	CALEA compliant; used in more than 75 countries. **Also see Verint in “Advanced Analytics,” “Mobile Location,” “Military” and “OSINT and Social Media” and “Malware.”**

Chapter 3: Packet Monitoring

Packet monitoring technologies are an outgrowth of network management and analytics, subsequently applied to ISS. Current thinking revolves around three approaches: *Deep Packet Inspection*; *IP Flow Monitoring*; and *Network Packet Brokers.* All are used in both commercial enterprises as well as lawful intercept and other intelligence gathering areas.

In the ISS arena, packet monitoring technologies are nearly always deployed in Lawful Intercept Solutions for the purpose of monitoring IP networks. DPI, IP Flow Monitoring and Network Packet Brokers may also be used standalone for other surveillance needs.

Although we treat the three types of solution as “separate” here for academic purposes, they perform similar tasks and often use aligned technology platforms. All collect and analyze packets. Many rely on field programmable gate array (FPGA) hardware accelerators to speed performance. Finally, the three packet monitoring solutions may be combined in various ways. One often sees IP Flow Monitoring paired with DPI, the former to sample anomalous packets on high-speed networks, and the latter to perform full inspection of the suspect packets.

Deep Packet Inspection

Deep packet inspection is a multi-purpose tool, a primary vehicle for intercepting and inspecting data communications, as well as for improving the efficiency of networks based on identification and prioritization of traffic. In both disciplines, DPI has the power to determine the traffic and application type, protocol, origin, content and destination of every packet of data that transits a network – or of specifically targeted data streams.

There is little agreement on when or where DPI began, or even if it is qualifies as a “technology.” Like many developments in the tech and networking world, DPI represents an evolution and agglomeration of capabilities. Many features common to DPI, such as packet sniffing and packet inspection as part of the routing process, were in existence for many years before the term “DPI” surfaced to define the combination of these and other functions.

DPI, like the older version of packet inspection, focuses on live data. But unlike classic packet inspection, DPI goes doesn’t stop at un-packing the packet header. DPI opens the entire packet or any part therein including the payload.

DPI also does far more than decide where to route a packet. It analyzes bit streams to perform two core functions essential to surveillance: recognition and notification of patterns. A third DPI function, manipulation, is widely deployed on the commercial side, as well as by nation states to censor or block access to outlawed Web content.

Exactly what a specific DPI application recognizes depends entirely on the patterns or trends it is programmed to identify. This function, controlled in the DPI Engine, might tell the DPI applications to search for and single out particular protocols, urls, content, applications, text strings, malware exploits or specifically formatted data such as a credit card number.

The rules that are programmed into and from then on direct the DPI Engine have various names including “expressions,” “signatures,” “rules sets” and “fingerprints.” Important note: the DPI app will only act on the rules in the DPI Engine, nothing else. Omit a rule that might track evidence critical to a crime or terrorist act and the operator is out of luck. DPI cannot find what it is not instructed to look for. Because the criteria of a DPI hunt may change constantly, rules may require almost continuous updating — or new rules. In sum, DPI acts like a service.

Much confusion over the service nature of DPI arises from the fact that it can be configured in hardware as well as in software. See the word “box” and one thinks “fixed.” DPI is anything but. The predefined rules that make DPI work are in constant flux, just like those of a service.

In action, the recognition process moves from the simple to the complex quickly. Core rules might tell the DPI app the basics to look for in potential malware. A more sophisticated layer of rules will outline the patterns to be on the lookout for. A final set could be very specific, telling which identifiers to apply to a target’s traffic at precise points in the network.

Doing it all in real time is the trick. The use of DPI to scan and assess vast amounts of data in real time can quickly lead to scalability issues depending on the complexity and number of predefined patterns the DPI Engine is asked to search for. Scalability may not be so much of a problem for NSA facilities at Fort Meade, Maryland or Camp Williams, Utah, but it can be for routine use of DPI in many lawful intercept products.

A central component of all DPI apps is the ability to send notifications or alarms, depending on the priority determined by a set of predefined rules. In the commercial arena, the alert might pertain to a customer reaching the halfway mark on his or her mobile minutes. For government agencies, an alarm might be triggered when individuals with suspected criminal or terrorist affiliations set a meeting or give some indication of an imminent attack. Or, at the most basic level, the DPI app might simply produce a report or set of statistics.

As used in surveillance, DPI apps are “passive,” i.e., they perform recognition and notification — not manipulation which, for obvious reasons, would alert the target that he’s under scrutiny. Depending on the user’s computing bandwidth, surveillance DPI may be either in-line to capture targeted traffic in real time — a huge scalability issue given today’s data network volumes — or off-line, in which event, copies of network traffic are captured and stored. The chief benefit of an in-line set-up is that it is completely invisible to the target. The downside is that the processing power behind the DPI must be on par with the speed of the network, either through massive parallel processing, FPGAs, or both.

As a profiling tool, DPI is equally useful to government agencies, the military and law enforcement. And, by inputting predefined rules that look for patterns associated with “dark” activities, or the use of Tor or other encryption methods, virtually any DPI engine can be programmed to profile individuals, activities and threats. DPI systems designed for national police and other government agencies profile using DPI all the time.

DPI solutions are often integrated with other manufacturers' lawful intercept and intelligence platforms. Lawful intercept device manufacturers such as **Utimaco**, for example, use DPI products made by **Procera Networks** of California, USA. France's **Qosmos** ixEngine is widely used by communications service providers for traffic management, but also by Russia's **Protei** for lawful intercept and government intelligence – even though Qosmos contends that it expressly forbids the use of its ixEngine for ISS purposes.

IP Flow Monitoring

The concept of IP Flow Monitoring surfaced in 1996 with **Cisco's** commercial launch of the NetFlow protocol, roughly concurrent to when DPI emerged. Similarly to DPI, NetFlow was developed as a network management tool, in this case to help users of Cisco routers better understand traffic flows and support customer needs, or to signal the need for more scalable hardware able to meet rising bandwidth demands. Like DPI, NetFlow quickly gained competitors as other makers of IP routers introduced their own versions of the protocol for their devices. At the same time, NetFlow evolved as a surveillance tool. Because NetFlow is a generic term and not trademarked by Cisco, it has become interchangeable with "IP Flow Monitoring" in both the commercial and ISS arenas.

At one level, IP Flow Monitoring seems to act exactly like DPI. It collects data at a network device interface and exports data to an analysis engine. But the two approaches differ radically.

DPI can be configured to mirror, open and analyze selected packets or every packet that enters or exits a router interface. IP Flow Monitoring "samples" traffic and uses the IPFIX international standard to format data captured from routers and probes, then forwards the data to network management, mediation devices or other systems. To underscore the importance of IPFIX, vendors often include the term in descriptions of product capabilities, e.g., "NetFlow/IPFIX."

As network speeds race from 10GB to 40GB and 100GB, IP traffic sampling is an effective measurement of network activity at each node monitored. However, critics contend that IP Flow Monitoring falls short because sampling inevitably misses packets. While dropped packets may be of little interest to a network operator seeking a good general picture of network conditions, to LEAs and intelligence agencies the same prospect raises concerns that evidence might go missing. Advances in a sister technology have all but eradicated such concerns.

Hardware accelerators known as field-programmable gate arrays (FPGAs) today are often used in conjunction with both DPI and IP Flow Monitoring systems. FPGAs facilitate massive parallel processing with zero packet loss even in 100GB networks. Because FPGAs are "programmable," they can be configured differently to meet the objectives of changing network or surveillance scenarios, in contrast to ASICs-based hardware, which is "wired" at the factory to perform specific functions. With FPGA-enabled IP Flow Monitoring tools, the user can perform most of the same jobs typical of DPI: target and identify specific IP addresses, MAC addresses and other identifiers, as well as examine packet content.

Network Packet Brokers

Network Packet Brokers (NPBs) are packet filtering systems capable of monitoring IP traffic flows at line rate speeds, providing dynamic visibility into the network, both for commercial and surveillance purposes. NPBs have grown in popularity with the evolution of software defined networks, virtualized networks, the cloud, and the attendant rise in the volume, bandwidth and complexity of network traffic.

Traditionally, NPBs have been hardware-based, using either ASICS or FPGAs. Increasingly, however, vendors are looking to “virtual” of software-centric NPBs to provide the same functionality at lower cost. As usual, a battle of words has ensued between hardware and software vendors.

Software proponents contend that NPB hardware is too complex and expensive, meddles with the network, and is slower and harder to reconfigure than software. NPB hardware proponents fire back that its competitors’ virtual NPB products are less reliable. Over the horizon, some foresee network equipment that comes packaged with NPB capability, rendering both sets of NPB vendor irrelevant. Meantime, the two primary forms of NPB, virtual and hardware-based, co-exist in the marketplace and find buyers, depending on applications and budgets.

Any discussion of how NPBs operates begins with “SPANs” and “TAPs.” SPANs are Switched Port Analyzer ports, interfaces on network switching devices that copy and aggregate traffic, then send it on to monitoring devices or software for analysis. TAPs are more sophisticated mechanisms for monitoring two-way IP traffic on a pass-through basis.

SPAN ports, which emerged in the legacy network era, maintain a role in communications service provider networks today. They have good and “not so good” characteristics to consider. At the link level, SPAN ports may interface with copper, fiber or both types of line connectivity at various speeds. As a result, SPAN ports offer the advantage of low cost compared to more advanced alternatives. But they come with built-in issues.

One problem is that most network switching hardware is equipped with only one or two SPAN ports, meaning that multiple lines must compete for connectivity to access traffic for monitoring and analysis. Before long, port availability is overwhelmed and can lead to data loss during a network monitoring scenario. New types of traffic that consume more bandwidth, such as social media and video, may contribute to data loss.

Another issue: As network speeds advance, legacy monitoring tools designed for 1G networks must be replaced by tools for 10G, then for 40G and 100GB. With each installation of new monitoring tools, any savings generated by reliance on SPAN ports tends to diminish.

Finally, SPAN ports may encounter hurdles such as switches or routers that do not support port mirroring at all, or that slow traffic flows when port mirroring is introduced.

The next generation of data collection and aggregation came about with development of the TAP, a term sometimes deemed an acronym for “test access port,” though there is no firm proof to back up the argument. Originally designed as a portable test device, the TAP evolved into hardware for permanent deployment in the network, or in an enterprise database, to monitor traffic on a pass-through basis in “dual mode,” i.e., both directions simultaneously.

At present there are three types of TAPs: (1) basic TAPs where the number of ports on the TAP hardware is equivalent to the number of network ports; (2) aggregation TAPS that use one port to monitor multiple network ports; and (3) regeneration TAPs wherein a single TAP is used to mirror traffic from one part of the network, then passes the data along to multiple monitoring and analysis systems.

A TAP may be either in-line (active) or off-line (passive). When a TAP is deployed in active mode, network traffic flows through the device and may be modified or blocked. Passive TAPs, in contrast, simply mirror the traffic and send alerts to users when the device observes targeted communications. Note that a *network* TAP may be configured in either active or passive mode for data collection, but monitoring is strictly passive or off-line. In other words, any data missed in the collection stage cannot, for obvious reasons, be subjected to deeper analysis.

The arrival of Network Packet Brokers or NPBs represented, to many, a breakthrough. An NPB literally sits between a network switching device’s SPAN ports or routers to take charge of traffic flows. In addition to performing the essential monitoring function of filtering high bandwidth traffic flows, an NPB can do much more: filter, de-duplicate and time-stamp packets, and be coupled with Deep Packet Inspection (DPI) capabilities from Layers 2 – 7 of the OSI stack. In other words, an NPB can provide end-to-end inspection of targeted packets through the OSI Layer 7 application level – where much intelligence resides – together with the target’s IP address, MAC address and content.

The NPB can scale to monitor entire networks while at the same time drilling down to provide visibility and analysis of the link layer of IP traffic. It can see and identify any packet on the network, and provide full packet capture with accurate time and port stamping. With an assist from DPI, the NPB can also open and view full packet content.

Given its capabilities, speed, intelligence and redundancy, the NPB is perfect for network forensics when connected to probes, mediation devices and other intercept hardware. But again, NPBs don’t necessarily operate in isolation. NPBs are often found in combination with DPI capabilities. The same goes for NPBs and NetFlow. The Cisco Series 9000 router uses both Cisco “NetFlow IOS” IP Flow Monitoring and the “Cisco Network Data Broker,” an FPGA-based NPB for accelerating packet capture.

Table 3: Packet Monitoring

Company	Location	Solution	Function	Market	Of Note
Aglaya	New Delhi, India.	**Country Internet Interception.**	**Country Internet Interception:** DPI with 50-seat Command Center and multiple Controller Nodes installed outside the target region or country. Can be provided on a turnkey basis with training for users – or outsourced to Aglaya.	Govt. & Intel. agencies.	**Also see Aglaya in “Mobile Location” and “Malware.”**
ALBEDO Telecom	Barcelona, Spain	**NetHunter.** **NetShark.**	**NetHunter:** Hand-held device performs wire speed capture of any/all types of packets including VoIP, data, email, SMS, TCP/IP, IPTV and others in either Ipv4 or Ipv6. Filters can be set to capture specific or “all” IP traffic. Operates in port or pass-through mode. No MAC or IP address appears during surveillance – NetHunter is invisible to target. Available in either rack-mounted or portable hand-held battery-powered versions. **NetShark:** Same capabilities as NetHunter except operates in pass-through mode only, thus captures all packets and is ideal for higher-speed networks – 10G, 40G & 100G	LEAs, Govt. & Intel. agencies.	ALBEDO is renowned for focus on miniaturization– First hand-held device incorporating a touch-screen (1996), first portable wire speed tap with active filters, etc. Both NetHunter and NetShark use FPGA hardware accelerators for massive parallel processing. ALBEDO partners with WireShark to provide clients an add-on for data analytics.

ALBEDO Telecom (continued)			and capturing high-bandwidth apps including VoLTE & streaming video.		
Alcatel-Lucent	Paris, France.	**1357 ULIS (Unified Lawful Interception Suite).**	**1357 ULIS (Unified Lawful Interception Suite):** DPI for fixed, wireless & IP networks. Provides signaling and content intercept.	CSPs, LEAs.	Package includes automated court order management.
Amdocs	Chesterfield MO, USA. And Ra'ana, Israel.	**VoLTE Controller.**	**VoLTE Controller:** DPI identifies and filters targeted VoLTE traffic.	CSPs.	Acquired DPI company Bridgewater Systems (2011). Amdocs provides BSS/OSS systems to CSPs. Amdocs was investigated in 2000 for alleged involvement in Israeli "spy ring" operating in U.S. but FBI dropped case for lack of evidence. BSS systems are a core source of customer metadata.
Blue Coat	Sunnyvale, California, USA. Bad Homburg, Germany.	**ProxySG.**	**ProxySG:** DPI and packet filtering. Tunnels, intercepts and performs "man in the middle" (MITM) attacks that access SSL and transport layers, then mirrors IP comms between sender and recipient.	LEAs, Govt. & Intel. agencies, Military.	Partners with Cisco, VSS Monitoring. Effective June 13, 2016, Blue Coat is owned by Symantec. Use of Blue Coat DPI products for

Blue Coat (continued)		**PacketShaper.** **SSL Visibility Appliance.** **WebPulse.**	**Packet Shaper:** DPI integrated with WebPulse, real time Web intelligence. **SSL Visibility Appliance:** Performs MITM attacks to compromise and replicate encrypted SSL and HTPPS (HTTP over SSL) certificates. **WebPulse:** Web intelligence package tailored to Blue Coat DPI devices.		ISS is documented in over 25 nations.
Cisco Systems	San Jose, CA, USA.	**Cisco Series 7600. Router with TAP2-MIB, TAP2-MIB Processing.** **Cisco Series 12000 Router.** **Cisco ASR 1000. SCE8000.** **Cisco SCE8000.** **Cisco Meraki.** **Cisco Series ASR 9000 Router.**	**Series 7600:** NetFlow IP Flow Monitoring. Ipv4, IEEE 802 data streams & individual sessions. **Series 12000:** VoiP and dial-up calls. **ASR 1000:** midrange router – Ipv4 & Ipv6. **SCE8000:** DPI Control Engine for application and session-based classification. **Meraki:** Cloud networking DPI. **ASR Series 9000:** Monitors Ipv4 and Ipv6 traffic. Built-in hardware sensors for rich traffic flow telemetry and line-rate data collection. Uses Cisco Nexus Data Broker support for network traffic monitoring and analysis	CSPs, Govt. & Intel. agencies.	Cisco is migrating to the Series 9000 and other newer series. All Cisco routers can be programmed to intercept, mirror and process targeted traffic, including signaling, type of message and full content. Cisco SCE 8000 & Meraki DPI are used in the “Great Firewall of China.” Compare Cisco NetFlow to Flowmon and Juniper Networks Flow-Tap.

ClearTrail Technologies	Indore, India.	**ComTrail Inline.**	**ComTrail Inline:** Monitors, intercepts & decrypts targeted https traffic in real time, including webmail, social media & chat. Blocks content.		**Also see ClearTrail in “Lawful Intercept Solutions,” “Mobile Location,” “Malware” and “Advanced Analytics.”**
ComWorth	Ota, Japan.	**SwiftWing SIRIUS.**	**SwiftWing SIRIUS:** Line rate DPI packet capture for support of streaming analytics.		ComWorth is a pure play DPI vendor. Analytics provided by partners.
DATAKOM GmbH	Ismaning [Munich], Germany.	**Poseidon.**	**Poseidon:** DPI at Layers 2 – 7 of the OSI stack.	CSPs, LEAs.	Through purchase of GTEN (2016). Note:Munich-based Elaman also sells DPI trademarked “Poseidon.”
Decision Group	Taipei, Taiwan.	**E-Detective.** **Wireless Detective.** **VoIP Detective.** **Cloud app.**	**E-Detective:** LAN/Internet tool to intercept and decode packets; reconstructs & saves packets in original format so user can see how data appeared on the network. Decodes POP3, HTTP, videos, Twitter, Facebook. Captures login info of target. Same functionality for wireless, VoIP and cloud intercept and monitoring solutions.	CSPs, LEAs, Govt. & Intel. agencies.	Distributers & resellers: Axxera (Santa Ana, CA, USA), Daitek Technology (Buenos Aires), Merz-Decision Computer (Lienen, Germany), Anxinwei (Guangdong, China), Prodata Consult (Copenhagen, Denmark). **Also see Decisions Group in “OSINT & Social Media Monitoring”**

DESOMA	Rosenheim, Germany.	**DAISY.**	**DAISY:** “virtual” real time DPI. Copies all packets and hashtags each to avoid duplication. Metadata and “useful” content stored separately for efficient storage, access, analysis. Discards irrelevant data to accelerate speed.	LEAs, Govt. & Intel. agencies.	Founded in 2010. Key strategic partner of Gamma/Fin-Fisher beginning 2011.
DigiTask	Hesse, Germany.	**DigiNet.**	**DigiNet:** DPI at OSI Layers 2 – 7. Compromises SSL certificates and for man-in-the-middle attacks.	LEAs.	**Also see DigiTask in “Mobile Location” and “Malware.”**
Elaman	Munich, Germany. Amriswil, Switzerland.	**CS-2000 High End**. **Poseidon Internet Monitoring Center.** **Poseidon Mobil.** **Munin POTS.**	**CS-2000 High End:** DPI probe. **Poseidon Internet Monitoring Center:** centralized management of DPI probes. **Poseidon Mobil:** portable DPI. **Munin POTS:** DPI for monitoring, blocking and shaping.	CSPs, LEAs, Govt. & Intel. agencies	**Also see Elaman in “Malware.”**
Emulex	Costa Mesa, CA, USA (HQ). Bangalore, India. Dublin, Ireland. Paris, France. Wokingham UK.	**Endace Probe 304.** **EndaceProbe 3000.** **EndaceProbe 4004.** **EndaceProbe 4104.** **EndaceProbe 7000.** **EndaceProbe 8004.** **EndaceVision and Data Mining.**	**From Endace acquisition:** Suite of six “Intelligent Network Recorders” (INRs) for DPI. From entry-level 500 Mbps **EndaceProbe304** to multi-GB Ethernet **EndaceProbe 8004** unit. **EndaceVision and Data Mining:** provides aggregate view and visualization of data.	CSPs, LEAs.	Acquired Endace (New Zealand) Oct 2013.

Expert Team	Singapore.	**3i-Web.** **3i-Tactical System.**	**3i-Web:** Classic DPI uses in-house developed rules-based engine, IRGO (Intelligent Reconstruction Gear OS). **3i-Tactical System:** Lightweight laptop version of 3i-Web, but with addition of Deep Web OSINT capabilities. Built for field ops. Available in models with input ranging from 1 GB to 160 GBs	LEAs, Govt. Intel. agencies.	
Fiberblaze	Soborg, Denmark.	**Fiberblaze DPI.**	**Fiberblaze DPI:** DPI and analysis via series of field-programmable gate array (FPGA)-based data capture interfaces.	CSPs, LEAs, Govt. & Intel. agencies.	
Flowmon Networks	Brno, Czech Republic.	**Flowmon Probe.** **Flowmon Collector.** **Flowmon Traffic Recorder.**	**Flowmon Probe:** 100GB wire speed processing via network probe with built-in Flowmon/IPFIX. Captures and analyzes traffic through Layer 7. **Flowmon Collector:** Uses NetFlow v5/v9 to collect, visualize, analyze and store of network statistics on network traffic on routers, switches, firewalls. **Flowmon Traffic Recorder:** A plug-in for Flowmon Collector, to record intercepts by IP and MAC address, port number or other criteria.	LEAs, Govt. & Intel. agencies.	One of two companies split off from IP Flow Monitoring pioneer, Invea-Tech in (Sept. 2015_. Like its predecessor Invea-Tech, Flowmon OEMs voice biometrics from Phonexia. Compare to Cisco Netflow and Juniper Networks Flow-Tap.

Gigamon	Santa Clara, CA, USA.	**Gigamon G-TAP.** **Gigamon GigaVUE.** **Gigamon GigaVUE VoIP Recorder.**	**Gigamon G-TAP:** high-density passive TAP for 40GB/100GB fiber optical networks. **Gigamon GigaVUE:** Mid-density Traffic Visibility Node for 10Gb networks **Gigamon GigaVUE VoIP Recorder:** Recording and data retention.	CSPs, LEAs, Govt. & Intel. agencies.	
Huawei	Shenzhen, China.	**SIG 9810.** **SIG 9820.**	**SIG 9800 Series:** Identifies targets on wireline, mobile and W-FI networks, in multiple languages. Collects traffic including P2P, VoIP, IM, video and Web search, as well as 850 protocols and 1,000 apps. Configurable to watch for 65 million urls in 40+ categories.	Govt. & Intel. agencies.	Used in the “Great Firewall of China.”
Incognito	Vancouver, BC Canada.	**Broadband Command Center.**	**Broadband Command Center:** DPI provisions and collects subscriber IP records and generates reports for law enforcement. Monitors any device or IP address.	LEAs.	
Ipoque (Rohde & Schwarz Company)	Leipzig, Germany.	**DPX Probe with PACE and PADE.**	**DPX Probe PACE:** DPI engine classifies Layer 7 protocols and applications. **PADE:** Extracts & decodes encrypted data.	LEAs, Govt. & Intel. agencies, Military.	Acquired by Rohde & Schwarz (2011).

Ixea	Calabasas, CA, USA.	**Net Optics Flex Tap.** **Net Optics Gig Zero Delay Tap.** **Net Optics Slim Tap.** **Net Optics HD8 Tap.**	**Net Optics Flex Tap:** passive high density fiber tap via Network packet broker. **Net Optics Gig Zero Delay Tap:** 10/100/1000GB tap. **Net Optics Slim Tap:** passive fiber tap. **Net Optics HD8 Tap:** total traffic visibility in 1GB tap.	CSPs, LEAs, Govt. & Intel. agencies.	Acquired Net Optics (2013).
Juniper Networks	Sunnyvale, CA, USA.	**Flow Tap.** **Junos Packet Vision.**	**Flowtap:** IP Flow Monitoring dynamically captures sample packets in high-speed networks. **Junos Packet Vision:** DPI.	CSPs, Govt. & Intel. agencies.	Flow-Tap is supported on Juniper Networks M Series and T Series routers, except for M160 and TX Matrix routers.
Mantaro	Germantown MD, USA.	**Session-Vista EX-20 Exporter.** **Mantaro Network Intelligence Solutions.**	**Session-Vista EX-20 Exporter:** DPI for Level 4 thru Level 7. IP traffic interception at multi-GB speeds at session level. **Mantaro Network Intelligence Solutions:** FPGA-based packet filtering. Visualizes network activities of specific hosts for suspicious activity. Examines OSI Levels 1 – 7. Searches by IP address, user name or portion of user name from social media, email, peer-2-peer and file servers.	CSPs, LEAs, Govt. & Intel. agencies.	Mantaro specializes in extensible FPGA framework solutions compatible with FPGAs made by Xilinx, Altera – and Mantaro.

Neti	Budapest, Hungary.	**BONGO.** **Compact BONGO**.	**BONGO:** DPI. Integrated monitoring for national networks. Filters and decodes traffic from IP, PSTN & mobile networks. **Compact BONGO:** Workstation version of BONGO for tactical DPI.	LEAs, Govt. & Intel. Agencies.	Owned by a non-profit organization that reports to the office of Hungary's Prime Minister.
NetQuest	Mount Laurel, NJ, USA.	**Web Opticop Interceptor.**	**Web Opticop Interceptor:** DPI device selects and filters traffic from SONET/SDH/ PDH networks. Single stage (selected frames) and Multi-stage (packet targeting by protocol type).	CSPs, LEAs, Govt. & Intel agencies.	
Netronome	Pittsburgh, PA, USA.	**NFP-3420** hardware and **Netronome Flow Manager** software	**NFP-3420** and **Netronome Flow Manager**: Deep Content Inspection, behavioral heuristics, forensics and network intrusion prevention. Filters out 90 percent of irrelevant traffic.	CSPs, LEAs.	NFP -3420 is used by SS8.
NETSCOUT SYSTEMS	Westford, MA, USA.	**NGENIUSONE.** **Intelligent Data Sources.** **nGENIUS Taps.**	**NGENIUSONE:** DPI traffic analysis of VoLTE, IMS, WiFi, circuit-switched 2G/3G, broadband Internet, messaging & OTT services. **Intelligent Data Sources:** Analyzes OSI Layer 7 protocols and applications. **nGENIUS Taps:** Enables DPI taps by multiple groups from any point in network.	CSPs, LEAs, Govt. & Intel. agencies.	Partners with Alcatel-Lucent, Avaya, Cisco, EMC (for packet data flow monitoring). Acquired FOX-IT Replay and Simena PacketFlow Switch (2011). Acquired ONPATH Technologies UCS

NETSCOUT SYSTEMS (continued)		**nGENIUS Packet Flow Switch.** **InfiniStreamNG Platform.** **Sniffer Analysis.** **nGENIUS Infinistream Appliance.**	**nGENIUS Packet Flow Switch:** Aggregator for wire speed DPI. For up to 24 ports of 1GB or 10GB Ethernet. **InfiniStreamNG Platform:** Portfolio of six physical and 2 virtual solutions for real time streaming analysis of 10GB, 40GB and 100B packet networks. **Sniffer Analysis:** Granular packet-level analysis, mining and decoding of packets. **nGENIUS Infinistream Appliance:** All-in-one Packet Flow switch for intercept and analysis.		3900 – Universal Connectivity System with HorizON Software: Unified real time intercepttion and manage ment of international TDM, IP & mobile traffic (2013). Acquired **VSS Monitoring** (2015).
Nexa Technologies	Paris, France and Dubai, UAE.	**EAGLE SMINT.** **EAGLE GLINT.**	**EAGLE SMINT:** portable DPI. **EAGLE GLINT:** Real time DPI for intercept of wireline, mobile, and microwave.	Govt. & Intel. agencies, Military.	Nexa is a group member of Germany's **PLATH GmBH**. Formerly **Amesys** with "Eagle System," the company was spun off from Bull Amesys following Arab Spring. PLATH acquired then reopened Amesys as Nexa, in Paris. In Dubai, Nexa is "Amesys."

NORSI-TRANS	Moscow, Russia.	**Vitok-Defragmentator.**	**Vitok-Defragmentator:** Removes IP-fragmentation or tunneling from Internet traffic before its analysis. For IP, VLAN, MPLS, 3G and LTE networks.	LEAs, Govt. & Intel. agencies.	**Also see NORSI-TRANS in "Lawful Intercept Solutions," "Mobile Location," Advanced Analytics," and "OSINT and Social Media."**
		Vitok-CDR.	**Vitok-CDR:** Decodes, edits, renames, deletes and/or censors call detail record files including FTP and SFTP. Performs multi-level search of files to infiltrate, stream read and record for processing. Creates database to prevent re-processing of files or introduction of errors.		
		Compact L7 Network Traffic Analyzer.	**Compact L7 Network Traffic Analyzer:** Portable standalone DPI device for 10GB Ethernet networks. Provides OSI Layer 2 – 7 decoding. Extracts metrics of user session data including target's content and affiliations with co-conspirators. Collects and stores statistics. Analyzes "tunneled" traffic. Applicable to VLAN, IGRP, MPLS, GPRS, CDMA, WiMAX, 4G and LTE networks.		

NORSI-TRANS (continued)		**Vitok-TEXT.**	**Vitok-TEXT:** Collects unstructured text data for retention, search and analysis. Extracts file in any MS Office or Open Office format, as well as txt, rtf, pdf, html, mht, xml, eml and wpd. Works in all Slavic & European languages as well as scrip languages including Hebrew, Arabic, Persian and others. Query elements may be words or objects. Filters may be set to query for time range, headings, subjects and type of document.		
Packet Forensics	Tempe, AZ, USA.	**LI-5-LEO.**	**LI-5-LEO:** DPI "man in the middle" attacks at SSL and transport layers via replication of secure certificates; capable of packet modification, inject & replay functions.	LEAs, Govt. & Intel. agencies.	$500K NSA contract documented (Sept. 2012). **Also see Packet Forensics in "Lawful Intercept Solutions."**
Procera Networks	Fremont, CA, USA.	**PacketLogic Platform.**	**PacketLogic Platform:** NetFlow software platform truns on off-the-shelf hardware. Flow inspection and advanced application classification including pattern matching, conversation semantics, protocol analysis, behavioral and statistical analysis, flow association and "future flow" possibilities.	LEAs, Govt. & Intel agencies, plus ISS vendors.	Germany's Utimaco uses Procera DPI products.

Procera Networks (continued)		**PacketLogic Perspective.**	**PacketLogic Perspective: I**ntelligence libraries that provide context to network traffic.		
Protei	St. Petersburg, Russia.	**Protei DPI 8.** **Protei DPI 20.** **Protei DPI 80.**	**Protei DPI 8**: 8 GB throughput with 100,000 flows per second. **Protei DPI 20:** 20 GB throughput with 250,000 flows per second. **Protei DPI 80:** 80 GB throughput with 1,000,000 flows per second.	CSPs, LEAs, Govt. & Intel**.** agencies primarily in Russia and CIS states.	Uses Qosmos ixEngine for DPI. Partners with Silat Solutions of Jordan for sales in Africa and the Middle East**.** All devices perform Layer OSI 2 – 7 analysis, and can identify up to 2,000 protocols. **Also see Protei in “Mobile Location”**
Qosmos	Paris, France.	**ixEngine.** **ixMachine Probe.**	**ixEngine:** DPI software parses communication flows and links them to a suspect’s virtual online identities. **iXMachine Probe:** DPI hardware/software	CSPs, Govt. & Intel. agencies, other surveillance vendors.	Licenses ixEngine to Russia’s **Protei** but denies its use in surveillance.
Radisys	Hillsboro, OR, USA	**Radisys TDE (Traffic Distribution Engine).** **Radisys FlowEngine.**	**Radisys TDE:** Hardware platform interfaces with 10G/40G/100G networks. **Radisys FlowEngine:** Software that runs on Radisys TDE. Integrates with industry-leading DPI software to deliver wire speed packet capture.	CSPs, LEAs.	Powers end-to-end radio access network used by Polaris Wireless Omnilocate mobile location solution.

Riverbed	San Francisco, CA, USA.	**Wireshark.** **SteelCentral Aternity.**	**Wireshark:** Free open-source DPI supports over 1,000 protocols – often used as platform for ISS-focused DPI. ID's app traffic by IP addresses, ports, protocols or urls. **SteelCentral Aternity:** Monitors every app on any physical, virtual or mobile end user device.	CSPs, LEAs.	
Rohde & Schwarz	Munich, Germany.	**CMW-KM051.**	**CMW-KM051:** Uses ipoque PACE DPI engine to capture each packet, see IP connections, protocols, data volume, and user names via RADIUS server.		See more on Rohde & Schwarz under ipoque.
Savvius (formerly WildPackets)	Walnut Creek, CA, USA.	**Omnipliance CX.** **Omnipliance MX.**	**Omnipliance CX:** Affordable IP Flow Monitoring with network forensics and analysis for 1GB and 10GB networks. Uses Savvius OmniPeek software for packet analysis. Provides up to 16 terabytes of storage. **Omnipliance MX:** Same Omnipliance hardware can accommodate up to four 1GB or 10GB cards to support higher bandwidth networks. Uses OmniPeek for packet analysis. Storage of 32 terabytes.		Savvius uses hardware accelerators from **Napatech** and DPI by **Procera** to operate at wire speed. **Also see Savvius in "Lawful Intercept Solutions" and "Packet Monitoring"**

Savvius (continued)		**Omnipliance TL.**	**Omnipliance TL:** Packet flow monitoring for 10GB or 40GB networks. Includes OmniPeek analytics software. Real time packet capture plus heuristic traffic analysis. Instant data search & retrieval. Accommodates an additional four 10GB cards. 128 terabytes storage.		
Semptian	Shenzhen, China.	**FS3200.** **FS9000.** **FT5000.** **MC Box II.**	Dedicated DPI hardware for lawful intercept, intelligence, traffic blocking.	Govt. & Intel. agencies.	Used in the "Great Firewall of China."
SS8	Milpitas, CA, USA.	**Protocol Extraction Engine.**	**Protocol Extraction Engine:** FPGA-optimized DPI.	CSPs, ISPs, LEAs.	**Also see SS8 in "Lawful Intercept Solutions," "Malware" and "Advanced Analytics."**
Telesoft Technologies	Dorset, UK (HQ). Atlanta, GA, USA. Uttar Pradesh, India	**ThinkEngine Probe.** **Data Retention Probe.**	**ThinkEngine Probe:** FGPA-assisted DPI extracts, decodes and collects data and content. Captures user ID, timestamp and duration, location. Includes analytics. **Data Retention Probe:** New as of Aug 2016 – Probe parses data from carrier NAT iPv4 IP addresses to single out individual target IP addresses – on wireline, IP and mobile networks.	CSPs, LEAs, Govt. & Intel. agencies.	**Also see Telesoft in "Mobile Location."**

Thales	Neuilly-sur-Seine, France.	**Net Spyder.** **IPTr@pper.**	**Net Spyder:** DPI for fixed and mobile IP. Decodes web pages, e-mails, web-mail, chat, webcam use, file transfer, VoIP. **IPTr@pper:** DPI tactical hardware that connects to ISP, router or LAN to access data, VoIP, video.	LEAs, Govt. and Intel. agencies.	**Also see Thales under “Lawful Intercept Solutions” and “Military.”**
Ultra Electronics	Middlesex, UK.	**PacketAssure iQ1000.** **ARIES.**	**PacketAssure iQ1000:** Layer 2 switching hardware platform for voice, video and data service delivery. Diverse array of service classifiers and policies quickly create APIs for any monitoring applications in lawful intercept and military surveillance. **ARIES:** DPI software run on the PacketAssure 1Q1000 or other hardware. Can handle mass or targeted surveillance, capturing IP and MAC address, keywords, events, known figures, transactions, metadata and content, including audio and video.	CSPs, LEAs, Military.	**Also see Ultra Electronics in “Advanced Analytics,” “Biometric ID” and “Military.”**
VSS Monitoring	Sunnyvale, CA, USA. Beijing, China. Singapore.	**vBroker.**	**vBroker:** Network packet broker for active and passive IP network monitoring. Filters high bandwidth traffic flows on IP networks. De-duplicates and time-stamps	CSPs, LEAs, other LI vendors.	Acquired by **Danaher Corp**. (2012). Spun off to **NetScout** (2015). VSS Monitoring operates as a semiauto-

VSS Monitoring (continued)		**Distributed TAPS.** **Network TAPS.**	packets. Provides Layer 2 – 7 DPI including targets' IP address, MAC address and apps. **Distributed TAPS:** entry level packet filters. **Network TAPS:** Provides two-way flow-through monitoring of router traffic.		nomous unit. Partners with Alcatel-Lucent, Blue Coat (Symantec), Fastech, IBM, Narus, Netronome, Nokia Siemens and Qosmos.
Yaana Technologies	Milpitas, CA, USA.	**DeepProbe Packet Inspection Appliance.** **Data Analytics System.**	**DeepProbe Packet Inspection Appliance:** Dedicated DPI device. **Data Analytics System:** DPI with real time analytics.	CSPs, Enterprise Customers, Govt. & Intel. agencies.	Yaana's DPI products result from acquisition of IP Fabrics from ATIS UHER (June 2015). **Also see Yaana in "Lawful Intercept Providers" & "Malware."**

Chapter 4: Mobile Location

Mobile location solutions enable the user to determine the target’s precise or approximate physical whereabouts, either in real time or historically. The solutions include:

- A “beeper” attached to a suspect’s vehicle.
- Continuous signaling (“pinging”) of the suspect’s cell phone.
- Use of Signaling System 7 (SS7) on 2G/3G networks to find the cell tower nearest to the target in real time often used under authority of a FISC order to track foreign intelligence operatives offshore.
- Use of Session Initiation Protocol (SIP) on VoIP networks.
- Special interfaces for the Diameter protocol that support location-based services as network operators evolved to IP networks supporting LTE.
- IMSI catchers that emulate a mobile base station and determine target device location, plus perform a man-in-the-middle attack on device encryption to intercept communications content.
- RF pattern matching that calculates target device location based on the unique radio “signature” of each point in a cell network.

Two other commonly used mobile location data methods:

- A non-tracking mobile location service under CALEA. Not real time. Data is confined to the target’s proximity to the nearest cell tower.
- Use of a target’s mobile location records, stored by his or her service provider, to associate the use/day/time/whereabouts of the target’s mobile device with the geophysical location of a criminal/terrorist event. Similar to CALEA mobile location data.

Beepers and Continuous Pinging

“Beepers” are radio signaling devices attached to the target’s vehicle to transmit his location continuously.

“Continuous Pinging” leverages the built-in location-based tracking capabilities of cellular networks (e.g., used in 911 services) to signal the target’s device and track its physical whereabouts. Continuous pinging is conducted either via court-ordered cooperation with the target’s mobile service provider, or may be implemented directly by the LEA to save time in “exigent” (emergency) circumstances.

Signaling System 7

Signaling System 7 (SS7), a technology introduced in 1980 by the International Telecommunications Union (ITU), came about to provide a more efficient means of managing point-to-point voice calls – using a separate data signal with all call routing information embedded that sped ahead to alert the network on the specific handling required for a call. Because wireline, wireless and data messages are still routed from their point of origin to their destination via SS7, and all 2G/3G mobile service providers internationally use SS7, it provides a convenient mechanism to track a target's location on those networks, whether in the U.S., or for calls made between the U.S. and another country. Agents can discretely send single or multiple tracking queries to mobile operators through the SS7 network and obtain a target's location with "cell accuracy."

The upside of SS7 for mobile location is that the SS7 network is global. The downside: "cell accuracy" merely determines location in a given mobile network cell, thus its accuracy may be greater in an urban mobile network cell with multiple base stations that are smaller and closer together than in suburban, rural or remote areas with larger cells that cover more territory. Also, the SS7 protocol stack applies strictly to GSM and UMTS networks. LTE, which uses the more modern Diameter protocol on top of TCP/SCTP/IP stacks for signaling.

Mobile Location on LTE Networks

Tracking of LTE device position via network-enabled methods hinges on the type of location-based service selected by the mobile operator. Commonly applied methods include:

- **Cell ID (CID)**: This is LTE Diameter's version of SS7 mobile location. Cell ID is accurate only within range of the nearest Evolved Node B (eNB or mini-base station) to the target's LTE device. It's not accurate but it's cheap compared to other methods, hence its popularity among operators.

- **Enhanced Cell ID (ECID)**: Uses added radio measurements to fine tune CID, but again as with SS7, the accuracy of mobile location is confined to the distance between the target's device and the nearest network base station.

- **Observed Time Difference of Arrival (OTDOA)**: OTDOA measures timing of downlink signals received from three or more eNBs to pinpoint the target via triangulation.

- **Assisted Global Positioning System (AGPA)**: For GPS-enabled LTE devices, AGPS is the most accurate form of LTE network-enabled mobile location. AGPS enhances the accuracy of an LTE's embedded GPS receiver with supplemental SATCOM data on reference position and time. Caveats: AGPS tends to break down when tracking targets indoors or in high-rise buildings. If the operator adds ECID and OTDOA, mobile tracking inside or in densely populated cities may improve.

- **Uplink time difference-of-arrival (U-TDOA)**: The best that carriers have to offer in network-enabled mobile location. U-TDOA determines location based on the time it takes for an uplink signal from an LTE device to reach special receivers in a base station. U-TDOA takes advantage of multilateration, the difference in the distance to two stations at known locations by broadcast signals at known times using multiple measurements.

What if the agent wants more?

IMSI Catchers

IMSI (international mobile subscriber identity) catchers are highly effective, but controversial in that their use does not require cooperation by a mobile operator. IMSI catchers work in two modes: “active,” to locate targets on the network and capture communications and content; and passive, to map all mobile devices in a given mobile network cell or area.

In active mode, the IMSI catcher locates the target device by triangulating the device’s signal links to other mobile base stations. It then emits a stronger signal than the adjacent mobile base station in order to lure the target’s device. Because mobile devices always hunt for the strongest base station signal, they are easy targets for an IMSI catcher and invariably log in.

Once a target’s device authenticates with the “fake base station,” the IMSI catcher launches its MITM attack, decrypts the device and intercepts calls, messages or any content on the device. GSM phones are typically outfitted with A.5/1 A.5/2 encryption, and all IMSI catchers come ready to decrypt A.5/1 A.5/2 in real time. In the case of an LTE network, the IMSI catcher can use circuit-switched fallback, a technique that signals the device that it is on a GSM network and must revert to 2G.

In passive mode, the IMSI catcher does not interfere with the network by inserting itself and acting like a legitimate base station. Instead, it tunes into a base station to receive uplink signals from mobile devices and downlink signals from the base station. The uplink signal is the information being sent by the mobile device, while the downlink consists of replies from the base station. Passive mode also lets the IMSI catcher see all mobile devices connecting to a network base station.

Another technique involves radio signature technology, which is growing in popularity as an effective, often lower-cost mobile location alternative. RF signature mobile location matches the location patterns of the target to the unique location signature of a point in the network.

As networks evolve to 5G, mobile location will present new challenges such as “radio localization,” the use of many small cell sites outfitted with small antennas to efficiently and economically handle massive bandwidth via multiple paths. Radio localization’s reliance on multipath propagation undermines radio direction finding. The investigator may see multiple signals arriving from a variety of different paths, making it virtually impossible to track an RF signal by its direction of arrival.

In Germany, **MEDAV** and **Rohde & Schwarz** have made significant gains in developing “5G Mobile Location” that pinpoints the location of subscribers or even of “throwaway” phones on tomorrow’s networks. **Keysight** is another contender in this space.

Table 4. Mobile Location

Company	Location	Solution	Function	Market	Of Note
Ability	Tel Aviv, Israel.	**3G-CAT.** **IBIS-II.** **IRIS.** **TAIS.** **SLIS.** **Unlimited Interception System (ULIN).**	**3G-CAT:** Portable IMSI catcher; forces the target's 3G phone into 2G mode, opening it to active interception. **IBIS-II:** available only to LEAs, permits GSM off- air interception & monitoring. **IRIS:** for Iridium SATCOM. **TAIS:** Thuraya **SLIS:** Satellite Link Interception. **ULIN**:Intercepts calls,SMS and metadata from GMS/UMTS/LTE phones – for any number of targets. Exploits weakness in SS7 to determine location of targets without assistance from service providers. Operation requires IMSI numbers of targets.	CSPs, LEAs, Govt. & Intel. agencies, Military.	Ability launched ULIN in November 2015. ULIN price reportedly scales up to US $20M per license depending on number of targets. Ability merged with Cambridge Capital in December 2015. Israel's **NSO Group** reportedly uses Ability-made Zero Days to plant malware on mobile devices. Investor note: Rosen law firm filed class action suit against Ability on May 25, 2016 for falsification of financial reporting from 2012-2015. Ability shares on NASDAQ plummeted from USD 7.41 to 2.66. **Also see Ability in "Malware."**
Aculab	Milton Keynes, UK + offices in Germany & USA.	**SS7 Signaling Monitor.**	**SS7 Signaling Monitor:** SS7 tracking is used to pinpoint targets in relation to nearest cell tower.	LEAs.	**Also see Aculab in "Lawful Intercept Solutions."**
Aglaya	New Delhi, India.	**WiFi Interceptor.**	**WiFi Interceptor:** Automatically connects with any open WiFi network, captures encrypted handshakes and takes control of a target's device without being detected. Can also do selected or blanket jamming of WiFi networks. Remote operation up to 5 miles from target.	LEAs, Govt. & Intel. agencies.	**Also see Aglaya in "Packet Monitoring" and "Malware."**

AQSAQOM	Paris, France. Melbourne, Australia. Washington, DC USA.	**AQSAQOM Geolocation Enhanced Solution (AGES).**	**AQSAQOM Geolocation Enhanced Solution (AGES):** Active & passive geolocation of 2G/3G and LTE devices. Active via SS7 or Assisted GPS tracking with operator cooperation. Passive via tracking of interaction between network servers and target's handset to obtain target's location by IP address – without service provider. AGES can be integrated with AQSAQOM's ALIS lawful intercept solution.	LEAs, Govt. & Intel. agencies.	**Also see AQSAQOM in "Lawful Intercept Solutions."**
ATIS UHER	Bad Homburg, Germany.	**Klarios GIS.**	**Klarios GIS:** Location tracking of mobile devices and PCs. Uses relation analysis based on stored mobile metadata for GIS mapping.	CSPs, Govt agencies, LEAs, Military.	**Also see ATIS UHER in "Lawful Intercept Solutions," "Advanced Analytics" and "Military."**
BEA	Torino, Italy.	**ENEA.** **ENEA REC.** **ENEA MANAGER.** **Quad Finder LL/V.** **Polo GPS.** **Thoro.** **Thoro Manager.** **Jamm Bag.** **Gate Lawful Intercept.**	**ENEA products:** Passive "off the air" GSM monitoring and location. **Quad Finder LL/V:** GSM Mobile location. **Polo GPS:** GPS tracking. **Thoro products**: WiFi interception & analysis. **Jamm Bag:** Jams GSM, WiFi and Bluetooth signals. **Gate Lawful Intercept:** Data retention system stores data from mobile intercepts for retrieval & analysis.	LEAs, Govt. & Intel. agencies.	

Boeing	Germantown, MD, USA	**DRT 1101B.** **DRT 1183B.** **DRT 1201C.** **DRT 1301C.** **DRT 1301C+** **DRT 4411B.**	**DRT 1101B:** Dual mode RF monitor. In active mode provides IMSI catcher capabilities over a wider range than Harris Stingray.In passive mode monitors all mobile devices in range of receiver. Uses automated channel monitoring to capture signals of interest. **DRT 1183B**: Uses field programmable gate arrays (FPGAs) for more throughput in processing wideband and narrowband signals. Automated channel monitoring. **DRT 1201C**: Software configurable for use with any mobile network. Monitors up to 544 channels. Automated monitoring. FPGAs for high throughput. **DRT 1301C**: Manpack version for field use. Lightweight. Monitors 16 full-duplex and 32 half-duplex channels. **DRT 1301C+**: More robust & lighter manpack version. Monitors up to 72 channels. Uses GPS receiver for precise location. **DRT 4411B**: Top-of-the line “DRT Box.” Lightweight & miniature. Simultaneously captures traffic from GSM, CDMA, EV-DO, UMTS, TD-	LEAs, Govt. & Intel agencies.	Made by Digital Receiver Technology (DRT, hence origin of popularized name, “DRT Box”). DRT is a Boeing subsidiary, acquired in 2008. The DRT 4411B is popular in fixed wing aerial mobile location,

Boeing (continued)			SCDMA, LTE-FDD and LTE-TDD networks. FPGAs for speed. 50-channel GPS for precise location. Comes with removable storage or can stream data to other devices for analysis.		
Cambridge Consultants	Cambridge, UK & Cambridge, MA, USA.	**Sidewinder.**	**Sidewinder**: Pocket size Femtocell Base Station acts as an IMSI catcher – "fake" base station. Compact, low-cost portable mobile device captures IMSIs and provides mobile location.	LEAs, Govt. & Intel. agencies.	
ClearTrail Technologies	Indore, India.	**QuickTrail.** **mTrail.**	**QuickTrail:** tactical WiFi monitoring. **mTrail**: tactical off the air mobile monitoring.	LEAs	**Also see ClearTrail in "Lawful Intercept Solutions," "Malware" "Packet Monitoring" and "Advanced Analytics."**
CRYPTON-M	Kiev, Ukraine.	**AquaGSM.** **TerraLine Global.** **TerraLine Portable.**	**AquaGSM:** Passive GSM interception system for through-the-the-air recording and decryption of voice and SMS. **TerraLine Global:** Intercepts all trunked communications including mobile. Also identifies the target by IMSI number and location. Includes database for storage and analysis. **TerraLine Portable:** Same as Terraline Global but scaled down to handle eight digital duplex trunk lines of mobile or fixed wireline networks.	LEAs, Govt. & Intel. agencies.	**Also see CRYPTON-M in "Lawful Intercept Solutions" and "Military."**

DigiTask	Hesse, Germany.	**WiFi Catcher.**	**WiFi Catcher:** WiFi interception.	LEAs.	**Also see DigiTask in “Malware” and “Packet Monitoring.”**
ELTA Systems	Ben Gurion Intl Airport, Israel.	**EL/K-7077OE.**	**EL/K-7077OE:** Compact passive off-the-air GSM interception with direction finding and geolocation. Covers multiple GSM bands including U.S. and European. Deciphers A/5.2 in real time and A/5.1 in near real time. Can be operated remotely from a central command center.	LEAs, Govt. & Intel. agencies.	**Also see ELTA Systems in “Military.”**
Group 2000	Almelo, Netherlands. Oslo, Norway. Freienbach, Switzerland. Wilmington, DE, USA.	**LIMA Cell Monitor.**	**LIMA Cell Monitor:** GPS measurement from a mobile or fixed position of targets on 2G, 3G, GSM and LTE networks.	LEAs, Govt. & Intel. agencies.	**Also see Group 2000 in “Lawful Intercept Solutions,” “Biometric Identification,” and “OSINT and Social Media.”**
Harris Corporation	Melbourne, FL, USA.	**StingRay II.** **Gossamer.** **Triggerfish.** **Kingfish.** **Amberjack.**	**StingRay II:** IMSI catcher captures cell phone numbers and extracts target data by mimicking a cell tower. **Gossamer:** Same capabilities as StingRay II in a smaller, cheaper portable unit with added ability to launch DoS attacks. **Triggerfish:** Location-based data + real time call content interception. **Kingfish:** Tracks mobile device, identifies user, tracks connections to other devices. **Amberjack:** vehicle antenna that supports direct-finding for StingRay II, Gossamer and Harpoon.	LEAs, Govt. and Intel. agencies, Military.	**Also see Harris in “Malware.”**

Harris Corporation (continued)		**Harpoon.** **Hailstorm.**	**Harpoon:** amplifier that boosts signal of IMSI catchers to extend range. **Hailstorm:** Dual-mode (GSM/LTE) IMSI catcher for mobile location, with malware for capturing content and control of targeted devices. May be purchased as hardware, or as a software upgrade to a StingRay II or other Harris IMSI catcher.		
Intercept Monitoring Systems (IMS) – a Division of Discovery Telecom Technologies (DTT)	Moscow, Russia.	**AIBIS-2 IMSI Catcher.** **Advanced CDMA Interception Monitor.** **Iridium Satellite Interception (ISI) System.** **Advanced Thuraya Satellite Interception System (ATIS).**	**AIBIS-2 IMSI Catcher:** Active mobile location and content intercept of targets on GSM networks. **Advanced CDMA Interception Monitor:** Passive interception of CDMA calls/callers. **Iridium and Thuraya products**: Provide off-air interception of Iridium and Thuraya SATCOM "in the clear."	LEAs and Govt. agencies in Russia, CIS nations, Western Europe, Africa, LATAM and Asia.	OEMs geolocation devices. **Also see IMS under "Malware."**
iPS	Aprilia, Italy.	**G-TRACK.**	**G-TRACK:** Mobile location via beeper with GSM or GPS antenna, aided by RFID for precise tracking.	LEAs, Govt. & Intel. agencies.	**Also see iPS in "Lawful Intercept Vendors," "Malware," "Advanced Analytics," "Biometric Identification" and "OSINT and Social Media."**
MEDAV GmBH	Uttenreuth, Germany	**EiLT** (Emitter Localization under MulTipath Propagation Conditions).	**EiLT:** 5G blind mobile location: ability to track subscriber and future 5G throwaway phones.	CSPs,LEAs, Govt. & Intel. agencies, Military.	**Also see MEDAV under "Military."**

Elbit Systems CYBERBIT	Ra’anana, Israel.	**Target 360° Location.**	**Target 360° Location:** End-to-end mobile location n with 3D Accurate Positioning (X,Y and Z) axes in real time. on any network: GSM, UMTS, CDMA or LTE.	LEAS, Govt. & Intel. agencies.	**Also see Elbit Systems CYBERBIT in “Advanced Analytics,” “Lawful Intercept Solutions,” “Biometric ID,” “Malware,” “OSINT and Social Media” and “Military.”**
NORSI-TRANS	Moscow, Russia.	**Vitok-SIGTRANS.** **Vitok-MONITOR.**	**Vitok-SIGTRANS:** IMSI Catcher: Captures caller/called party MSISDN identifiers, IMSI and IMEI numbers plus call and device content. **Vitok-MONITOR:** IMSI catcher for tracking mobile location and content or communications, including bank transactions in real time.	LEAs, Govt. & Intel. agencies.	**Also see NORSI-TRANS in “Lawful Intercept Solutions,” “Packet Monitoring,” “Advanced Analytics,” and OSINT and Social Media.”**
Paladion	Mumbai & Bangalore, India.	**Cybercafe Tactical.** **Cybercafe Handheld.**	**Cybercafe Tactical & Handheld:** Provide tactical mobile location and onsite WiFi monitoring.	LEAs, Govt. & Intel. agencies.	**Also see Paladion in “Lawful Intercept Solutions,” “Malware,” “Advanced Analytics” and “Forensics.”**
Persistent Systems	Pune, India and 10 global locations including Australia, France, Germany, Japan, Kuala Lumpur and the U.S..	**Persistent Location Platform for Lawful Intercept.**	**Persistent Location Platform for Lawful Intercept:** Versatile mobile location and call interception system selects the appropriate technology per each case for positioning & content access. Supports GSM, UMTS and LTE. Stamps CDRs with accurate time & positioning for start & termination of call.	CSPs, LEAs.	

Polaris Wireless	Mountain View, CA, USA.	**OmniLocate.** **Altus.**	**OmniLocate:** Pattern matching tracks the target’s signaling to the precise wireless signature of a point in a cell network. Interoperates with third party lawful intercept systems and analytics. **Altus:** Real time OmniLocate functionality with on-demand location, tracking and geofencing of targeted subscribers. Plus mobile location of all subscribers in service provider’s network.	CSPs, LEAs, Govt. & Intel. agencies, Military.	Polaris end-to-end radio access network is powered by Radisys.
Protei Research Technologies	St. Petersburg, Russia.	**Protei Probes.**	**Protei Probes:** Hybrid Cell ID, Time Advance and GIS mobile location.	CSPs, LEAs, Govt. & Intel. agencies.	**Also see Protei in “Packet Monitoring.”**
Rafael Advanced Defense Systems	Haifa, Israel.	**PowerSpy.**	**PowerSpy:** Unique solution tracks mobile location by measuring power usage of device apps relative to distance from base stations.	LEAs, Govt. & Intel. agencies.	Joint project with Stanford University. Disclosed in 2015 academic research. No commercial product as of January 2016, but worth watching.
Rayzone	Tel Aviv, Israel.	**InterApp.** **Piranha.**	**InterApp:** WiFi interception solution uses Zero Days to “bug” a WiFi network. Can “pwn” (own) any target device, capturing and deciphering user email address and password, contact list, Dropbox, photos, Internet history browsing, as well as locations visited, IMEI number and MAC address. **Piranha:** Dual-mode (GSM/LTE) IMSI catcher for mobile location and	LEAs, Govt. & Intel. agencies.	**Also see Rayzone in “Malware.”**

Rayzone (continued)		**GeoMatrix.**	full content capture. Also works in “passive” mode to locate all mobile devices in targeted area. **GeoMatrix:** Advanced SS7-based system locates, tracks and “manipulates” GSM UMTS, 3G and LTE subscribers devices worldwide.		
RCS Labs	Milan, Italy	**MITO^3**	**MITO^3** suite includes**:** IMSI catcher; SS7/ GPS monitoring; passive GSM interception; WiFi Monitor.	LEAs, Govt. & Intel. agencies.	**Also see RCS Labs in “Lawful Intercept Solutions,” “Malware,” “OSINT and Social Media” and “Advanced Analytics.”**
Septier	Petach Tikva, Israel.	**Septier Hunter.** **Septier Gateway Mobile Location Center (GMLC).** **Septier Locator.**	**Septier Hunter:** “Unified” last mile positioning device monitors both GSM and UMTS (3G) phones. Forces the target’s mobile device to transmit at high power, making it easy to single out in crowded urban area. Hunter has the longest range of any last mile positioning device, is operated by smart phone and easily concealed for close-up surveillance or rapid arrest. **Septier GMLC:** GSM-based hybrid approach precisely IDs target locations based on IMSI, IMEI, MSISDN and TMSI when the user masks the phone number. **Septier Locator:** Works three ways**:** GPS, signal cross-referencing, and		**Also see Septier in “Lawful Intercept Solutions,” “Advanced Analytics” and “Military.”**

Septier (continued)		**Septier Cellular Extractor.** **Septier IMSI Catcher.** **Septier IMSI Catcher Mini.** **Septier Call Detail Record Generation.**	radio frequency "fingerprinting." **Septier Cellular Extractor:** Real time passive monitoring for extraction of all mobile call data in a designated area. **Septier IMSI Catcher:** In active mode, extracts GSM ID, IMSI and content of targeted device, or in passive mode, of all known devices in target area. **Septier IMSI Catcher Mini:** Pocket-sized tactical IMSI Catcher. **Septier Call Detail Record Generation:** Mobile CDR data retention.		
Shoghi Communications	Himachal Pradesh, India.	**SCL-5020.** **SCL-5020WB.** **SCL-5020SE.**	**SCL-5020**: Passive GSM device intercepts all network traffic without network interference. Parameters: IMEI, IMSI, TMSI, Target distance from the base station, type of target handset, target's dialed & received number. Uses circuit-switched fallback for LTE traffic. **SCL5020WB:** Passive GSM device. Intercepts all traffic in 50km area without network interference. Same parameters as SCL-5020. **SCL-5020SE:** Semi-active device GSM monitoring for SMS and GPRS	LEAs, Govt. & Intel. agencies, Military.	**Also see Vision Group in "Lawful Intercept" and "Military."**

Shoghi Communications (continued)		**SCL-GSMDF.** **SCL-5020C.**	data from GSM 2G, 2.5G,3G and 4G/LTE (with circuit-switched fallback). GPRS system integrates with HTTPS/SSL decryption engine to intercept and process the HTTPS/SSL encrypted traffic. Monitors social media. Does not require carrier's SIM and is invisible to target. **SCL-GSMDF:** Used with the SCL-5020SE Semi-Active device to mobile locate the target by measuring strength of signal. Can locate target in multi-story buildings. **SCL-5020C:** Passive monitoring for CDMA networks. Intercepts target's content and metadata and IDs caller number.		
Stratign	Dubai, United Arab Emirates.	**Passive GSM Monitoring & Management System** **STN 5020C.** **WiFi Interception System.**	**Passive GSM Monitoring & Management System:** Tactical interception of GSM & CDMA. **STN 5020C**: SATCOM. Radio interception of CDMA. **WiFi Interception System:** WiFi interception system collects WiFi packet, chat conversation and IP telephony from all 802.11x channels. Supports host-swappable disks.	CSPs, LEAs, Govt. & Intel. agencies, Military.	**Also see Stratign in "Malware" and "Military."**

Suntech – Verint Group	Florianópolis, Brazil.	**ENGAGE G12. (Verint)**	**ENGAGE G12:** Passive off-air interception of GSM and SATCOM networks.	LEAs, Govt. & Intel. agencies, Military.	**Also see Suntech in "Lawful Intercept Solutions" and "Advanced "Analytics."**
Syborg – Verint Group	Bexbach, Germany.	**ENGAGE G12. (Verint)**	**ENGAGE G12:** Passive off-air interception of GSM and SATCOM networks.	LEAs, Intel. agencies	Acquired by Verint (Aug 2011). Partners with Cisco, Ericsson, Oracle. **Also see Syborg in "Lawful Intercept Solutions."**
Telesoft Technologies	Blandford, Dorset, UK (HQ). Atlanta, GA, USA. Uttar Pradesh, India.	**Hinton ABIS Probe.**	**Hinton ABIS Probe:** Mobile geo-fencing. Finds the physical location of the mobile phone by measuring and triangulating signal links between mobile base stations.	LEAs, Govt. & Intel. agencies, Military.	**Also see Telesoft in "Lawful Intercept Solutions."**
Trovicor	Munich, Germany.	**Fusion System.**	**Fusion System:** Comprehensive surveillance system includes mobile location and Geomapping from call detail records.	LEAs, Govt. & Intel. agencies.	**Also see Trovicor under "Lawful Intercept Solutions," "Malware," "Advanced Analytics" and "OSINT and Social Media."**
Verint	Melville, NY, USA.	**ENGAGE G12.**	**ENGAGE G12:** Passive off-air interception of GSM and SATCOM networks.	LEAs, Govt. & Intel. agencies, Military.	**Also see Verint in "Advanced Analytics," "Lawful Intercept Solutions," "OSINT and Social Media," "Military" and "Malware."**

Chapter 5: Biometric Identification

Biometric identification is defined as the investigative or security use of human characteristics that uniquely distinguish the individual. It may be done in multiple ways: voice, facial, hand, fingerprint and retina or scan, DNA and others. Of these methods, the two most relevant to ISS are voice biometrics and facial recognition.

Voice biometrics is a technology that makes a biometric voice print (**BVP**) and audio signature that are as infallible a form of identification as a fingerprint.

Voice biometrics or “speaker recognition” is the identification of the speaker by voice characteristics. It is not to be confused with “speech recognition,” which identifies what is said. There are two types of speaker recognition: verification – for authentication – and identification. In ISS, voice biometrics solutions focus on the latter goal: identification.

Solutions by market leaders such as **AGNITiO** can scan hundreds of thousands of voice records in real time and identity the speaker by sex, language, dialect, keyword and other factors, even if the target switches language, device or location. The end result is a BVP specific to that individual.

Vendors like **Elbit Systems** subsidiary **CYBERBIT** provide voice biometrics that add the dimensions of context and semantics, determining the intent of the speaker. However, for the most part, systems rely on text-independent capabilities, identifying a target at random based on real time or recorded events, and without the target’s knowledge.

Voice biometrics is commonly used in combination with Big Data analytics solutions to create a holistic picture of the target and his or her affiliation with criminal and terrorist networks.

Facial biometric identification is based on the uniqueness of the human face, which cannot be disguised from such systems by eyeglasses, facial hair, hats or other means of partially hiding the face. The technology has delivered proven results even when the target’s face is turned and viewed at an angle. Facial recognition is often critical to identifying known or suspected criminals and terrorists and tracking their movements.

Facial biometrics has evolved beyond older 2D to new 3D capabilities. Further enhancements such as use of artificial intelligence (AI), advanced algorithmic analysis of 2D and 3D Big Data video banks, as well as the application of LIDAR (illumination and measurement of facial bone structure via laser light) have rendered facial biometrics a superb method of quickly identifying and tracking targets including the lone wolf.

Table 5. Biometric Identification

Company	Location	Solution	Function	Market	Of Note
AGNITiO	Madrid, Spain.	**BATVOX.** **BS3 Strategic.** **BS3 Tactical.** **SIFT.** **ASIS.**	**BATVOX:** BS3 core engine uses “Bayesian network” approach, a statistical model that draws the links between random variables and conditional dependencies to create target’s unique BVP with 99.2 percent accuracy. Scalable to 100K voices/minute. Identifies targets in different languages. **BS3 Strategic:** New in 2016 – BS3 uses computer clustering to enhance voice mining and reveal “spider nets” of related speakers. Separates multiple speakers, determines the gender of the target and generates a match. Removes artifacts, non-voice events and noises. **BS3 Tactical:** Light-weight version of BS3 Strategic for tracking finite group of targets. **SIFT:** BVP identification on a laptop. Processes 1,000 targets per 19 seconds. Provides noise blocking, multi-speaker identification and separation. **ASIS:** Client/server system for access to BVP database holding up to 1.0M voiceprints. Searchable to match target BVP to those stored in database.	LEAs, Govt. & Intel. agencies.	Acquired by Nuance, Nov. 2016. Companies that resell AGNITiO: Verint, VAStech, Ultra Electronics, Morpho, Dictao. Pen-Link & SecureReset. Companies that provide systems integration: SAIC, Thales, Cassidian, Indra.

Auraya Systems	Sydney, Australia.	**ARMORVox Speaker Identity System.**	**ARMORVox 16 Speaker Identity System:** Language, accent and dialect independent. Universal Background Model (UBM) process supports UBM models for local language and accent, globally.	LEAs, Govt. & Intel. agencies.	
BlueLight	Croydon, UK.	**BlueLight Global Solutions.**	**BlueLight Global Solutions:** Automated biometric speaker identification for any voice for language. Database for analytics.	LEAs, Govt. & Intel. agencies.	
Elbit Systems CYBERBIT	Ra’anana, Israel..	**Target 360° Voice Biometrics.**	**Target 360° Voice Biometrics:** Voice biometric solution determines the language, dialect, gender of the target. Semantic analytics indicates intent of the speaker.	LEAs, Govt. & Intel. agencies.	**Also see Elbit Systems CYBERBIT in “Advanced Analytics,” “Lawful Intercept Solutions,” “Mobile Location,” “Malware,” “OSINT and Social Media” and “Military.”**
Group 2000	Almelo, Netherlands. Oslo, Norway. Freienbach, Switzerland. Wilmington, DE, USA.	**LIMA Biometric Identity Surveillance.**	**LIMA Biometric Identity Surveillance:** 3D facial recognition solution uses LIDAR and stereovision to capture 40,000 data points per face, generating a facial topography of the target.	LEAs, Govt. & Intel. agencies.	**Also see Group 2000 in “Lawful Intercept,” Mobile Location,” and “OSINT and Social Media.”**
iPS	Aprilia, Italy.	**G-SPEECH.**	**G-SPEECH**: Voice biometrics.	Govt. & Intel. agencies.	**Also see iPS in “Lawful Intercept Solutions,” “Mobile Location,” “Malware” “Advanced Analytics” and “OSINT and Social Media.”**

NEC	Tokyo, Japan. Worldwide offices in Asia, the Americas, Europe, Africa and the Middle East.	**NeoFace Watch.**	**NeoFace Watch:** 3D video ID of targets using an AI/Big Data system that integrates with any camera array. Neural network (AI) algorithms map target’s face to identical match in video Big Data banks. Perturbation Space Method (PSM) algorithm renders various head angles to create “face print.” Adaptive Regional Blend Matching (ARBM) algorithm eliminates distortion from different facial expressions and blinking. Fully automated system “does the work” for the user.	LEAs, Govt. & Intel. agencies, commercial enterprises.	Per the U.S. National Institute of Standards and Technology (NIST), NeoFace Watch has the lowest error rate (3.1 percent), and twice the processing rate of its nearest competitor. Deployed by clients in 40+ nations. **Also see NEC in “Forensics.”**
Nuance	Burlington, MA, USA.	**Speaker Identification and Detection (S.P.I.D).**	**Speaker Identification and Detection (S.P.I.D.):** Biometric voice analysis and tracking. Language and gender ID. Keyword spotting.	LEAs, Govt. & Intel. agencies.	Acquired S.P.I.D. with purchase of Israel’s PerSay (2010). Acquired Italy’s Loquendo (2011). Acquired AGNITiO (Nov 2016)
Phonexia	Brno, Czech Republic.	**Speech Intelligence Resolver.**	**Speech Intelligence Resolver:** Real time ID of speaker in recorded or streaming audio. Biometric voiceprint extraction & comparison. Recognizes 50+ languages and can add new ones. Identifies dialects. Analyze multilingual content. Real time gender ID.	LEAs, Govt. & Intel. agencies.	Partners with Flowmon Networks. **Also see Phonexia in “Forensics.”**

STC	St. Petersburg, Russia.	**VoiceGrid Nation.**	**VoiceGrid Nation:** Country-wide solution for any number of users. Automatically compares "voice models" against voice recordings obtained from different sources such as cell phones, land lines, covert recordings and recorded investigative interviews. Conducts search/match in 10,000 voice samples in 5 seconds. Stores up to 2,000,000 samples. Integrates with STC forensics and other vendors' voice biometrics.	LEAs, Govt. & Intel. agencies.	Formerly known as Speech Technology Solutions. **Also see STC in "Forensics."**
		VoiceGrid Local.	**VoiceGrid Local:** Same as VoiceGrid Nation but limited to 10 seats.		
		VoiceGrid RT.	**VoiceGrid RT:** Real time voice biometrics and analysis for real time target ID. Processes "millions" of speakers per day and maps against database of 10K known targets. Text and language independent.		
Ultra Electronics	Middlesex, UK.	**Voice Print Analysis (VPA).**	**VPA:** Captures target ID and location via biometric voice print. Data can be merged with findings from other Ultra products: ARIES DPI and SAGE RF analysis, GEOINT and satellite imagery.	Govt. Intel., agencies, Military.	**Also see Ultra Electronics in "Packet Monitoring," "Advanced Analytics" and "Military."**
Voice Biometrics Group	Newtown, PA, USA.	**VMM-1.**	**VMM-1:** Voice biometric engine, a high-volume request broker. Provides scalable database, and web-based administration and reporting.	Enterprises, LEAs.	Primary use is VBM identification of prison inmates.

Chapter 6: Ethical Malware Vendors

Ethical malware solutions are intrusive systems with the ability to capture device traffic and content, “keyboard sniff,” view web surfing, view and modify content uploads or downloads, take charge of a device’s microphone, camera or video camera, and send messages on behalf of the target. The malware may be installed directly via USB into the target’s PC or laptop, or remotely through the subterfuge of phishing, emails, advertisements, “rogue” (fake) websites, social media and social engineering that gull the target into clicking on a link that uploads the intrusion.

Also growing in popularity: “drive-by” attacks via rogue websites engineered to the target’s known “likes” or via DNS hijacking, i.e., reconfiguring the target’s domain name search (DNS) capabilities to route him or her to a website that plants malware. Drive-by attacks are similar in nature to “packet injection,” a hacking technique commercially introduced by Gamma Group International around 2007 and possibly inspired by the NSA. Packet injection is a sophisticated form of intrusion that injects packets into backbone networks or specific devices, redirecting targets to a rogue server which then launches a MITM attack. The technique is identical the NSA’s **QUANTUMINSERT** program, which follows the same process and redirects the target to the agency’s rogue **ACID** website for a MITM attack and malware plant.

Lawful malware often leverages Zero Days, i.e., system vulnerabilities that are not published or known. For years, **Vupen** was the key provider of military grade Zero Days for Western intelligence agencies. Vupen officially closed shop in May 2015 and was replaced by **Zerodium** under the same management team. Zerodium now offers bounties to researchers for premium Zero Days, but professes that it no longer produces them.

Endgame Systems is another respected Zero Days company. Perhaps the best-known player is **The Equation Group**, a coined name for Zero Day/malware experts thought responsible for the cyberattack that disabled Iranian nuclear reactors. You won’t find The Equation Group in this book, though they are reviewed by *Insider Surveillance.* They are strictly a government operation, most likely a joint initiative by the U.S. and Israel, and they do not sell their work.

Providers of communications devices often unwittingly open the door to Zero Days and malware by failing to implement patches for weaknesses. Even Apple, renowned for its device security, has its lapses. A much publicized vulnerability in Apple’s Thunderbolt USB port went uncorrected for many months until January, 2015. There are many other such examples.

Ethical malware surveillance technologies that invade and control a target’s device have been available for well over a decade, and are commonly used by U.S. law enforcement, intelligence and government agencies worldwide.

Despite efforts to curb it, ethical malware surveillance continues to grow, spanning products by niche players, defense contractors and lawful intercept vendors, and spurring new market entrants from the Middle East and Asia. Note: Malware providers are not immune to cyber attacks. FinFisher was hacked in August 2014, and The Hacking team was hacked in July 2015.

Table 6. Ethical Malware Vendors

Company	Location	Solution	Function	Market	Of Note
Ability	Tel Aviv, Israel.	NA	Zero Days used for Ability's ULIN product.	Intel. agencies, ISS partners.	**NSO Group** uses Ability Zero Days to plant malware on mobile devices. Ability has discussed partnership with Italy's The Hacking Team and is possible reseller of HT malware. **Also see Ability in "Mobile Location."**
Aglaya	New Delhi, India.	**iOSBackdoor.** **Android Backdoor.**	**iOS and Android Backdoors:** Remote control of target's device. Both require an unattended device and knowledge of its passcode. Malware is installed via direct access to device (not remotely).	LEAs, Govt. & Intel. agencies	**Also see Aglaya in "Packet Monitoring" and "Mobile Location."**
		Supercomputer Instances.	**Supercomputer Instances:** Users may buy time on Aglaya's supercomputers for brute force attacks on target passcodes. System checks up to 30K passwords per second.		
ClearTrail Technologies	Indore, India.	**Astra SEED.**	**Astra SEED:** Remote intrusion software targets devices via SEED bot. Complete visibility and control of encrypted content.	LEAs, Govt. & Intel. agencies.	**See ClearTrail in "Lawful Intercept Solutions," "Packet Monitoring," "Mobile Location," and "Advanced Analytics."**

DigiTask	Hesse, Germany.	**R2D2.**	**R2D2:** Remote forensic stealth software deployed on target’s device that decodes encrypted data (PGP, GnuPG, Tor/JAP) including IM regardless of location or movement.	LEAs.	**Also see DigiTask in “Packet Monitoring” and “Mobile Location.”**
Elaman	Munich, Germany. Amriswil, Switzerland.	**FinFisher.**	**FinFisher:** Elaman resells FinFisher as “Elaman FinFisher.”	Govt agencies; LEAs.	**Also see Elaman in “Packet Monitoring.”**
Endgame Systems	Arlington, VA, USA	**Bonesaw.**	**Bonesaw:** Zero Day exploits for specific vulnerabilities.	Govt. & Intel. agencies.	Since public exposure in 2011, Endgame has moved into cyberdefense. Still provides Zero days to U.S. and the “Five Eyes” nations.
FinFisher GmbH	Munich, Germany.	**FinSpy.** **FinFly.** **FinWiFiKeySpy.**	**FinSpy:** System for remote spying on target’s fixed or mobile device. Plants malware to intercept encrypted and anonymous traffic. Performs live surveillance through target’s camera & videocam. Extracts device files. Provides remote device forensics. Effective against Windows, MAC and Linux systems. **FinFly:** Transparent HTTPs proxy for modifying target files during download. **FinWiFiKeySpy:** Remotely	LEAs, Govt. & Intel. agencies.	FinFisher software generates encryption certificates and deciphers/imports data remotely or from dongles. Modifies files while being uploaded or downloaded – works for one or many targets; bypasses anti-spyware & anti-virusware. Cracks passwords & hashes. Sees all websites visited by the target(s). Professional Trojan for Skype, IM. Sniffs strokes on wireless keyboards. Records voice between mobile

FinFisher GmbH (continued)		**FinBluez.** **FinFisher Crawler.** **FinFisher Case Management.** **Finfisher HQ.** **FinTraining.**	monitors target's keystrokes on WiFi networks. **FinBluez:** Conducts advanced attacks against Bluetooth devices. **FinFisher Crawler:** Infects and monitors social networks. **FinFisher Case Management:** Advanced analytics keyed to data intercepted by FinFisher products. **FinFisher HQ:** Graphical user interface for analysis of hacked data. **FinTraining:** IT intrusion training and support in FinFisher products.		device & Bluetooth. Activates device webcam & microphone. Ostensibly spun off by Gamma Group Intl (GGI) in 2014 and now an independent German company, with "Branch office" in Andover, UK – also the HQ location of Gamma Group. FinFisher partners with Elaman. **Also see FinFisher in "OSINT and Social Media."**
The Hacking Team	Milan, Italy. Singapore. Annapolis, MD, USA.	**Remote Control System.**	**Remote Control System:** Controls suspect's device via undetectable infection – installation can be remote or on-site via USB.	CSPs, Govt. & Intel. agencies.	Italian regulators revoked Hacking Team's global export license in April 2016. Company continues to market at ISS World events and sells RCS through network of partners. 2015 hack by "Phineas Fisher" black hat captured 1.0 million company emails, with disclosure of cases where company defrauded clients by faking results during live product demos or distracting clients when tests failed.

Harris Corporation	Melbourne, FL, USA.	**Hailstorm.**	**Hailstorm:** 4G LTE interception upgrade. Like a Trojan, takes over mobile device: remotely turns on microphone, camera, sends messages.	LEAs, Govt. & Intel. agencies.	**Also see Harris in “Mobile Location.”**
Intercept Monitoring Systems (IMS) – a Division of Discovery Telecom Technologies (DTT)	Moscow, Russia.	**Tomahawk 7 Click Infection System.**	**Tomahawk 7 Click Infection System:** Remote Trojan capability for intrusive monitoring of PCs and Android devices.	Govt. & Intel. agencies only, upon receipt of a user certificate.	**Also see IMS in “Mobile Location.”**
iPS	Aprilia, Italy.	**G-SEC.** **ITACA.**	**G-SEC:** Man-in-the-middle attacks. **ITACA:** Remote Trojan capability to take over any Windows or Android device.		**Also see iPS in “Lawful Intercept Solutions” “Mobile Location,” “Biometric ID,” “Advanced Analytics” and “OSINT and Social Media.”**
Elbit Systems CYBERBIT	Ra’anana, Israel.	**CYBERBIT PC Surveillance System.**	**CYBERBIT PC Surveillance System:** Zero Days for network penetration. Trojan capability for monitoring keystrokes, taking control of the target’s device to intercept content and view all web pages or co-conspirators contacted.	LEAs, Govt. & Intel. agencies	NICE, acquired by Elbit in 2015, resold Hacking Team RCS. CYBERBIT Zero Day & malware capabilities are now developed in-house. **Also see Elbit Systems CYBERBIT in “Advanced Analytics,” “Lawful Intercept Solutions,” “Mobile Location,” “Biometric ID,” “OSINT and Social Media” and “Military.”**

NSO Group	Herzliya, Israel.	**Pegasus.**	**Pegasus:** Zero Days and malware for taking down smart phones. Attacks via one-click (text message with a link to a malicious website) or zero-click (WAP Push SL message that causes phone to automatically open a link). Device is then routed to a Pegasus Installation Server for malware deployment. Agent’s ID is kept anonymous.		Successful against Apple IoS. Per Ability Group Chairman, NSO Group uses Zero Days by Ability.
Paladion	Mumbai & Bangalore, India.	**Decryption Remote.** **Remote Monitoring.**	**Decryption Remote:** In-line & parallel man-in-the-middle attacks on SSL. **Remote Monitoring:** Malware installed by USB or via behavioral techniques; intercepts any content from user device.	LEAs, Govt. & Intel. agencies.	**Also see Paladion in “Lawful Intercept Solutions,” “Mobile Location, “Advanced Analytics,” and “Forensics.”**
Rayzone	Tel Aviv, Israel.	**The Hacking Team RCS.**	“Trojan system for PCs, mobile devices, cloud and apps.” [**See The Hacking Team.]**	LEAs, Govt. & Intel. agencies.	Rayzone resells Hacking Team’s RCS malware. **Also see Rayzone in “Mobile Location.”**
RCS Labs	Milan, Italy	**MITO^3 Intrusive.**	**MITO^3 Intrusive:** Trojan infests and monitors any target PC or mobile device.	LEAs, Govt. & Intel. agencies.	**Also see RCS Labs in “Lawful Intercept Solutions,” “Mobile Location” “OSINT and Social Media” and “Advanced Analytics.”**

SS8	London, UK.	NA	Co-produces malware with BT for the GCHQ.	LEAs, Govt. & Intel. agencies, Military.	**Also see SS8 in "Lawful Intercept Solutions" "Packet Monitoring" and "Advanced Analytics.**
Stratign	Dubai, United Arab Emirates.	**Spy Phone.**	**Spy Phone:** Takes over target's cell phone, sees calls and SMS, takes over microphone to monitor room conversations.	LEAs, Govt. & Intel. agencies, Military.	**Also see Stratign in "Mobile Location."**
Trovicor	Munich, Germany.	**Fusion System.**	**Fusion System:** Comprehensive surveillance system includes Zero Days and malware.	LEAs, Govt. & Intel. agencies.	**Also see Trovicor under "Lawful Intercept Solutions," "Mobile Location," "Advanced Analytics" and "OSINT and Social Media."**
Verint	Melville, NY, USA.	**Hacking Team RCS.**	**[See The Hacking Team.]**	LEAs, Govt. Intel. agencies.	Verint resells Italy's The Hacking Team malware. **Also see Verint in "Advanced Analytics," "Lawful Intercept Solutions," "Mobile Location," "Military" and"OSINT and Social Media."**
Yaana Technologies	Milpitas, CA, USA.	**TunnelBox**	**TunnelBox:** "Remote traffic access" of IP streams and device memories: man-in-the-middle attacks.	LEAs, Govt. & Intel. agencies	**Also see Yaana Technologies in "Lawful Intercept Providers" and "Packet Monitoring."**
Zerodium	Montpelier, France. Annapolis, MD, USA.	**Zerodium Payout.**	**Zerodium Payout:** Purchases Govt.-grade Zero Day exploits for operating systems, web	Govt. & Intel. agencies.	Zerodium, run by Chaouki Bekrar, replaced Vupen in August 2015. Zerodium offers bounties for Zero Days, which is

Zerodium (continued)			browsers, plug-ins & readers, mobile devices and phones, Web and email servers, Web apps, and for techniques including mitigation bypass, Tor de-anonymization and anti-virus RCE/LPE (remote customer edge router/local privilege escalation).		sells to clients. Zerodium ostensibly does not product Zero Days as Vupen did, but retains the same staff and capabilities.

Chapter 7: Advanced Analytics Solutions

Today terms such as “Advanced Analytics,” “Big Data” and “Data Science” are used with abandon. To appreciate their meaning and value it is worthwhile to delve into their origins: the evolution of computing, the rise of “structured” data and the explosion of “unstructured” data fueled by the personal computer, the Web, universal mobility, streaming data and video. All of these factors have contributed to what we call “Big Data,” sets of data so large and complex that they surpass the capabilities of conventional computing.

Big Data actually began more than a century ago. At the time it was known as storage by paper documents in file cabinets which accumulated by the ton at government agencies and corporate enterprises. Like early digital data, data on paper, too, defied analytics.

From Punch Cards to Big Iron

The first “computer” to address the vast corridors of plain paper storage was the “punch card” calculator of 1929, which used paper cards dotted with holes in predefined positions representing specific elements of data. Initially confined to simple calculations, the punch card computer evolved into more complex processing machines, but still relied on paper cards for storage, processing and memory for years to come.

Although invented by a separate company, this semiautomatic processing was quickly taken over by IBM, which dominated the field until a better alternative arrived: the first card-free digital processer, the IBM 701, introduced in 1952. Also known as the Defense Calculator – which gives a hint as to the forces behind its development – the IBM 701 launched the era of computers with internal electronic memories. Within a year, memory switched to tape on reels. In 1956 IBM formed its “Big Iron” division to manufacture what soon became known as the mainframe computer.

By the early 1960s, the business end of enterprise and defense IT were in the hands of numerous mainframes that used large scale computer architectures to process bulk data. Burroughs, UNIVAC, Control Data and RCA and three other companies entered the field, but because IBM commanded 90 percent market share its competitors were often dismissed as the “seven dwarves.”

Structured vs. Unstructured Data

As data sets grew more “bulky,” engineers sought new ways to improve their management and utilization. Among the key breakthroughs was the development of the “relational database” by IBM in 1970. The importance of the relational database: It provided a simple way to organize data in formally-recognized tables that could be accessed, analyzed and manipulated without having to rewrite the tables that held the data. Properly formatted, such data was termed “structured,” that is, cast in predesignated models that defined how data would be recorded, stored, processed and accessed. Though dated in many ways and declining in popularity today, relational databases for structured data still have their advocates.

With structured data, decisions are made on the types of fields to be used for storage of each data type – alphabetic, numeric, currency, name, date, address, etc. – plus their *relations*, and any restrictions on types of data to be retained. Structured data is typically stored in a relational database such as SQL (Structured Query Language), which became a formal standard when adopted by the American National Standards Institute in 1986.

SQL databases were, and still are, relatively simple to use within certain parameters. Limitations include the high cost of storage, memory and processing. Also, any data that does not fit a predefined category may “fall out.” Such irregular data would eventually become a problem.

In the early 1990s, along came the personal computer, word processing and then the World Wide Web packed with images, photos and video. None of these new types of data fit the standard SQL models. Being “unstructured,” they had no home in the relational database. Unfortunately for those fond of SQL, the services that hinged on these rebellious packets were also highly popular. By the late 1990s, it was estimated that between 80 – 90 percent of useable data originated in unstructured form, that is, outside the management capabilities of a standard SQL database.

SQL Gets a Sequel

IBM and others had been aware of the problem as early as the 1960s, working on early versions of what would later become the “Not Only SQL” or NoSQL database. The NoSQL database introduced the concept of accessing data via “associative” modeling outside the limitations of SQL’s tabular modeling.

NoSQL’s arrival was timely for another reason: the bandwidth boom. NoSQL could “horizontally scale” to other nodes outside the system to either increase or decrease the amount of computing power required for complex tasks. Today the common term for this capability is "distributed computing," the practice of spreading massive parallel processing requirements across a near-infinite array of servers in the network.

NoSQL is not a perfect solution to the challenge of unstructured data, nor in every way a "besting" of SQL. NoSQL offers availability and speed, sometimes at the sacrifice of consistency, although new developments have reduced correction times to milli-seconds. SQL is still better at simple transactions such as one-function needs – bank transactions, transfer of files within a single database, etc.

But NoSQL paved the way for innovative advances such as data mining, Natural Language Processing and text analytics systems that reveal patterns in data. Bulk metadata collection and analysis is one example. Voice tagging used in voice biometrics systems is another.

With the advent of NoSQL, distributed computing and databases, relational databases are quickly fading into the past as standalone solutions. Simply put, NoSQL scales, SQL does not. NoSQL is used by the CIA, Google and other organizations with massive data management requirements. That said, as Big Data soars to multi-zettabyte levels, NoSQL and similar database systems require an enabler to facilitate ever-faster distributed processing.

Distributing Computing – How it Works

Enter the Apache Software Foundation, a U.S.-based non-profit organization representing a community of developers dedicated to finding new and better ways of accelerating Big Data management. Apache's most famous contribution is Hadoop, a "software ecosystem" that organizes the process of massive parallel processing across multiple servers.

Hadoop itself is not distributed processing, but rather, a set of interfaces that facilitate computing clusters. In action, Hadoop enables creation of a "data lake" of information relevant to specific queries. Other Apache solutions such as Apache Spark build on Hadoop, further accelerating data flow and computing, and accepting content from any data source including traditional SQL databases.

All Apache programs are free and downloadable from their website. From the analytics standpoint, whether for ISS or other needs, the action begins with paid programs that use special algorithms to "score" findings from data, that is, narrow the data field to the most relevant items in real time – and see what potential futures they point to. These "real time predictive" capabilities cross the line from traditional to Advanced Analytics.

Real Time Predictive Analytics

To the data scientist, classic data analysis is "heuristic" or historic, drawing conclusions from past incidents. Real time analytics goes an important step further by collecting data "in the moment," or alternately, at whatever improved time parameter is set by the user. To understand the distinction, consider that definitions of real time can vary and “real time” can be a relative term. For example, in a system previously set to collect data monthly or weekly, the transition to “real time” might mean collecting data by the day or the hour. However, real time is generally considered as being within seconds, or increasingly, milliseconds, to gather and analyze data from thousands of sources. What keeps the process real time (and processing costs under control): As a new data item is collected, the oldest is jettisoned.

Predictive analytics operates in similar fashion, aggregating and scoring both heuristic and real time data to produce “actionable intelligence” based on trends and patterns that point to the most likely set of future actions or events.

Once again, IBM holds the lead. A pair of products – IBM Netezza and IBM SPSS – are, respectively, the best known and most commonly used software applications for real time and predictive analytics or RTPA.

What if the findings of Advanced Analytics are themselves so “big” that they defy comprehension or fail to provide complete understanding? Here visualization tools come into play, providing 2D or 3D graphics that clearly illustrate what numbers alone might not say: the scope of a major data event, even hidden connections that were previously unrecognized. One of the best in that game is **Palantir**, a company whose visualization products have proven their value in bringing Advanced Analytics to life for users across a range of fields: financial services, first responders, military and intelligence organizations.

There you have it: the origins and operations of computing, database management and Advanced Analytics in a nutshell.

Advanced Analytics and ISS

With the influx of communications and Web data covered by surveillance technologies, Advanced Analytics play a vital role in the job of evidence and intelligence gathering. Analytics reduces this maze of information to useable granules that can reveal previously undetected patterns and networks. Examples: the ability to build on social media analysis to identify co-conspirators not even *on* the social media network, or to locate and visualize the hidden source behind distributed denial of service (DDoS) attacks.

The end game of analytics is deeper understanding of meaning and intent: what the data reveals about the identity, relationships, behaviors, areas of activity, timeframes and imminent threats posed by targets known and unknown. The arsenal of capabilities now available to address these issues is impressive and growing:

- Big Data Real time Predictive Analytics (RTPA).

- Semantic Analytics

- Link Analysis
- Visualization
- Data Retention with Purpose-Built Search
- Deep Web Analytics [OSINT and Social Media are covered in Chapter 9]
- “Cognitive” computing, aka Artificial Intelligence (AI)
- Cryptanalysis

There is no “one best tool” in the universe of analytics. Each system provides a set of capabilities that contribute to a holistic picture of the target and the threat: Big Data RTPA for current insights and future likelihoods; Deep Web Monitoring for lost or forgotten threads of OSINT insights that contribute context; semantics for precise understanding of what is spoken or written; link analysis to build connections; visualization to graphically represent mission critical data and reveal hidden parties; comprehensive storage of structured and unstructured data that is continuously added in a real time collection environment; and purpose-built navigation of the data sources.

Among the most significant developments in advanced analytics: systems that learn, make decisions based on variations in what is observed, single out potential risk, and thereby come as close to thinking as a machine possibly can. In development for nearly 50 years, “cognitive computing,” “machine learning” or as it is more commonly known – “artificial intelligence” – is far from perfect. But some, such as Elon Musk of Tesla and SpaceX, believe that we are close to seeing the first true thinking machines. Musk would know: He is a major investor in AI.

Of course, analytics can only be applied when data is “in the clear,” and with the growing popularity of encryption, the mission of cryptanalysis has taken on increased urgency. The challenge to most users is that excellent encryption systems such as PGE (Pretty Good Encryption) can be difficult to master. Tor is simpler to use, but as the NSA and academic researchers have proven, Tor is by no means a 100 percent guarantee of anonymity. For that matter, neither is PGP.

ISIS and other terrorist organizations have become adept at encryption. Government agencies and ISS vendors are equally committed to thwarting them. But cryptography vs. cryptanalysis is a neck-and-neck race where the lead constantly changes hands.

Table 7. Advanced Analytics Solutions

Company	Location	Solution	Function	Market	Of Note
ATIS UHER	Bad Homburg, Germany.	**Klarios F3S.** **Klarios RDC.** **Klarios SEE.** **Klarios IDA.**	**Klarios F3S:** Petabyte data retention. **Klarios RDC:** Combines access to CSP retained data with real time intercept for added context. **Klarios SEE:** Purpose-built search engine for Klarios SCP. **Klarios IDA:** Big Data analytics & visualization.	LEAs, Govt. & Intel. agencies, and Military.	**Also see ATIS UHER in "Lawful Intercept Solutions," "Mobile Location" and "Military"**
BAE Systems Applied Intelligence	Guildford, UK. Manassas, VA, USA.	**NetReveal Identifier.** **NetReveal Visualizer.** **NetReveal Analyzer.** **Real time Scoring and Scenario Building.** **Real time Predictive Analytics.**	**NetReveal Identifier:** Applies search criteria to the target entities and their connected network. **NetReveal Visualizer:** Shows associations via graphics. **NetReveal Analyzer:** Visualization of targets, associates, terms, times and locations. **Real time Scoring and Scenario Building:** Target and network profiles in real time. **Real time Predictive Analytics:** Heuristic + streaming real	LEAs, Govt. & Intel. agencies, and Military.	**Also see BAE Systems in "Lawful Intercept Solutions."**

BAE Systems Applied Intelligence (continued)			time data with “next best action” guidance from predictive analytics.		
BrightPlanet	Sioux Falls, SD, USA.	**Deep Web Harvester.** **OpenPlanet Enterprise Platfform.** **DeepWeb Monitor.**	**Deep Web Harvester:** SaaS or enterprise solution for web data acquisition. Finds data sources not available in Hidden Web. **OpenPlanet Enterprise Platform:** Big Data analytics. **DeepWeb Monitor:** Twitter, Facebook, RSS feeds, blogs, criminal records + BrightPlanet’s Deep Web database.	LEAs, Govt. & Intel. agencies, Military.	**Also see BrightPlanet in “OSINT & Social Media Monitoring.”**
ClearTrail Technologies	Indore, India.	**ClearInsight.**	**ClearInsight:** Provides analytics and visualization of intercepts from all networks including SATCOM + social media.	CSPs, LEAs, Govt. & Intel. agencies.	Also see **ClearTrail in “Lawful Intercept Solutions,” Packet Monitoring,” “Mobile Location” and “Malware.”**
Elbit Systems CYBERBIT	Ra’anana, Israel.	**WIT.**	**WIT:** Bulk metadata collection & analytics platform for HUMINT, SIGINT, OSINT, GEOINT and IMINT (image intel.)	LEAs, Govt. & Intel.agencies.	**Also see Elbit Systems CYBERBIT In “Advanced Analytics,” “Lawful Intercept Solutions,” “Mobile Location,” “Biometric ID,” “Malware,” “OSINT and Social Media” and “Military.”**

Expert System	HQ: Modena, Italy. Offices in Rockville, MD, Cary, IL & San Francisco, CA, USA.	**Cogito Intelligence**.	**Cogito Intelligence:** Semantic analysis software identifies targets by their writing. Provides text mining, categorization, semantic tagging, fact mining, and extraction of entity and relationships.	CSPs, LEAs, Govt. & Intel. agencies.	
Fifth Dimension	Tel Aviv, Israel.	**Fifth Dimension.**	**Fifth Dimension:** Pre-crime. "Deep Learning" (AI) approach implants complex algorithms on GPUs to accelerate Intel. gathering speeds up to 30 percent. Solution "thinks and acts" to assess threats in real time.	LEAs, Govt. & Intel. agencies.	
Glimmerglass Networks	Hayward, CA, USA.	**CyberSweep.** **Insight Analytics.**	**CyberSweep:** International gateway, submarine cable landing station and central office point-of-presence for acquisition and analysis of content on TDM, IP, ATM and social media networks. **Insight Analytics:** Discovers known or	CSPs, LEAs, Govt. & Intel. agencies.	

Glimmerglass Networks (continued)			suspected targets and depicts the communication pattern among associates. Discovers the source and entity relationships from raw data and addresses.		
HP Enterprise	Palo Alto, CA, USA.	**HAVEn.** **HP Vertica Dragline.** **HP Distributed R.** **HP DRAGON Green.** **HP DRAGON Orange.** **HP DRAGON Red.** **HP DRAGON Purple.**	**HAVEn:** Big Data Analytics on HP Vertica platform. **HP Vertica Dragline:** Real time insights. **HP Distributed R:** Predictive analytics. *Data management & analytics by database type:* **HP DRAGON Green** for Oracle. **HP DRAGON Orange** – for MySQL. **HP DRAGON Red** – for RainStor. **HP DRAGON Purple** – for HP Vertica.	LEAs. Govt. & Intel. agencies.	Effective March 2017 HP Enterprise Services Division (including ISS) is acquired by Computer Sciences Corp. **Also see Hewlett-Packard in "Lawful Intercept Solutions."**
IBM	Armonk, NY, USA.	**IBM i2 Safer Planet.** **IBM i2 Analyst's Notebook with i2 Analysis.**	**IBM i2 Safer Planet:** Master brand for the i2Safer Planet portfolio. **IBM i2 Analyst's Notebook with i2 Analysis:** Sifts through target data to determine target ID and	LEAs.	IBM's i2 Safer Planet suite is used by more than 6,000 police departments. But the suite reflects IBM's nosedive on R & D and strong dependence on acquisitions. IBM acquired i2 (2011), and

IBM (continued)		**I2 Enterprise Insight Analysis – Core and Advanced:** **COPLINK.**	networks of affiliates, patterns, timelines and imminent threats – from SIGINT, COMINT and OSINT. Provides data visualization. **I2 Enterprise Insight Analysis – Core and Advanced:** Identical to i2 Analyst's Notebook but with “3D data” and geospatial coordinates of target. “Core” version is for users with small data sets. “Advanced” is for “Big Data. **COPLINK:** IBM's “pre-crime” tool for LEAs. Shows likely location and timing of criminal acts by profiling targets and past crimes from criminal databases, OSINT and social media.		after 25 years i2 tech is showing its age. Real time analytics is by Netezza (acquired 2010), predictive analytics from SPSS (acquired 2009) and an eclectic mix of other analytics products from four separate IBM divisions.
iPS	Aprilia, Italy.	**G-WISE.** **G-SEARCH.**	**G-WISE:** Big Data analytics of metadata and content for trend analysis + predictive analytics. **G-SEARCH:** Semantic text analysis for precise meaning of target's text.	Govt. & Intel. agencies.	**Also see iPS in “Lawful Intercept Solutions,” “Mobile Location,” Malware,” “Biometric ID,” and “OSINT and Social Media.”**

Kofax	Irvine, CA, USA.	**Kofax Capture.**	**Kofax Capture**: Collects and provides real time intelligence from all types of text, including machine print, hand print and cursive handwriting, in more than 140 languages.	Govt. & Intel. agencies.	Lexmark acquired Kofax (May 2015). Kofax acquired Kapow Software (Irvine, CA), Aug 2013. **See Kofax Kapow in "OSINT and Social Media."**
Leidos	Reston, VA, USA.	**Mission Solutions.**	**Mission Solutions:** Big Data and real time predictive analytics for SIGINT. Delivers Content and thematic analysis via Natural Language Processing.	Govt.& Intel. agencies and Military: DHS, the Intelligence Community – notably DoD & NSA.	Leidos was created as a defense-focused spinoff of SAIC in Sept 2013. **Also see Leidos in "OSINT & Social Media Monitoring."**
MemSQL	San Francisco, CA, USA.	**MemSQL In-Memory Database.**	**MemSQL In-Memory Database:** Accelerates Big Data analytics by scaling out storage in RAM versus disc, and using distributing processing.	Govt. & Intel. agencies.	Backed by CIA VC In-Q-Tel.
NORSI-TRANS	Moscow, Russia.	**Vitok-3X.**	**Vitok-3X:** Visualization software for Big Data. Presents vivid graphics showing intersection of target's communication with financial info and geolocation.	Govt. & Intel. agencies.	**Also see NORSI-TRANS under "Lawful Intercept Solutions," "Packet Monitoring," "Mobile Location," and "OSINT and Social Media."**

Paladion	Mumbai & Bangalore, India.	**Link Analysis.**	**Link Analysis:** Analyzes target relationships.	LEAs, Govt. & Intel. agencies.	**Also see Paladion in "Lawful Intercept Solutions," "Mobile Location," "Malware" and "Forensics."**
Palantir	Palo Alto, CA, USA.	**Palantir Intelligence.**	**Palantir Intelligence:** Analytical reasoning facilitated by interactive visual interfaces. Fuses SIGINT, HUMINT, OSINT, GEOINT and other sources, integrating structured, unstructured, relational, geospatial and temporal data into a single model. Delivers visualization of trends, events, relationships. For operational strategic planning & tactical response.	CIA, other Govt. & Intel. agencies, enterprise market including financial sector and first responders.	Based on Java. Received start-up funding from In-Q-Tel, CIA's non-profit VC. **Also see Palantir in "Military."**
Raytheon	Waltham, MA, USA.	**Data Clarity.** **Raytheon Sureview.**	**Data Clarity** and **Raytheon Sureview:** identical products sold by two different divisions – Raytheon Websense and Raytheon Cyber Products – in both cases targeting the same market, LEAs. For visualization of	LEAs.	Both Raytheon products derive from Raytheon's acquisition of Visual Analytics (2012). Visual Analytics was founded in 1998 and predates Palantir by 5 years. Raytheon does not offer Data Clarity or Sureview to U.S. military –

Raytheon (continued)			complex data from OSINT, evidence and other sources. Applies network analytics, computational analytics & temporal analytics of events and behaviors to Big Data.		the 2 products compete with the Distributed Common Ground System (DCGS), a joint venture of Raytheon and Lockheed. **Also see Raytheon in "Military."**
Roke Manor Research (a Chemring Group company)	Romsey, Hampshire UK.	**Big Data Exploitation.**	**Big Data Exploitation:** Real time analytics. Extracts, scores and applies statistical analysis to heuristic and streaming data to deliver "actionable insights."	Govt. & Intel. agencies, Military and Enterprises.	**Also see Roke Manor Research in "Lawful Intercept Solutions," "Forensics" and "Military."**
RCS Labs	Milan, Italy.	**MITO^3 Analytics.**	**MITO^3 Analytics:** Statistical analysis of targets and groups for trends and behavior; matched to maps, dates, times; Palantir-like visualization.	LEAs, Govt. & Intel. agencies.	**Also see RCS Labs in "Lawful Intercept Solutions," "Mobile Location" "OSINT and Social Media" and "Malware."**
SciEngines	Kiel, Germany.	**RIVYERA S6-LX150.**	**RIVYERA S6-LX150:** Performs brute force custom hardware attack for cryptanalysis. Massive parallel processing system based on FPGAs (field programmable gate arrays)	Govt. & Intel. agencies.	

SciEngines (continued)		**RIVYERA S6-LX150 DDS.**	made by Xilinx. **RIVYERA S6-LX150 DDS:** Desktop version of the S6-LX150.		
Septier	Petach Tikva, Israel.	**Septier Information Explorer.**	**Septier Information Explorer:** Big Data Analytics system provides a data pool like Hadoop , then applies scoring, statistical analysis, heuristic and predictive analytics to determine targets of interest, and guide preemptive actions.	LEAs, Govt. & Intel. agencies, Military.	**Also see Septier in "Lawful Intercept Solutions," "Mobile Location" and "Military."**
Sqrll	Cambridge, MA, USA.	**Sqrll Enterprise.**	**Sqrll Enterprise:** Real time predictive analytics software, powered by Apache Accumulo to reveal threat patterns from metadata.	NSA, Govt. & Intel. agencies.	Sqrll Enterprise is the alleged basis of NSA's PRISM. Sqrll was founded by six former NSA employees. Company is led by former White House cybersecurity strategy director.
SRI International	Menlo Park, CA, USA.	**Angler.** **SEAS.**	**Angler:** Web-based collaboration tool for consensus and ranking. Uses SRI's "AI" programs AI2 for clustering, consensus and ranking. **SEAS**: "Structured Evidential Argumentation System."	Govt. & Intel. agencies.	AI2: marketed as cognitive or "human like" reasoning, but involves as much human as AI collaboration.

SRI International (continued)			Designed for Intelligence Community, provides analytics for assessing stability and terror threats.		
SS8	Milpitas, CA, USA.	**Intelligo Investigator.** **Intelligo iDossier.**	**Intelligo Investigator:** Analytics for visualization of intelligence, trends and threats revealed by voice, data, social media, CDRs, OSINT and Link Charting. **Intelligo iDossier:** Provides storage and analysis of CDR, IPDRs, OSINT and social media intelligence.	LEAs, Govt. & Intel. agencies	**Also see SS8 in "Lawful Intercept Solutions," "Packet Monitoring" and "Malware."**
Trovicor	Munich, Germany.	**Intelligence Platform.**	**Intelligence Platform:** Surveillance system includes analytics, visualization and semantics analysis.	Govt. & Intel. agencies.	**Also see Trovicor in "Lawful Intercept Solutions" "Mobile Location," "Malware" and "OSINT and Social Media."**
Ultra Electronics	Middlesex, UK.	**End-to-End Communications Analysis System (ECAS).**	**ECAS:** Real time predictive analytics.Folds in data from Ultra DPI, OSINT, voice biometrics, RF monitoring and GEOINT solutions. Analyzes and scores data to ID target, threat level. Recommends response.	Govt. & Intel. agencies, Military.	**Also see Ultra Electronics in "Packet Monitoring," "Biometric ID" and "Military."**

Ultra Electronics (continued)		**Signal Analytics and Geospatial Exploitation (SAGE).** **Miderva.**	**SAGE:** Pinpoints target location through RF Signal Analysis + highly-directional antennas, triangulation, GPS, Angle-of-Arrival (AOA), Time Difference of Arrival (TDOA) and Received Signal Strength (RSS) + GEOINT and satellite imagery. Collates target comms date from Ultra's DPI solution, ARIES. **Miderva:** Unified recording and storage platform for all types of data: audio, video and screens from IP, mobile and wireline networks		
Verint	Melville, NY, USA.	**Fusion Intelligence Center.**	**Fusion Intelligence Center:** Big Data Analytics with visualization. Uses Verint Skylock for target location. Correlates feeds from Web content, police field reports, criminal records, vehicle info, personal and CDRs.	Govt. & Intel. agencies.	**Also see Verint in "Lawful Intercept Solutions," "Mobile Location," "Ethical Malware," "Military," "OSINT and Social Media" and "Malware."**

Chapter 8: Forensics Solutions

Few cases involving forensics have generated greater attention or controversy than the U.S. Federal Bureau of Investigation (FBI) effort to examine an iPhone owned by one of the San Bernardino terrorists. This story was headline news from late 2015 well into 2016. When Apple refused to assist the investigation and create a “backdoor” into the device, the FBI responded with a court order under a 227-year-old law – the “All Writs Act” – ordering them to do so. Apple refused again and the case was set to go to court in March 2016.

One day before the trial, the FBI announced that it had been able to hack into the iPhone with assistance from an ISS vendor. Rumors circulated about possible involvement by Israel’s **Cellebrite**, or **Mandiant** of the U.S. in successfully exploiting a flaw in Apple’s software.
The vendor’s name was never released, though FBI Director James Comey revealed the price tag for this one hack: US $1.3 million. Other sources contend that the work was done primarily by the FBI, using a brute force attack similar to what **SciEngines** does.

Welcome to the new world of electronic forensics, where ISS, cryptanalysis and traditional evidence gathering techniques often merge.

Criminal forensics is often considered an “after the fact” exercise separate from ISS, which is viewed as more preemptive. In practice, the disciplines overlap.

Vendors such as **Radio Tactic**s and **Savvius** provide “wireless forensics” over the network in real time. **Roke Manor Research** of the UK helps investigators pursue evidence on suspects “in the cloud” well before any arrest is made. At the same time, vendors like **Cellebrite** devote resources to both fields: classic and real time forensics.

Varying challenges to forensics have arisen on both the legal and technical fronts. A 2014 ruling by the U.S. Supreme court determined that data held in mobile devices falls under the protection of the Fourth Amendment of the Constitution, and law enforcement agencies now must obtain a court order to access any data on the devices. However, as demonstrated in the Apple/FBI case, law enforcement can typically meet that requirement through a variety of legal avenues – or simply find a way to hack suspect electronic equipment seized in an arrest. LEAs in other nations go through similar legal drills and when all else fails can apply their own technical measures to obtain evidence.

Table 8. Forensics Solutions

Company	Location	Solution	Function	Market	Of Note
Cellebrite	Petah Tikva, Israel.	**Cellebrite Touch.**	**Cellebrite Touch:** Small standalone touch-screen unit performs physical, file system, and logical extractions of all data and passwords from a device, including deleted data**.**	CSPs, LEAs,Govt. & Intel. agencies, Military.	Used by 50 wireless CSPs worldwide.
		UFED4PC.	**UFED4PC**: Full mobile extraction capabilities in software for any PC.		
		UFEDTK.	**UFEDTK**: For field operatives. Provides full extraction capabilities in ruggedized Panasonic laptops/tablets.		
		UFED InField Kiosk.	**UFED InField Kiosk:** Field version platform for real time mobile data extraction. Can be networked to share or access data. Captures screen shots. **Two systems available with all products:** **UFED Logical** (extracts mobile data). **UFED Ultimate** (extraction + analytics)		

Guidance	Pasadena, CA, USA.	**EnCase Forensic.**	**EnCase Forensic:** Rack-mounted or laptop forensics system for evidence gathering. Acquires and analyzes data from multiple devices, both fixed & mobile.	LEAs, Govt. & Intel. agencies.	
MSAB	Stockholm, Sweden.	**XRY.** **XRY Field Version.**	**XRY**:. Mobile forensics. Attacks at three points of boot-up: (1) chipsets; (2) bootloaders with generic features that can be cracked by inserting code; and (3) operating systems with generic profiles. Penetrates over 600 apps. Add-on modules include analytics, visualization and mapping. **XRY Field Version**: XRY system in rugged case.	LEAs, Govt. & Intel. agencies, Military.	**Formerly Micro Systemation – re-branded as MSAB in 2016.**
NEC	Tokyo, Japan. Worldwide offices in Asia, the Americas, Europe, Africa and the Middle East.	**NeoFace Reveal.**	**NeoFace Reveal:** Forensics solution that matches faces captured by NeoFace Watch with criminal or terrorist mugshots.	LEAs, Govt. & Intel. agencies, commercial enterprises.	**Also see NEC in "Biometrics."**

Ockham Solutions	Paris, France.	**Mercure3.**	**Mercure3:** Mobile forensics with advanced analytics. Collects all data in the target device & maps against Intel. from financial and criminal records, GEOINT, HUMINT, OSINT or SIGINT to determine target networks. Works with structured & unstructured data. Custom-designed input engine handles any data format. Sophisticated but user friendly.	LEAs, Govt. & Intel. agencies.	
Oxygen Software	Moscow, Russia. Alexandria, VA, USA.	**Oxygen Forensic Analyst.** **Oxygen Forensic Detective.**	**Oxygen Forensic Analyst:** Collects data over 15,000 mobile devices and 340 , capture apps. Provides analytics and visualization of all content and metadata and exports data to common file formats. **Oxygen Forensic Detective:** Same functionality as Analyst + finds device passwords, disables	LEAs, Govt. & Intel. agencies.	**Also see Oxygen Software in “OSINT and Social Media.”**

Oxygen Software (continued)		**Oxygen Forensic Cloud Extractor.**	screen lock on Android devices, extracts data from clouds, imports and analyzes data and provides visualization of target's common routes and mobile location. **Oxygen Forensic Cloud Extractor:** Extracts data from 25 cloud services including Google, Apple iCloud, Microsoft Live Dropbox, Box and BitCasa.		
Paladion	Mumbai & Bangalore, India.	**Computer & Cellphone Forensics.**	**Computer & Cellphone Forensics:** System actively deciphers PC and mobile device encryption for evidence gathering.	LEAs, Govt. & Intel. agencies.	**Also see Paladion in "Lawful Intercept Solutions," "Mobile Location" "Advanced Analytics" and "Malware."**
Paraben Mobile Forensics	Ashburn, VA, USA.	**DS 7.**	**DS 7.6:** "Device Seizure" of "logical" evidence extraction from any operating system including Apple iOS 10 and Android Marshmellow OS. Limits on combined logical/physical extraction for Android and Apple.		"Logical extraction" duplicates data on the mobile device itself. "Physical extraction" duplicates all data including deleted files held in flash drives.

Paraben Mobile Forensics (continued)		**Mobile Field Kit.** **Stronghold Faraday Protection.**	**Mobile Field Kit:** Portable DS 7.6. **Stronghold Faraday Protection:** Prevents interference with, contamination or deletion of evidence on a captured mobile device.		
Phonexia	Brno, Czech Republic.	**Phonexia Voice Inspector.**	**Phonexia Voice Inspector:** Forensics software solution based on voice biometrics. Creates biometric voice prints of recording of unknown targets. Maps against biometric database.	LEAs, Govt. & Intel. agencies.	**Also see Phonexia in "Biometrics."**
Radio Tactics	Southampton UK.	**Aceso Kiosk.** **Aceso Field.** **Handset Access Card (HAC).**	**Aceso Kiosk v 7.4:** Desktop data extraction from mobile phones, GPS devices, SIM and media cards for forensics. Includes iOS 10. **Aceso Field:** Portable version of Aceso Kiosk. **Handset Access Card:** (HAC): mobile device forensics via SIM card replication.	LEAs, Govt. & Intel. agencies, Military.	**Also see Radio Tactics in "Military."**

Radio Tactics (continued)		**Integrated Camera Capability.** **POLUS.**	**Integrated Camera Capability:** For Aceso Kiosk – high resolution images of captured mobile device IMEI and SIM numbers. **POLUS:** Automated data retention of forensics evidence in encrypted “evidential container.” Can be used with 3rd party Advanced Analytics.		
Roke Manor Research (a Chemring Group company)	Romsey, Hampshire UK.	**Roke Forensics.** **Base Station Survey.**	**Roke Forensics:** Mobile, cloud and OSINT forensics. Penetrates target’s mobile device to access content, websites visited, and recent activities. Works on Android devices as an app, and on OSINT and the cloud. **Base Station Survey:** Smart phone app can pull all data from a mobile base station for analysis.	LEAs, Govt. & Intel. agencies.	**Also see Roke Manor Research in “Lawful Intercept Devices,” “Advanced Analytics,” and “Military.”**
Savvius	Walnut Creek, CA, USA.	**Omnipeek Distributed Analysis.**	**Omnipeek Distributed Analysis:** Wireless forensics with real time	CSPs, LEAs.	**Also see Savvius in “Lawful Intercept Solutions” and “Packet**

Savvius (continued)			analytics. Captures and analyzes all WiFi or other targeted mobile traffic including email, IM and VoIP.		**Monitoring.”**
STC	St. Petersburg, Russia.	**Ikar Lab.**	**Ikar Lab:** The full package of STC audio forensics solutions including **SIS II** software, **Sound Cleaner II** noise reduction, **EdiTracker** audio authenticity analytics, **Caesar** audio transcription, **STC-H246** audio hardware, **ANF II** noise filtering, **VoiceGrid Local** biometrics database, and **Voice Sampling** workstation.	LEAs and Govt. Intel. agencies.	STC’s core product. 360 deployments worldwide. **Also see STC in “Biometrics.”**
		SIS II.	**SIS II:** Core software platform for speech signal analysis, visualization, segmentation and text transcript.		
		Sound Cleaner II.	**Sound Cleaner II:** Noise filtering and sound enhancement.		
		ANF II.	**ANF II:** Dedicated noise filtering hardware.		

Chapter 9: OSINT and Social Media Monitoring

OSINT has evolved to become the new SIGINT. By pointing directly to the individuals behind acts of crime and terrorism, social media monitoring, the Deep Web and other forms of OSINT have earned the respect of law enforcement, government and military intelligence personnel.

Social media is now an accepted "beat" for law officers who can quickly see the most likely times and places for crimes that are about to occur or recur, and for military users tracking opponents via:

- **Troop movements**. A combatant posting on Twitter from an occupied village one day, then from a city hundreds of miles away just later days later may point to troop movements.

- **Armament Ramp-ups**. Images of mobile-missiles and tank brigades posted to social media can provide a clear indication of opposing forces' strengths and readiness for combat.

- **Geolocation**. Tools by companies such as Snaptrend can precisely position every Facebook or Twitter post to a specific site. Combined with satellite image analysis, other tools can plot posts from any social media site on a high-resolution map.

Police dispatchers now can enter an individual's name into software provided by **Tyler Technologies** that tells whether that person has previously contacted police and why. **PredPol** (short for "predictive policing") sells software that scans three data points — past type, place and time of crime — uses a priority algorithm to help police predict future crimes. Other companies provide mobile apps that scan millions of records to create a unique profile of any individual designated by the analyst.

As the "new kid on the block" in ISS, social media monitoring has attracted not only new players but also established vendors such as **FinFisher** and **Elbit Systems CYBERBIT**, which have added the capability to their repertoire of services – and made the market intensely competitive. Competition has also driven some early entrants from the marketplace. Among the best known, **BrightPlanet** this year discontinued its Blue Jay Twitter monitoring service for LEAs, citing "higher costs and low customer volume." The company remains active in Deep Web monitoring.

For all its popularity, critics make a fair point in contending that OSINT is not fool-proof. For example, it is a given that nation states and operatives leverage social media for propaganda and counter-intelligence. ISIS commonly posts images of supposed victories from past or unrelated conflicts, including some that pre-date the Islamic State. As 2016 closed, some analysts have cautioned that "fake news" is common on the Deep Web.

Table 9. OSINT and Social Media Monitoring

Company	Location	Solution	Function	Market	Of Note
BrightPlanet	Sioux Falls, SD, USA.	**Deep Web Monitor.**	**Deep Web Monitor:** harvests tweets, blogs, RSS feeds, surface sites and Deep Web sites.	LEAs, Govt. & Intel. agencies, Military.	BrightPlanet abandoned its Blue Jay Twitter monitoring service (2016), which came with a unique feature: malware that took over the target device’s camera and coordinated visual surveillance with street videocams. **Also see BrightPlanet in “Advanced Analytics.”**
CrowdControl	Birmingham, UK.	**CrowdControlHQ.** **BuzzMonitor.**	**CrowdControlHQ:** Tracks keywords in Google+ public profiles, Twitter, Facebook, Google news and blog conversations to monitor “social media risk.” **BuzzMonitor:** Twitter user geolocation by postal code.	LEAs.	
Decisions Group	Taipei, Taiwan.	**E-Detective.**	**E-Detective:** DPI with rules engine set to capture Twitter & Facebook user ID, profile and location.	LEAs.	**Also see Decisions Group in “Packet Monitoring.**”
DigitalStakeOut	Suwanee, GA, USA.	**Digital StakeOut.**	**Digital Stakeout:** Web-based threat intelligence from 20+ social media firms, Deep Web and Dark Web. Collects and filters relevant intelligence by geo-fence,	LEAs, Govt. & Intel. agencies.	Partners with LexisNexis.

DigitalStakeOut (continued)			keyword, phrase, metadata or complex rule. Sentiment algorithms assess threats, security algorithms for vulnerabilities. Statistical signal processing algorithms alert re: dangerous anomalies. Provides geo-spatial, cluster, social graph and cloud visualizations.		
FinFisher	Munich, Germany.	**FinFisher Crawler.**	**FinFisher Crawler:** Uses FinFisher FinSpy to infect and monitor social networks.	LEAs, Govt. & Intel. agencies.	**Also see FinFisher in “Malware.”**
Geofeedia	Chicago, IL, USA.	**GeoSearch.** **GeoStreamer.** **Monitoring & Analytics.**	**GeoSearch:** User can create a perimeter around any location and monitor social posts media from Twitter, Facebook, Instagram, YouTube, Flickr, Picasa and Viddy. **GeoStreamer:** Monitor multiple feeds generated from one location or targeted area simultaneously. **Monitoring & Analytics:** Applies predictive analytics to social media for breaking trends. Integrates with e-discovery platforms including Concordance and CaseMap to combine location data with case-related data.	Primarily commercial use, but relevant to LEAs, Govt. & Intel. agencies.	

Group 2000	Almelo, Netherlands. Oslo, Norway. Freienbach, Switzerland. Wilmington, DE, USA.	**LIMA Social Media Insights.**	**LIMA Social Media Insights:** Discovery, collection and analysis of social media and other OSINT, including linguistic analysis, to reveal target identity, networks, trends and threats.	LEAs, Govt. & Intel. agencies.	**Also see Group 2000 in "Lawful Intercept Solutions," "Mobile Location" and "Biometric ID."**
iPS	Aprilia, Italy.	**G- SNAKE.** **GENESI-DATA.**	**G-SNAKE:** Intrusion into social networks. **GENISI-DATA:** Provides portal to target's Facebook account to profile & build relationship network for analysis.	Govt. & Intel. agencies.	**Also see iPS in "Lawful Intercept Solutions," "Mobile Location," "Advanced Analytics," "Malware" and "Biometric ID."**
Kapow	Irvine, CA, USA.	**Kapow Extraction Browser.**	**Kapow Extraction Browser:** Real time Deep Web harvesting views and sorts dynamic changes in a web page. Provides analytics for context and visualization.	LEAs, Govt. & Intel. agencies.	**Also see Kofax Capture in "Advanced Analytics."**
Leidos	Reston, VA, USA.	**Digital Echo.**	**Digital Echo:** "Customizable virtual scalpel" for OSINT and social media. Targets and analyzes selected or broad content fields. Assesses regions and populations, content and sentiment analysis. Locates, maps and visualizes targets on social media and their connections.	Govt. & Intel. agencies.	**Also see Leidos in "Advanced Analytics."**

LexisNexis – a subsidiary of Reed-Elsevier	Dayton, OH, USA.	**Accurint Social Media Monitor.**	**Accurint Social Media Monitor:** Intercepts, monitors, locates targets and “controls social media”: Facebook, Twitter, Google+, others.	LEAs.	Powered by DigitalStakeout See Digital Stakeout and in “Military”)
NetBase	Mountain View, CA, USA.	**NetBase.**	**NetBase:** Delivers and visualizes real time social media data, showing key influencers Leverages Natural Language Processing (NLP) with text analytics and AI to understand context of social media posts and streams. Platform works in 42 languages and “decodes” colloquialisms, abbreviations and misspellings. Captures trends and individual conversations. Tracks target sentiment for any topic or trend, showing “share of voice” over time.. Enables Boolean (true or false) queries. Provides up to 27 months of historical data.	LEAs, ISPs, search engines, social media sites.	Re-sold by SAP NetBase claims that its platform processes posts nine-times faster and 50 to 70% more accurately than other tools.
Ntrepid	Herndon, VA, USA.	**Ion.** **Ion Sessions.**	**Ion:** Provides secret Deep Web dispersing Web search activities across thousands of anonymous IP addresses. **Ion Sessions:** For session-dependent queries, enables user-controlled IP persistence for Deep Web searches.	Govt. & Intel. agencies, LEAs.	Integrates with popular Web harvesting solutions including Kofax Kapow, Connotate and eGrabber. Ntrepid also produces “Anonymizer,” a VPN service for concealing user identity.

Ntrepid (continued)		**Tartan.** **Timestream.**	**Tartan:** Leverages user data information to determine key influencers and hidden links in social networks. Also reveals IDs behind aliases. **Timestream**: Organizes data into case evidence.		Ntrepid has held contract to provide “online personas” for U.S. Central Command since 2011.
Elbit Systems CYBERBIT	Ra’anana, Israel.	**WEBINT.** **Text Analysis.**	**WEBINT**: Deep Web tracking for OSINT. Can be integrated with other data for analysis. **Text Analysis**: searches for keywords and patterns that identify a target, and trigger alerts.	Govt. & Intel. agencies.	**Also see Elbit Systems CYBERBIT In “Advanced Analytics,” “Lawful Intercept Solutions,” “Mobile Location,” “Biometric ID,” “Malware,” and “Military.”**
NORSI-TRANS	Moscow, Russia.	**Yakhont-R.**	**Yakhont-R:** Collects and stores details on Internet and social media users’ personal ID, user name, IP address registration with service, and records of reception, transmission and processing of data, written text, images or sounds.	LEAs, Govt. & Intel. agencies.	**Also see NORSI-TRANS in “Lawful Intercept Solutions,” Packet Monitoring,” “Mobile Location” and “Advanced Analytics.”**
PredPol	Santa Cruz, CA, USA	**PredPol.**	**PredPol:** Predictive policing. Combines Big Data analytics of heuristic crime data with real time social media analysis to create patterns that determine next likely crime scene and perpetrators.	LEAs	Reported to reduce crimes 15% - 30%.Some controversy over validity of testimonials – LA Police Dept. denied PredPol claim that it had used the product.

RCS Labs	Milan, Italy.	**MITO^3 Social Network Analysis.**	**MITO^3 Social Network Analysis:** Analytics tools applied to Twitter Facebook to identify users, relationships, sentiments and threats.	LEAs, Govt. & Intel. Agencies.	**Also see RCS Labs in “Lawful Intercept Solutions,” “Mobile Location,” “Malware,” and “Advanced Analytics.”**
Recorded Future	Boston, MA and Arlington, VA, USA. London, UK. Göteborg, Sweden.	**Temporal Analytics Engine (TAE).**	**Temporal Analytics Engine (TAE):** Applies real time predictive analytics to Deep Web and other OSINT to forecast trends and alert to imminent threats. TAE produces stream-generated analysis of events in the real world -- extracting the targeted entity or entities, the attacker, where and when they will strike.Unlike competing products reliant on link analysis, TAE uses “implicit” analysis revealing relationships between events, timing, location, attackers, attackers’ urls & sentiments and who attacked.	Govt. & Intel. agencies.	Backed by CIA In-Q-Tel venture capital and private financing. Co-founder and and Chief Scientist Staffan Truvé also serves as CEO of the Swedish Institute of Computer Science (SICS), and is co-founder of Carlstedt Research and Technology (CRT).
SunTech – Verint Group	Florianópolis, Brazil.	**FOCAL-INFO.**	**FOCAL-INFO:** Deep Web harvesting for OSINT.	LEAs, Govt. & Intel. agencies.	**Also see Suntech in “Lawful Intercept Solutions” and “Mobile Location.”**
Tencent	Shanghai, China.	**QQ Circle.**	**QQ Circle:** Analytics target social media relationships.	Govt. of China.	China’s largest Internet portal.

Trackur	Raleigh, NC, USA.	**Trackur.** **Senfluence.**	**Trackur:** Provides social media tracking and sentiment analysis. **Senfluence:** Monitors news, social media, videos & images. Extracts sentiment of any url and understands its influence/footprint on the Web. Extracts relevant content.	Primarily commercial use, but relevant to LEAs, Govt. & Intel. agencies.	
Trovicor	Munich, Germany.	**Intelligence Platform.**	**Intelligence Platform:** Surveillance system includes interception, trend tracking, analytics and visualization of social media integrated with other intelligence collected.	Govt. & Intel. agencies.	**Also see Trovicor in “Lawful Intercept Solutions” “Mobile Location,” “Malware” and “Advanced Analytics.”**
Verint	Melville, NY, USA.	**Web Alert.** **Web Intelligence Center.**	**Web Alert:** Pre-crime social media monitoring. Crawls all major sites plus emojis and blogs in 82 languages. Shows links between targets & affiliates and those with strongest connections. Some location capabilities. Customizable to specific geozones. “Time machine” recreates events to find suspects and possible witnesses. **Web Intelligence Center:** Collects analyzes content from Open Web, blogs, social media, news sites, hosting services, Deep Web and Dark Web.	LEAs.	**Also see Verint in “Lawful Intercept Solutions,” Mobile Location,” “Advanced Analytics,” “Military” and “Malware.”**

Chapter 10: Military Intelligence

Worldwide, military departments play a central role in intelligence. In the U.S., nine out of 17 member agencies of the Intelligence Community report to the Department of Defense: the National Security Agency, the Defense Intelligence Agency, the National Geospatial Intelligence Agency, the National Reconnaissance Office, and the separate intelligence divisions of all five military services.

The U.S. Intelligence Community has two primary areas of responsibility: the National Intelligence Program (NIP) and the Military Intelligence Program (MIP). Both report to the Office of the Director of National Intelligence (ODNI), which is charged with managing strategic military intelligence. Tactical intelligence, however, is the business of the respective military branches. Control and administration of MIP falls to the Under Secretary of Defense for Intelligence.

In the field, military services often have the final say. In the hunt for IEDs in Iraq, DCGS-A was known to pronounce bomb-laden roads as being “clean.” The U.S. Marines and Special Forces had enough, and replaced DCSG-A with Palantir, which proved its ability to pull together 10s of thousands of data points in real time, and provide life-saving solutions.

The same holds true in other nations. The largest contingent in the Israeli Armed Forces is the Central Collection Unit of the Intelligence Corps, also known as the Israeli SIGINT National Unit, or simply Unit 8200 – some 3,000 strong. Reporting up to Unit 8200 is Unit Hatzav, responsible for collection of OSINT. Israeli military intelligence and “commercial” ISS vendors are closely intertwined, both for business and as mutual spawning grounds of technical advances.

Germany provides yet another example of this symbiotic relationship. It is no accident that the German ISS firms – **FinFisher**, **Datakom**, **Dreamlabs**, **Elaman**, **Rohde & Schwarz**, **Trovico**r and others – are centered around Munich. Just down the road is the Bad Aibling Station (BAS), a former military base run by the NSA through 1994 and for years the third largest site of ECHELON, the global SIGINT network of “The Five Eyes” –- the U.S. UK, Canada, Australia and New Zealand – until turned over to German foreign intelligence in the early 2000s. Through 2014, Pullach, a suburb of Munich, was also the central location of the Bundesnachrichtendienstn (BND), the Foreign Intelligence Service of Germany.

Table 10. Military Intelligence

Company	Location	Solution	Function	Market	Of Note
AECOM	Los Angeles, CA.	**Intelligence and Language Support.**	**Intelligence and Language Support:** Translation and interpretation services + native-speaking linguists. Provides research, development, and testing capability in 153 less commonly taught languages. Provides analytics and COMINT/HUMINT support.	Military, Govt. & Intel. agencies.	Manages cyber security for U.S. DoD CyberCom global missions. Also a partner of malware company, The Hacking Team.
ATIS UHER	Bad Homberg, Germany	**Klarios RMS.**	**Klarios RMS:** RF signal monitoring. Provides direct control of connected or integrated radio receiver and antenna systems via a special interface. Focuses on targeted channels, filtering out irrelevant signals. Results can be fed into Klarios IDA for analytics and visualization.	CSPs, Govt. & Intel. agencies, LEAs, Military.	**Also see ATIS UHER in "Lawful Intercept Solutions," "Mobile Location" and "Advanced Analytics."**
Cintel	Peachtree City, GA, USA.	**Acuity.**	**Acuity:** Web-based software platform serves as field sensor intelligence collection solution. Aggregates covert/overt CCTV feeds: logs data, captures still images, integrates location data; social network analysis; plus metadata search. Provides interactive mapping for GEOINT.	Military, LEAs, Govt. & Intel. agencies.	
CRFS	Cambridge, UK.	**RFeye Node.**	**RFeye Node:** Four models of frequency monitoring nodes delivering between 20 Mhz to 100 Mhz of bandwidth. Provides real time monitoring for suspicious radio activity. Uses GPS to find & time-stamp transmissions. Recent advance includes expansion of frequency range 18GHz.	Military, Govt. & Intel. agencies, LEAs.	

CRFS (cont.)		**RFeye Monitor.**	**RFeye Monitor:** Network of distributed RFeye nodes for 24X7 collecting and managing spectrum data.		
		RFeye Roofbox.	**RFeye Roofbox:** Vehicle-based spectrum surveillance + GUI mapping & analytics devices.		
		RFeye Stormcase.	**RFeye Stormcase:** Portable intelligent RF receiver stand-alone operation or integrated with CRFS wideband spectrum monitoring network.		
		RFeye Backpack.	**RFeye Backpack:** Wearable RFeye RF monitoring with built-in GPS for urban or field operations.		
		Array 50 and 300.	**Array 50 and 300:** Suite of 2 fixed or vehicle mounted antenna/receiver for real time RF monitoring z. Intercepts, analyzes, classifies and geolocates targets. Measures “Angle of Arrival” and augmented “Time Difference of Arrival” and “Power of Arrival” of RF signals to pinpoint target location.		
		DRFM Platform.	**DRFM Platform:** Digital Radio Frequency Memory combines distributed RFeye nodes with portable monitoring center to monitor wide area. Data acceleration via Altera or Xilinkc field programmable gate arrays (FPGAs) for real time data feed with zero packet loss.		
		Site.	**Site:** Desktop app for monitoring wide area RF monitoring via RFeye Nodes.		

CRYPTON-M	Kiev, Ukraine.	**Terra-Pro.**	**Terra-Pro:** Digital Network Monitoring Center for GSM and VSAT satellite interception. Extracts, records, retains and analyzes signal type and content including documents. Determines mobile location via SS7.	Military, Intel. agencies.	**Also see CRYPTON-M in "Lawful Intercept Solutions" and "Mobile Location."**
DELTA SPE	Kiev, Ukraine.	**DELTA SPE.**	**DELTA SPE:** Interception of satellite packet data services (Internet, VoIP, FoIP). Tactical WiFi interception.	Military, Govt. & Intel. agencies.	
Digital Stakeout	Suwanee, GA, USA.	**Digital Stakeout.**	**Digital Stakeout:** People Search (250 Million+ Profiles): Archive Search (Billion+ Geo Enabled Posts); Social Tag, Track, & Location (STTL).Profile & Geo-Location Analytics.	Military, Govt. & Intel. agencies.	Partners with LexisNexis. **Also see "Digital Stakeout" in "OSINT and Social Media."**
Elbit Systems CYBERBIT	Ra'anana, Israel.	**NA.**	**SATCOM**: Partners with Imagesat Intl. to provide persistent wide area IMINT and GEOINT via low earth orbit satellite. Can be integrated with CYBERBIT's other capabilities in COMINT, HUMINT, SIGINT and OSINT including social media -- plus findings from the PSS malware.	Military, Govt. & Intel. agencies.	**Also see Elbit Systems CYBERBIT in "Advanced Analytics," "Lawful Intercept Solutions," "Mobile Location," "Biometric ID," "OSINT and Social Media," and "Malware."**
ELTA Systems, a division of IAI (Israeli Aerospace Industry)	Ben Gurion Intl Airport, Israel.	**ELI-6063.**	**ELI-6063:** Integrated mobile ground-based SIGINT,COMINT, ELINT and EW (electronic warfare) system. Detects, monitors, analyzes, locates, records and jams enemy radars and communications.Truck-based platform integrates with multiple fixed COMINT/DF, ESM (radar intercept), ECM (radar	Military, Govt. & Intel. agencies.	ELTA Systems is a subsidiary of Israel Aerospace Industries. **Also see ELTA Systems in "Mobile Location."**

ELTA Systems (cont.)		**ELK-7066.**	jamming) and radio-relay jamming stations. **ELK-7066:** Airborne passive off-the-air GSM interception system. Filters target calls by identity (IMSI, TMSI, IMEI, MSISDN), area of activity, calling/called party and location. Intercepts and retains call & IP metadata.		
Gita Technologies	Tel Aviv, Israel.	**Horizon.**	**Horizon:** Tactical interception of Iridium, Thuraya, and the Inmarsat Isatphone. Can intercept full voice/data content in the clear plus IMSI/TMSI/EMRI numbers, social media and web browsing and target location. Captures uplink to a satellite and line-of-sight connection to a target's mobile device. Hack-in techniques: spoofing to exploitation of GPS vulnerability and scanning. Also does man-in-the-middle attacks on SATCOM signals.	Military. Govt. & Intel. agencies.	
Keysight (formerly Agilent)	Santa Clara, CA, USA.	**N9041B UXA Signal Analyzer, Multi-touch, 3Hz to 100GHz.**	**N9041B UXA:** New top of the line signal analyzer characterizes elusive millimeter wave signals: 5G, 802.11, satellite and radar. Makes continuous sweeps and captures low-level spurious signals. Simplifies analysis of new or emerging bandwidth signals.	Military, Govt. & Intel. agencies.	In 2016, Keysight announced its own 5G "blind mobile location" solution, in competition with Medav. Keysight offers 54 signal analyzers that span needs for real time, desktop and hand-held RF signal signal interception and analysis.

Medav GmbH (Saab)	Uttenreuth, Germany.	**Medav Radio Monitoring and Surveillance.** **Ultra Wideband MIMO Real Time Channel Sounder.** **Intelligence Fusion.**	**Medav Radio Monitoring and Surveillance:** RF monitoring, direction finding & location. **Ultra Wideband MIMO Real Time Channel Sounder**: directional resolution. **Intelligence Fusion:** Big Data analytics for military SIGINT applications.	Military, Govt. & Intel. agencies.	Acquired by defense contractor Saab AB (Stockholm, Sweden), Oct. 2012. Operates as Medav. **Also see Medav in “Mobile Location.”**
Palantir	Palo Alto, CA, USA.	**Gotham.**	**Gotham:** Visualization. Integrates multiple databases to provide detailed real time profile of target, trends & potential outcomes. Tags and unifies structured & unstructured data: financial records & transactions, historic & recent travel, SIGINT, COMINT, human networks, DNA samples, biometric voiceprints, video surveillance, records of military & terrorist actions. Visualization reveals off-network target contacts.	Military, Govt. & Intel. agencies.	**Also see Palantir in “Advanced Analytics.”**
Panoptech	Hampshire, UK.	**Clarity.** **Convergent Intelligence Platform.**	**Clarity:** Situational awareness tool provides integrated overview of surveillance. **Convergent Intelligence Platform:** Fast Action Command Tasking Software (FACTS) platform as command and control element controls logging and analysis. Integrates with TransVisual Media Convergent Intelligence Platform (TVM-CIP). Tracks GPS inputs of mobile vehicle airwave radios in real time. Integrates with aerial photography and manages overt/covert CCTV surveillance. Sends alerts to target cameras.	Military, Govt. & Intel. agencies.	

PLATH Group	Hamburg, Germany.	**ACOS.**	**ACOS** (Automatic COMINT System)**.** Uses machine learning to automate the bulk of RF frequency surveillance, freeing operators to focus on suspicious traffic.	Military, Govt. & Intel. agencies.	**Also see PLATH under Nexa Technologies in "Packet Monitoring"**
		ICAS.	**ICAS** (Intelligence Control and Analysis System)**:** Intercepts and analyzes RF signals, serving as command and control center.		
		JDS.	**JDS** (Jamming and Deceiving System)**:**. Jams HF/VHF/UHF RF and can adapt to emulate the opponent's frequency to intercept and record, or reproduce the signals and act as the sender.		
		MACOS.	**MACOS:** Passive sensor for interception of GSM, hand-held radio and SATCOM phones. Primary use is coastal patrols where smaller opponent vessels do not track on radar.		
		NALOS.	**NALOS** (Narrowband Location System)**:** utomated COMINT system for locating standard and "low probability of intercept" (LPI) signals in the HF domain. Uses spectral data analysis of RF signals vs. conventional direction finding.		
		TRACE.	**TRACE:** "Mobile System for Electromagnetic Spectrum Intelligence." Modular platform scales from use for monitoring conventional mobile networks to RF.		
Providence Group	Hereford, UK and Haarlem, Netherlands	**NA**	**Procurement experts:** Choose best-in-class solutions for: Covert Audio and Video; Tag, Track and Locate; Long Range Video; Tactical Intercept Systems; Tactical Cyber Solutions; Store & Forward	Military, LEAs, Counter-Terrorism, Border Patrol.	Emphasis on solutions customized per need and hands-on training.

Providence Group (cont.)			Audio/Video Solutions; Covert Method of Entry (CMOE) Solutions; Alarm Defeat; Data Forensics; Infrared and Night Vision Cameras; RF Jamming; Technical Surveillance Counter Measures (TSCM) – "bug sweeping"; and, Tactical and Covert Radio Systems.		
Radio Tactics	Southhamp-ton, UK.	**ATHENA.**	**ATHENA:** Portable system for GPS location, interception, content & real time social media interception. Matches mission data to database for matches. Integrates with facial and finger print biometrics. Can intercept SIM Cards, GPS, SATCOM and "gray market" phones.	Military, LEAs, Govt. & Intel. agencies.	**Also see Radio Tactics in "Forensics"**
Raytheon	Waltham, MA	**Blackbird Gotham TTL.**	**Blackbird Gotham TTL:** Tracking, tagging and locating services (TTL) developed by Blackbird Accesses targets on mobile or SATCOM. Provides GPS and GSM mobile location.	Military.	Blackbird acquired by Raytheon (2014). **Also see Raytheon in "Advanced Analytics."**
Rheinmettal Defence	Dusseldorf, Germany.	**Ares.** **Artemis.**	**Ares:** For C/L band Thuraya satellite interception. Acquires, down-converts, demodulates, decrypts and decodes SATCOM signals. Analyzes the intercept for content, target position and target relation. Monitors 34 channels in either C or L band, and analyzes up to 68 channels simultaneously. Use of Digital Signal Processors and FPGA hardware accelerators brings performance to wire speed in a compact unit. **Artemis:** Same features and functions as Ares, but for L/L Band Thuraya.	Military.	

Roke Manor Research	Romsey, Hampshire UK.	**MILOR.** **RESOLVE.** **LOCATE.**	**MILOR:** Miniature eLORAN receiver penetrates any obstacle -- buildings, foliage, to find and maintain contact with the target's position. **RESOLVE:** compact RF signal interception for Military field use. **LOCATE:** Roke Electronic Warfare Manpack - portable version of RESOLVE.	Military, Govt. & Intel. agencies.	**Also see Roke in "Lawful Intercept Solutions," "Advanced Analytics" and Forensics."**
Shoghi Communi-cations	Himachal Pradesh, India.	**SCL-3412.**	**SCL-3412:** C, Ku, X and Ka-Band Satellite Monitoring System which can intercept International/national telecom carriers, GSM A and Abis links and IP Carriers over satellite. Intercepts content including Voice, Fax, SMS, EmailBrowsed Webpages, Chat Sessions and attachments. IDs originating point country and destination point country, outgoing/incoming number and Cell ID, IMSI, TMSI, IMEI numbers.	Military.	**Also see Shoghi in "Lawful Intercept Solutions" and "Mobile Location."**
Stratign	Dubai, United Arab Emirates.	**SATCOM Interception.**	**SATCOM Interception:** Separate systems for Thuraya, Iridium and ISAT.	Military.	**Also see Stratign in "Mobile Location" and "Malware."**
Thales	Neuilly-sur-Seine, France.	**PAC-ELSE.**	**PAC-ELSE:** Tactical RF signal analysis.	Military.	**Also see Thales in "Lawful Intercept Solutions" and "Packet Monitoring"**

Ultra Electronic	Middlesex, UK.	**UltraEagle.**	**UltraEagle:** Software defined radio interception to capture, record and analyze enemy radar transmissions.	Military.	**Also see Ultra Electronics in "Advanced Analytics," "Packet Monitoring" and "Biometric ID."**
VASTech	Stellenbosch, South Africa.	**VASTech Zebra.**	**VASTech Zebra:** "Massive passive" monitoring system for voice, SMS and fax. Interfaces with S-1, Gitabit Ethernet and 10GB Ethernet. Provides target location, content and metadata intercepts. Also performs optical character recognition of text and images, text search and speaker/gender ID.	Military, Govt. & Intel. agencies, LEAs.	
		VASTech Badger.	**VASTech Badger:** For monitoring broadband IP networks. Captures traffic including email, VoIP and multimedia messages on multiple 10GB networks.		
		VASTech Satellite Signal Analyzer.	**VASTech Satellite Signal Analyzer:** Automatic analysis of satellite signals per the appropriate terminal configuration – modem of DCME – depending on the SATCOM operator. Decodes protocols and extracts content.		
		Fiber Signal Analyzer.	**Fiber Signal Analyzer:** Classifies and records signals on multi-GB Ethernet networks. Decodes TDM and IP signals.		
Verint	Melville, NY, USA.	**ENGAGE G12.**	**ENGAGE G12:** Locates target via homing device, extracts target's GPS coordinates; can edit and re-route inbound and outbound calls/texts. Able to take over device microphone.	Military, Govt. & Intel. agencies.	**Also see Verint in "Advanced Analytics," "OSINT and Social Media," "Mobile Location,"**

Verint (cont.)		**ENGAGE P12.**	**ENGAGE P12:** Collects mass GSM intel over wide area. Analysis tools ID target by location, speech, link analysis, text matching. Intercepts voice and text calls. Decrypts A5/1 and A5/2 encryption with embedded decipher. Selectively downgrades UMTS traffic to GSM. Allows multiple users. Undetectable to target.		**“Lawful Intercept Solutions” and “Malware.”**
		ENGAGE S12.	**ENGAGE S12:** SATCOM interception.		
		SKYLOCK.	**SKYLOCK:** Global cellular location remotely locates GSM & UMTS targets to nearest cell tower in any locaton.		
		ENGAGE WiFi.	**ENGAGE WiFi:** WiFi interception & tampering.		
		ENGAGE TCC.	**ENGAGE TCC:** locate all targets on geo map. Custom solutions or out of the box.		
		VERINT TACTICAL.	**VERINT TACTICAL:** real time mobile location and satellite tracking for special operations.		

Glossary of ISS Terminology

3GPP – 3rd Generation Partnership Project, a group that unites the standards for wireless and radio communications across other standards-setting bodies including ATIS and ESPI (See **ATIS** and **ESPI** below). 3GPP, ATIS and ESPI are all involved in setting standards for electronic surveillance technologies.

ADSL – Asymmetric DSL, the most common form of DSL. Asymmetric because download speed is faster than upload speed.

Active Lawful Intercept – Electronic surveillance technology solutions that reside in a communications service provider's network.

ASIC – Application-specific integrated circuit designed for a specific use.

ATIS – Alliance for Telecommunications Industry Solutions: an organization involved in creating and setting standards for lawful intercept under CALEA and other laws.

BSS/OSS – Automated Business Support Systems (billing) and Operational Support Systems (inventory management systems, order management, provisioning) used by communications service providers (CSPs) by telecom vendors. BSS produces call detail records and IP data records for billing and is also the basis of metadata collected during intercepts.

BVP – Biometric Voice Print: the means of identifying a suspect by voice regardless of language, device or gender. A BVP is every bit as unique as a fingerprint, and a vital new method of identifying and tracking suspects. Biometric technology can isolate a single suspect out of millions of conversations, even if the target switches languages in mid-conversation.

Buffering – Back-up storage of real time lawful intercept data to prevent data loss in the event of problems or disparities in communications connections.

CALEA – The Communications Assistance for Law Enforcement Act, enacted in 1994. CALEA outlines the rules of electronic surveillance for criminal cases, the compliance requirements for communications service providers to support lawful intercept, and strict privacy protections for the service provider's customers.

CALEA II – A concept that would extend the domain of CALEA to include all IP, broadband and social media.

CDMA – Code Division Multiple Access, a channel access method used in mobile and other radio services. Improves efficiency of fixed frequency allocation utilization by allowing customers to share a band of frequencies without interference. CDMA is the access method used in many phone standards, e.g., 3G.

CIS – Commonwealth of Independent States, a regional organization formed following dissolution of the USSR, primarily comprised former Soviet Republics.

COMINT – communications intelligence gathered from people, including voice, text and signaling channel interceptions.

Counter-Terrorism Act of China – China's first comprehensive anti-terrorism law, enacted on December 28, 2015. The law defines terrorism, outlines the responsibilities of service providers in assisting law enforcement and government agencies, and the powers of government to use surveillance to detect, monitor, prevent and capture the perpetrators of terrorism. The scope of the Act is broad, extending to all network communications. Following objections other nations and the technology industry, the Act does not require service providers to maintain all switching and routing equipment in-country. A draft provision requiring "back doors" into communications equipment and devices was dropped after similar objections were made.

CSP – Communications service provider, e.g., a phone company, Internet provider, cable or satellite dish company.

DCME – Old school voice compression equipment deployed at either end link of a "long distance" communication.

DHCP – Dynamic Host Configuration Protocol. DHCP is the standard networking protocol used on IP networks for dynamically distributing network configuration parameters like IP addresses for interfaces and services.

DNS – Domain Name System, for connecting any computing device to the Internet. DNS translates search terms to urls.

DNS Hijacking – A common form of cyberattack. The hacker manipulates and overrides a device's TCP/IP settings to redirect the device to a rogue website.

DOCSIS – The standard used by cable TV companies to deliver high-speed Internet services over hybrid fiber-coax networks.

DPI – Deep packet inspection, a form of computer network packet inspection to examine individual packets as they pass through an inspection point. In lawful intercept, DPI filters packets, identifies those to or from a targeted suspect and creates a mirror image which is then forwarded to law enforcement or intelligence – without the suspect's knowledge or any interruption of the signal.

DRIPA – The United Kingdom's Data Retention and Investigatory Act of 2014. Following BREXIT, the UK passed the Investigatory Powers Act to replace DRIPA, which expired December 31, 2016. Under DRIPA, communications service providers in Great Britain were required to retain customer's call and IP metadata records for a period of up to 12 months. In

July 2015 the British High Court reviewed and upheld a challenge to DRIPA, stating that portions of the Act violated privacy protections under the European Charter of Fundamental Rights. In October 2015 the Homeland Secretary filed an appeal. In December 2015 the Appeal Court referred the case to the Court of Justice of the European Union.

ECPA – The Electronic Communications Privacy Act, enacted in 1986. ECPA extended rules on telephone wiretapping to include electronic communications via computer networks, added privacy protections on stored communications through the Stored Communications Act, and added "pen/trap" provisions allowing LEAs to capture the originating and terminating numbers of communications events.

ELINT –The gathering of intelligence other than personal communications, such as radio signal analysis and target location with use of electronic sensors.

Email Privacy Act – Proposed legislation (3Q2014) before the U.S. House of Representatives, that would require law enforcement agencies to obtain a warrant to intercept a suspect's emails.

Ethernet – A computer networking standard originally developed in the 1970s for local area networks (LANs) and now commonly used in metro area networks (MANs) accessing wide area networks (WANs). Metro Ethernet is popular for its low cost versus SONET/SDH MANs.

Ethical Malware – The use of malware, either via a dongle or network connection, to penetrate and take control of a suspect's mobile or other communications device. Also called "legal malware" and "legal Trojan."

ETSI – European Telecommunications Standards Institute: creates standards for lawful intercept for members of the European Union. Cooperates with other standards-setting bodies such as ATIS, 3GPP and TIA to ensure international consistency of standards used in lawful intercept.

Femtocell – A small low power-mobile base station typically used by small businesses and in homes, and providing a range of up to 10 meters.

FPGA - Field-programmable gate array: an integrated circuit that can be configured or modified by the customer after manufacture. Used by Fiberblaze in its DPI forensics solution.

FISA – The Foreign Intelligence Surveillance Act (FISA) of 1978. Determines how U.S. agencies may collect foreign intelligence information on foreign nations and their agents, including U.S. citizens suspected of espionage.

FISC – Foreign Intelligence Surveillance Court. Oversees requests for warrants to conduct surveillance on suspected foreign agents in the U.S.

FTTX – A generic term for any broadband network using optical fiber to connect to the local loop in the last mile of a telecommunications network.

GCHQ – Government Communications Headquarters, the British intelligence and security group in charge of signals intelligence (SIGINT) from telecom and IP networks. GCHQ operates listening stations in the UK and abroad, works closely with the NSA and has used NSA-designed programs including PRISM. During World War II, GCHQ's predecessor was responsible for breaking the Enigma code used by Germany. Code-breaking and decryption are still key areas of interest and responsibility at GCHQ.

Geofencing – Use of the satellite-based Global Positioning System (GPS) or radio frequency identification (RFID) to determine the geographic zone of a target's position.

GEOINT – Geospatial Intelligence. Visual identification of natural features and man-made structures on the earth's surface, using SATCOM and/or aerial photography images, infrared and ultraviolet sensors plus analytics to determine the precise location of a target.

GPON – Gigabit passive optical fiber network. Uses gigabit speed point-to-multipoint FTTP (fiber to the premises) economically over a single optical fiber. Considered highly secure, GPON was developed in 2009 to meet the Secret Internet Protocol Router Network (SIPRNet) requirements of the U.S. Air Force and was adopted by the U.S. Army in 2013.

GPRS – General Packet Radio Service, an IP packet-based method of data communications on 2G and 3G mobile networks.

GSM – A standard developed by ETSI to describe protocols for second generation (2G) digital cellular networks used by mobile phones. It is the de facto global standard for mobile communications available in over 219 countries and territories. Newer mobile standards developed by ETSI include UMTS (Universal Mobile Telecommunications System, for 3G) and LTE (Long Term Evolution, for 4G), which are not part of the GSM standard.

IAP – Intercept Access Point. In an active lawful intercept solution, the IAP is an interface built into network hardware. A mediation device programs IAPs across the CSP's network to collect communications data and content specific to a target designated by a lawful intercept court order.

IMEI – International Mobile Station Identity, a unique number assigned to every mobile device on GSM, UMTS or LTE network. The IMEI is 15 digits and typically found behind the device's battery. IMEIs are also stored in a mobile operator's Equipment Identity Register (EIR) to validate the user's device to use the network.

IMSI – International Mobile Subscriber Identity is a second unique code, also 15 digits, that is stored in a 64-bit field on the SIM card in a mobile device and used as the primary identifier of the individual user of a GSM or UMTS network, and for validation in home location and visitor location registers kept by the mobile operator.

IMSI Catcher – A surveillance device that works in “active” mode to emulate a legitimate mobile base station, emits a slightly stronger signal than the actual network, and capture a device’s IMSI and IMEI numbers by it making authenticate with the fake base station. The IMSI catcher then performs a man-in-the-middle attack that intercepts the mobile voice and data communications of targets. The IMSI catcher determines location of the target by triangulating the signal links of his mobile device to local mobile base stations.

Investigatory Powers Act – UK law approved by Parliament on November 29, 2016 requires Internet service providers to retain “Internet Call Records,” codify legal right to conduct bulk metadata collection, and establish law enforcement’s right to deploy/require “equipment interference” – back doors in network and end user devices that break end-to-end encryption. The law was scheduled to go into effect in 2017, replacing DRIPA. But the future of the Investigatory Powers Act remains uncertain. On December 19, 2016, the European Court of Justice declared the new British law “illegal.”

IPFIX – Internet Protocol Flow Information Export Internet. A standard protocol defining how packet data captured via Flow Monitoring is formatted and sent to a collection device.

IP Flow Monitoring – Also known as NetFlow, a system for monitoring and collecting representative packet samples on high speed IP networks. NetFlow was developed by Cisco and is used or mimicked in Flow Monitoring products by Juniper, Flowman and others.

Iridium – A satellite constellation of 66 low-earth orbital satellites supporting voice and data services from any location on earth, with 11 satellites in each of six pole-to-pole orbits. Next generation Iridium satellites planned for launch from 2016 – 2017 will provide higher bandwidth for data, and possibly sensors and cameras.

ISP – Internet service provider.

LEA – Law enforcement agency.

LI – Lawful intercept, the modern term for “wiretap,” but expanded to include all other forms of communications that may be subject to court ordered surveillance under current laws.

LIDAR – Light Detection And Ranging, a technology that measures distance by illuminating an object with a laser beam. LIDAR is commonly used in facial biometrics, creating a unique map of the human face through thousands of measurements.

LTE – Long Term Evolution. Describes a third generation (3G) high-speed mobile network services with peak download rates up to 299.6 MBs and upload rates up to 75.4 MBs.

MAC Address – Media Access Control Address. A unique, typically 15-digit code that serves as the physical address and identifier of a computer or other device allowing transmission of packets from one device to another. A MAC address is typically stored in Read Only Memory (ROM) and is a common target of IMSI catchers for identifying and taking control of targeted mobile devices.

Mediation Device – An appliance that provides centralized management of an "active" electronic surveillance system such as those used under CALEA. The device configures network hardware to intercept targeted suspects' communications, collects, filters and formats the data, then forwards it to a designated law enforcement agency.

Metadata – Record of call data including originating and terminating numbers of a call, time of day and duration of call. Does *not* include call content.

MLAT – Mutual Legal Assistance Treaties: agreements between nations establishing cooperation between their law enforcement agencies on the use of lawful intercept to investigate suspects who operate across borders, or whose communications data is stored outside the boundaries of a nation.

Mobile Location Data – Data gleaned from mobile networks or directly from a mobile device that pinpoints the location of a targeted device. In certain instances, call detail records are used to indicate a suspect's historic location relative to the scene and time of a crime.

NDCAC – The National Domestic Communications Assistance Center, founded in 2012 and located in Fredericksburg, VA. NDCAC is an information and training resource that provides support to state and local LEAs on lawful intercept.

NetFlow – IP Flow Monitoring solution for routers introduced by Cisco in 1996. "Samples" packet flows on high-speed networks and singles out anomalies for further investigation. Often powered by field programmable gate arrays (PGFAs) to accelerate performance, IP Flow Monitoring may be used in conjunction with Deep Packet Inspection for full packet examination.

Network Packet Broker – A hardware-based packet monitoring solution that collects, aggregates and copies network traffic from switch SPAN ports or network TAPs.

OSI Stack or Model – The Operational Systems Interconnection stack is an abstract model for partitioning a communications network in seven layers, each supporting the layer "above" it. The seven layers of the OSI stack are: Physical, Data, Network, Transport, Session, Presentation and Application. Packet monitoring systems such as DPI monitor Layers 2 – 7.

OSINT – Open Source Intelligence. OSINT refers to any information that is openly available and in the clear: websites, social media, news sources, blogs, and Deep Web.

Passive Lawful Intercept – A form of lawful intercept that relies on a device called a “probe” that operates independent of a communications service provider network and that “sniffs” designated communications traffic upon activation.

Passive “Off the Air” Monitoring – Direct interception of RF signals from mobile and other radio networks. Passive Off-the-Air RF surveillance intercepts signals from transmitters without interfering with the network.

Pen Register – Lawful intercept of a suspect’s call signaling data; does not include content.

PNIJ – “Plateforme Nationale des Interceptions Judiciaires” is France’s planned, integrated platform of domestic surveillance. Conceived in 2010. Contracted to Thales. Still not operational.

Probe – A passive surveillance device deployed at the edge of the network and independent of network hardware.

PSTN – Public Switched Telephone Network: the conventional voice network.

RIPA – the UK’s Regulation of Investigative Powers Act 2000, authorizing and outlining the allowed technical/legal means for lawful intercept of mass telecom and IP communications. Subsequently amended in 2003, 2005, 2006 and 2010. A fifth proposed amended version of RIPA was introduced in Parliament in November 2015.

Safe Harbor – Under CALEA, a status of compliance reached when deploying a technology solution that meets the technical standards for lawful intercept.

SCA – The Stored Communications Act (Title II of ECPA).

SDH/SONET – Standard protocols for transporting multiple bit streams synchronously over fiber optic cable.

SIGINT – Signals Intelligence. SIGINT is the master category defining intelligence gathering of signals whether from human communications (COMINT) or electronic signals not directly used on communications (ELINT). Examples of COMINT include voice, signal and email communications. Examples of ELINT include radar and other signals that indicate types of communications channel and their location.

SS7 – Signaling System 7, a technology developed in the 1980s to improve the efficiency of networks by creating a data signal pertaining to but separate from each voice or data communications event. More recently, SS7 is used to pinpoint cell towers nearest to a suspect using a mobile device, both for domestic and international surveillance.

Subprobe – In lawful intercept, a Subprobe is an intelligent device that is configured to collect targeted communications from a communications service provider network. Subprobes are managed remotely and intercepted data is forwarded to a probe or mediation device for aggregation and correct formatting in the protocols specified by a law enforcement agency.

TDMA – Time Division Multiple Access. Provides channel access on shared medium networks, allowing multiple users to share a single frequency channel by dividing the signal into separate time slots.

Thuraya – A satellite communications company based in Dubai, United Arab Emirates. Thuraya provides satellite-based voice and data communications via SATCOM phone in the Middle East, Europe, Central and Northern Africa, Australia and Asia. SATCOM signals are converted to GSM. Thuraya is the SATCOM service most commonly used by Middle Eastern terrorists.

TIA – Telecommunications Industries Association: an advocacy group representing manufacturers of telecom hardware. In the surveillance arena, TIA develops standards pertaining to lawful intercept of traditional telephony (See **PSTN**).

Title III – That part of The Omnibus Crime Control and Safe Streets Act of 1968 outlining the rules of conventional “wiretapping.”

Trusted Third Party – A company that meets the standards of the law for providing CALEA solutions to communications service providers.

USA Freedom Act – Passed by the U.S. Congress and signed into law in June 2015, the USA Freedom Act renewed the Patriot Act but eliminated Section 215 of the Patriot Act in order to ban bulk metadata collection by the National Security Agency.

VPN – Virtual Private Network. Provides the functionality and security of private line service, but over the public network.

Vendor Index

Ability, *Mobile Location, Malware*

Aculab, *Lawful Intercept Solutions, Mobile Location*

AECOM, *Military Intelligence*

AGNITiO (now part of Nuance), *Biometric Identification*

ALBEDO Telecom, *Packet Monitoring*

Alcatel-Lucent, *Packet Monitoring*

Aglaya, *Packet Monitoring*, *Mobile Location*, *Malware*

Altron, *Lawful Intercept Solutions*

Amdocs, *Packet Monitoring*

AQSAQOM, *Lawful Intercept Solutions, Mobile Location*

Apogee, *Trusted Third Parties*

ATIS UHER, *Lawful Intercept Solutions*, *Mobile Location*, *Advanced Analytics*, *Military Intelligence*

Auraya Systems, *Biometric Identification*

BAE Systems Applied Intelligence, *Lawful Intercept Solutions*, *Advanced Analytics*

BEA, *Mobile Location*

Blue Coat, *Packet Monitoring*

BlueLight, *Biometric Identification*

Boeing, *Mobile Location*

BrightPlanet, *OSINT and Social Media Monitoring, Advanced Analytics*

Cambridge Consultants, *Mobile Location*

CinTel, *OSINT and Social Media Monitoring, Military Intelligence*

Cellebrite, *Forensics*

Cisco Systems, *Packet Monitoring*

ClearTrail Technologies, *Lawful Intercept Solutions*, *Packet Monitoring, Mobile Location, Malware*, *Advanced Analytics*

CommuniGate Systems, *Lawful Intercept Solutions*

ComWorth, *Packet Monitoring*

CRFS, *Military Intelligence*

CrowdControl, *OSINT and Social Media Monitoring*

CRYPTON-M, *Lawful Intercept Solutions*, *Mobile Location*, *Military Intelligence*

DATAKOM, *Packet Monitoring*

Decision Group, *Packet Monitoring*, *OSINT and Social Media* Monitoring

DESOMA, *Packet Monitoring*

Delta SPE, *Military Intelligence*

Digital Stakeout, *Military Intelligence*

DigiTask, *Packet Monitoring*, *Mobile Location*, *Malware*

DigiVox, *Packet Monitoring*

DreamLab Technologies, *Lawful Intercept Solutions*

Elaman, *Packet Monitoring*, *Malware*

Elbit Systems, *Advanced Analytics, Lawful Intercept Solutions*, *Mobile Location*, *Voice Biometrics*, *Malware*, *OSINT and Social Media Monitoring, Military Intelligence*

ELTA Systems, *Mobile Location, Military Intelligence*

Emulex, *Packet Monitoring*

Endgame Systems, *Malware*

Expert System, *Advanced Analytics*

Expert Team, Packet Monitoring

Fiberblaze, *Packet Monitoring*

Fifth Dimension, *Advanced Analytics with "Deep Learning" (AI) for pre-crime threat assessment*

FinFisher, *Malware*

Flowmon Networks, *Packet Monitoring*

Geofeedia, *OSINT and Social Media Monitoring*

Gigamon, *Packet Monitoring*

Gita Technologies, *Military Intelligence*

Glimmerglass Networks, *Advanced Analytics*

Guidance, *Forensics*

Group 2000, *Lawful Intercept Solutions*, *Mobile Location*, *Biometric Identification*, *OSINT and Social Media Monitoring*

Hacking Team, *Malware*

Harris Corporation, *Mobile Location*, *Malware*

HP Enterprise, *Lawful Intercept*, *Advanced Analytics*

Huawei, *Packet Monitoring*

IBM, *Advanced Analytics*

Incognito, *Packet Monitoring*

Ipoque, *Packet Monitoring*

INNOVA , *Lawful Intercept*

Intercept Monitoring Systems, *Mobile Location*, *Malware*

iPS, *Lawful Intercept Solutions*, *Mobile Location*, *Biometric Identification*, *Malware*, *Advanced Analytics*, *OSINT and Social Media Monitoring*

ixea, *Packet Monitoring*

Juniper Networks, *Packet Monitoring*

Keysight (formerly Agilent), *Military Intelligence*

Kofax (now owned by Lexmark) *Advanced Analytics*, *OSINT and Social Media Monitoring*

Leidos, *Advanced Analytics, OSINT and Social Media Monitoring*

LexisNexis, *OSINT and Social Media Monitoring*

Mantaro, *Packet Monitoring*

Medav GmbH (Saab), *Mobile Location*, *Military Intelligence*

MemSQL, *Advanced Analytics*

MSAB (formerly Micro Systemation), *Mobile Forensics*

NEC, *Biometric Identification*

Netbase, *OSINT and Social Media Monitoring*

Neti, *Packet Monitoring*

NetQuest, *Packet Monitoring*

Netronome, *Packet Monitoring*

NetScout, *Packet Monitoring*

Nexa Technologies, *Packet Monitoring*

NORSI-TRANS, *Lawful Intercept Solutions*, *Packet Monitoring*, *Mobile Location, Advanced Analytics*, *OSINT and Social Media Monitoring*

NSF Telecom, *Lawful Intercept Solutions*

NSO Group, *Malware*

Ntrepid, *Advanced Analytics, OSINT and Social Media Monitoring*

Nuance, *Voice Biometrics*

Ockham Solutions, *Mobile Forensics, Advanced Analytics*

Oxygen Software, *Forensics*

Packet Forensics, *Lawful Intercept Solutions*, *Packet Monitoring*

PALADION, *Lawful Intercept Solutions*, *Mobile Location*, *Malware*, *Advanced Analytics*, *Forensics*

Palantir, *Advanced Analytics, Military Intelligence*

Paraben Mobile Forensics, *Forensics*

Panoptech, *Military Intelligence*

Pen-Link, *Lawful Intercept Solutions*

Persistent Technologies, *Mobile Location*

Phonexia, *Voice Biometrics, Forensics*

Pine Digital Lawful Interception, *Lawful Intercept Solutions*

PLATH Group, *Military Intelligence*

PowerSpy, *Mobile Location*

PredPol, *OSINT and Social Media Monitoring*

Procera Networks, *Packet Monitoring*

Protei, *Packet Monitoring*, *Mobile Location*

Providence Group, *Military, Counter-Terrorism Solutions and Training*

Qosmos, *Packet Monitoring*

Radio Tactics, *Forensics, Military Intelligence*

Radisys, *Packet Monitoring*

Raytheon, *Advanced Analytics, Military Intelligence*

Rayzone, *Mobile Location, Malware*

RCS Labs, *Lawful Intercept Solutions*, *Mobile Location*, *Malware*, *Advanced Analytics*, *OSINT and Social Media Monitoring*

Recorded Future, *OSINT and Social Media Monitoring*

Rheinmettal Defence, *Military Intelligence*

Riverbed, *Packet Monitoring*

Rohde & Schwarz, *Packet Monitoring*

Roke Manor Research, *Lawful Intercept Solutions*, *Advanced Analytics*, *Forensics*, *Military Intelligence*

Savvius [formerly Wildpackets], Lawful Intercept Solutions, *Packet Monitoring*, *Forensics*

SciEngines, *Advanced Analytics*

Semptian, *Packet Monitoring*

Septier, *Lawful Intercept Solutions*, *Mobile Location, Advanced Analytics*

Shoghi Communications, *Lawful Intercept Solutions, Mobile Location, Military Intelligence*

SIEMENS Convergence Creators, GMbH, *Lawful Intercept Solutions*

STC, *Voice Biometrics, Forensics*

Sqrll, *Advanced Analytics*

SRI International, *Advanced Analytics*

SS8, *Lawful Intercept Solutions*, *Packet Monitoring, Malware, Advanced Analytics*

SSI Pacific*, Lawful Intercept Solutions*

Stratign, *Mobile Location*, *Malware, Military*

Suntech – Verint Group, *Lawful Intercept Solutions*, *Mobile Location*, *Advanced Analytics*

Subsentio, *Trusted Third Parties*

SwitchRay, *Lawful Intercept Solutions: U.S. shell company for Russia’s MFI-Soft*

Syborg – Verint Group, *Lawful Intercept Solutions*, *Mobile Location*

Telesoft Technologies, *Packet Monitoring, Mobile Location*

Tencent, *OSINT and Social Media Monitoring*

Thales, *Lawful Intercept Solutions*, *Packet Monitoring, Military*

TraceSpan, *Lawful Intercept Solutions*

Trackur, *OSINT and Social Media Monitoring*

Trovicor, *Lawful Intercept Solutions, Mobile Location, Malware*, *Advanced Analytics*, *OSINT and Social Media Monitoring*

Ultra Electronics, *Advanced Analytics*, *Packet Monitoring*, *Biometric Identification*, *Military*

Utimaco, *Lawful Intercept Solutions*

VASTech, *Military Intelligence*

Verint, *Advanced Analytics, Lawful Intercept Solutions*, *Mobile Location*, *Military Intelligence, OSINT and Social Media Monitoring, Malware*

Voice Biometrics Group, *Voice Biometrics*

VSS Monitoring, *Packet Monitoring*

Wintego, *Mobile Location*

Yaana Technologies, *Trusted Third Parties*, *Packet Monitoring, Malware*

Zerodium, *Malware*