GlobalResearch
Center for Research on Globalization

Glimmerglass Intercepts Undersea Cable Traffic for Spy Agencies

By Pratap Chatterjee
Global Research, August 23, 2013
CorpWatch 21 August 2013
Theme: Intelligence

Glimmerglass, a northern California company that sells optical fiber technology, offers government agencies a software product called “CyberSweep” to intercept signals on undersea cables. The company says their technology can analyze Gmail and Yahoo! Mail as well as social media like Facebook and Twitter to discover “actionable intelligence.”

Could this be the technology that the U.S. National Security Agency (NSA) is using to tap global communications? The company says it counts several intelligence agencies among its customers but refuses to divulge details. One thing is certain – it is not the only company to offer such capabilities – so if such data mining is not already taking place, that day is not far off.

“Revolutions in communications technologies are usually followed by revolutions in collection capabilities,” Jeffrey Richelson, a senior fellow at the National Security Archives and the author of the definitive guide to the U.S. intelligence agencies, told CorpWatch.

The recent leaks by whistleblower Edward Snowden to the Guardian newspaper specifically suggest that the NSA is tapping undersea cables although no details on the specific technology have yet been published. Notably Snowden has revealed evidence that the NSA paid £15.5 million ($25 million) in 2009 to “radically” upgrade a listening stationoperated by its U.K. equivalent – the Government Communications Head Quarters (GCHQ) in Bude, north Cornwall, England, where many of the cables surface.

If GCHQ and the NSA installed Glimmerglass’s commercial optical fiber switching technology on the undersea cables to tap the torrent of data that crosses the Atlantic, they will be able to pair it up with CyberSweep to make sense of the information, according to advertising claims made in a treasure trove of documents on dozens of surveillance contractors released by Wikileaks.

Privacy experts say that if the NSA is using this Glimmerglass technology, it will prove whistleblower Edward Snowden's claim that the government is collecting everyone's communications, regardless of their citizenship or innocence.

Vanee Vines, a spokesperson for the NSA, declined to comment to CorpWatch on either Glimmerglass or the tapping of the undersea cables. Glimmerglass officials did not return multiple email and phone calls.

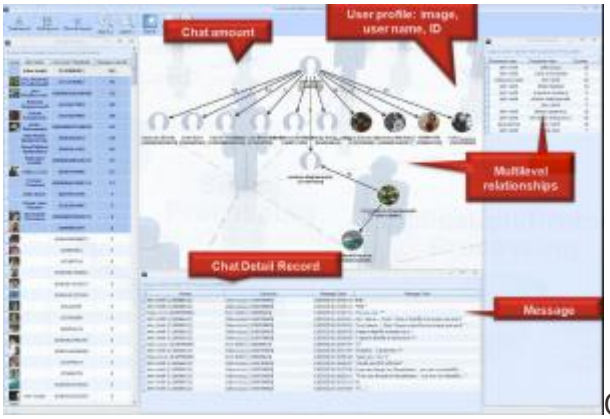
CyberSweep

On the Glimmerglass website, the company claims that CyberSweep can process optical signals to "extract the data source format" and aggregate the data for "probes" to uncover "actionable information from the flood of data on persons of interest, known and unknown targets, anticipated and known threats."

More details on what Glimmerglass claims CyberSweep can do are explained in "Paradigm Shifts" – a confidential 18 page Powerpoint presentation made in 2011 by Jim Donnelly, the Glimmerglass vice president of North American sales. The document was released by Wikileaks as part of the Spy Files series in December of that year.

On page five of the presentation, Glimmerglass notes that CyberSweep is an "end to end cyber security solution" that can "select, extract and monitor" all "mobile and fixed line data, voice and video, internet, web 2.0 and social networking" with "probes and sniffers." On the following page, it notes that its product can be used at "submarine landing stations" – a reference to the locations where the undersea cables are connected to terrestrial systems.

On page eight, Glimmerglass provides specific examples of what it can gather – like Gmail, Yahoo! Mail as well as Facebook and Twitter. Over the next four pages it offers screenshots of these capabilities.



One display of what CyberSweep is capable of is a visual grid of Facebook messages of a presumably fictional person named John Smith. His profile is connected to a number of other individuals with arrows indicating how often he connected to each of them. Each individual can be identified with images, user names and IDs. Another pane shows the detailed chat records. Yet another graphic shows Facebook connections between multiple individuals, presumably to identify networks.

A third graphic is a grid of phone calls made by an individual with a pane that allows an operator to select and listen to audio of any specific conversation. Other images show similar demonstrations of monitoring webmail and instant message chats.

Where is this product being used? In a product video on the company website, Glimmerglass states that their optical data management products have been used by the U.S. intelligence agencies for the last five years. The video specifically mentions data transmissions from Predator drones and well as the tapping of undersea fiber optic cables, but it does not go into any details.

"The challenge of managing information has become the challenge of managing the light," says an announcer. "With Glimmerglass, customers have full control of massive flows of intelligence from the moment they access them."

The description mirrors the technology described in documents provided by Edward Snowden to the Guardian newspaper.

Collecting All the Signals

The GCHQ Advantage
Why go overseas to collect the data? Well, there are legal obstacles in the U.S. to collecting phone calls made by U.S. citizens – such a program would violate the fourth amendment to the U.S. constitution that protects individuals against invasion of privacy. (Exceptions are granted for communications with foreigners if government agencies suspect terrorism under a 1981 presidential executive order, although they still need approval of the U.S. Attorney General).
But given that U.S. laws stop at the border, foreign spy agencies like GCHQ can legally pick up and store any and all information from data that travels outside the country, suggest reporters at the Guardian newspaper.
"We know the NSA is forbidden from spying on American citizens; in the case of (Faizal) Shahzad (the would-be Times Square bomber in New York), this question remains – was GCHQ doing it for them?" ask the Guardian reporters, noting that the GCHQ now has the "opportunity to build such a complete record of someone's life through their texts, conversations, emails and search records" allowing it to make a "unique contribution to the NSA in providing insights into some of their highest priority targets."

In a document released by Snowden, Lieutenant General Keith Alexander, the NSA director, was quoted on a June 2008 visit to an intelligence facility in the U.K., saying: "Why can't we collect all the signals all the time? Sounds like a good summer project."

According to the leaked documents, a three year trial project was soon set up with a $25 million grant from the NSA to "radically enhance the infrastructure" at the Cyber Development Centre in Bude, Cornwall, as well as potentially at other sites like the GCHQ base in Cheltenham.

Probes were installed on 200 undersea cables and in the fall of 2011, a project code-named Tempora was launched with the help of NSA analysts who came to help at the Bude site. At least seven companies took part in the project – British Telecom, Global Crossing, Interoute, Level 3, Viatel, Verizon Business and Vodafone Cable – according to the German paper Suddeutsche Zeitung, all of whom manage major undersea cable systems.

Under Tempora, a three day buffer of global internet traffic was held at any given time – totaling some 600 million "telephone events" a day or as much as 21 petabytes (million gigabytes) of data. While much of it was deleted through a process called Massive Volume

Reduction for reasons of space, the meta-data (such as the details of who called whom, and when, but not the content) was held for as long as 30 days.

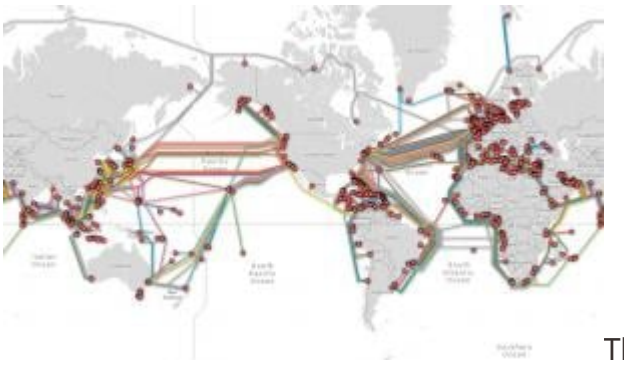
Snowden's documents suggest that GCHQ now "produces larger amounts of metadata than NSA" which was being analyzed by 300 U.K. analysts in addition to 250 NSA analysts, as of last May. The U.K. analysts were encouraged to dig deep since they had a less onerous oversight regime compared to the U.S.

"Over the last five years, GCHQ's access to 'light' (has) increased by 7,000%," a Tempora official is quoted as saying in another Powerpoint document cited in the Guardian. "We will have exploited to the full our unique selling points of geography, partnerships, the UK's legal regime and our skilled workforce."

A recent interview of a "senior intelligence official" by the New York Times confirmed that "the N.S.A. is temporarily copying and then sifting through the contents of what is apparently most e-mails and other text-based communications that cross the border" by making a "clone of selected communication links." The official did not state where the communications were being intercepted.

Optical Tapping

It so happens that the undersea cables are an extremely convenient place to collect all the signals all the time: An estimated 90 percent of trans-border telecommunications data travels along the transatlantic cables, even if they are merely connections between an individual in Asia and another in Africa, especially if they are using services like Skype.



These cables date back in history to 1858 when they were first installed to support the international telegraph system, with the British taking the lead to wire the far reaches of its empire. Today a multi-billion dollar shipping industry continues to lay and maintain hundreds of such cables that crisscross the planet – over half a million miles of such cables are draped along the ocean floor and snaked around coastlines – to make landfall at special locations to be connected to national telecommunications systems.

The original cables were made of copper but about 25 years ago, they were replaced by fiber-optic cables. The oldest undersea cable was Trans Atlantic-8 (installed in 1988 by AT&T to transmit data from Tuckerton, New Jersey to Bude, Cornwall) which transmitted data at 280 megabits per second. The latest cables like Yellow/Atlantic Crossing 2 (installed in 2000 and upgraded in 2007 by Level Three Communications from Brookhaven, New York to Bude, Cornwall) is capable of transmitting data at an astonishing 640 gigabits per second, which is roughly equal to 7.5 million simultaneous phone calls.

In order to make sure that data and voice are transmitted quickly and accurately across the world even if cables break or equipment fails, cable companies break the data into separate tiny packets that are dispatched over what they call “redundant fiber optic paths” across the ocean before it is captured and re-assembled on the other side, where it also becomes easy to intercept the data unobtrusively.

This is where Glimmerglass comes in. In September 2002, the company started to ship a pioneering technology to help transmit data accurately over multiple optical paths. Their patented “3D Micro-Electro-Mechanical-System (MEMS) mirror array” is composed of 210 gold-coated mirrors mounted on microscopic hinges, each measuring just one millimeter in diameter, etched on a single wafer of silicon.

Each mirror can be individually managed by remote operators anywhere in the world to capture or bounce the light signals and even more importantly, communicate with the other mirrors to make sure that the rest of the array stays in place, allowing very accurate data transmission. This technology slashed the cost of optical switching by a factor of 100, and the company claims that the switches are very robust with an expected failure rate of once in 30 years.

For telecommunication companies, Glimmerglass offers three hardware racks to handle optical data – the entry level “100” system which can handle as many as 96×96 fiber ports for traffic as high as 100 gigabits per second all the way up to the “600” system which can handle 192×192 fiber ports. It also offers the “3000” system which can hold up to 12 racks.

Another major advantage of the Glimmerglass technology, according to the company, is that operators can “monitor and test remote facilities” at undersea cable landings from a central office and then select any one of multiple optical signals to distribute it to multiple recipients, as well as ability to redirect any signal.

“With Glimmerglass Intelligent Optical Systems, any signal travelling over fiber can be redirected in milliseconds, without adversely affecting customer traffic. At a landing site, this connectivity permits optical layer connections between the wet side and dry side to be re-provisioned in milliseconds from the Network Operations Center with a few clicks of a mouse.”

In another section of the public website the company also promotes a product named Glimmerglass Intelligent Optical System (IOS) that combines the 3D-MEMS switches with CyberSweep into an integrated product that has the ability to “monitor and selectively intercept communications.”

“Service Providers can use the speed and flexibility of the IOS to select and deliver signals

to Law Enforcement Agencies (LEA)," add company brochures uncovered by Wikileaks. "The agency gains rapid access, not just to signals, but to individual wavelengths on those signals (and) make perfect photonic copies of optical signals … for comprehensive analysis."

Glimmerglass does not deny that its equipment can be used to capture global internet traffic by intelligence agencies, in fact it assumes that this is probably happening.

"If you are going to monitor (communications traffic), you need to do much of it optically. But clearly, the massive top of the (intelligence gathering) funnel is coming through optically and you need to manage that," Robert Lundy, the CEO of Glimmerglass for the last nine years, told AviationWeek in 2010. "If we were (installed) at an operations center of some country, our systems could be used to look at all the international entry and exit points for fiber optics. Once you have extracted the wavelengths, you can dynamically select the ones you are interested in and do it all from a remote location."

Keith May, his deputy in charge of business development, has gone even further. "We believe that our 3D MEMS technology – as used by governments and various agencies – is involved in the collection of intelligence from sensors, satellites and undersea fiber systems," May told the magazine. "We are deployed in several countries that are using it for lawful interception."

Cashing in on the Fiber Boom

Lundy is a graduate of the U.S. Military Academy at West Point, with two degrees from Stanford University in the heart of northern California's high technology Silicon Valley – a Master's degree in Electrical Engineering and a Masters in Business Administration –making him well placed to ride the fiber optic boom.

In addition to the right degrees from the right military and technology colleges, Lundy retired as an Army lieutenant colonel after working for the U.S. Army in Europe where his job was managing contracts for "tactical data systems." He worked as the first general manager of IBM's wireless business unit and then he helped found three successful start-ups: Wavtrace, a pioneer in manufacturing wireless broadband access systems for business; Optos, a company that builds optical switches for metropolitan networks; as well as Xtera, a company that provides equipment to push data via submarine cables.

Lundy was hired as chief operating officer for Glimmerglass in 2004 when it was a five year old start-up that had patented dozens of 3D MEMS inventions, from its offices in Hayward on the eastern edge of Silicon Valley. Initially the company made its money selling testing and measurement equipment for what Lundy calls their "core optical switch or engine" to a couple of dozen customers in the telecommunications industry like Cisco and Sandvine, but was unable to expand in a major way because of the collapse of the telecommunications industry at the time. (Global Crossing, a major cable operator, had just gone bankrupt, as had WorldCom)

The company branched out to make most of its profits from the software to manage the optical switches, rather than the physical hardware which sold for under $100,000 in competition with similar products from companies like Calient. Glimmerglass quickly landed contracts with AMS-IX, the largest internet exchange in Europe, and with Cable & Wireless in the UK.

Eavesdropping On The Whole World
Analysis of bulk telecommunications data to track as yet unknown targets has long been on the NSA wish list. For decades, the agency stuck to following specific individuals because there was no way to capture and analyze everything.
In 2000, two rival projects were commissioned to try to collect "all the signals all the time." Science Applications International Corporation, based in Tyson's Corner, Virginia, was given a contract to design a collection system called TrailBlazer, while the NSA's in-house Signals Intelligence (SIGINT) Automation Research Center (SARC) worked on a project called ThinThread.
Trailblazer was eventually jettisoned as unworkable after $1.2 billion had been spent. ThinThread was more successful, according to its proponents, because it was able to selectively process important information and dump the rest. The designers also created controls to anonymize the data collection to avoid violating privacy laws.
ThinThread could "correlate data from financial transactions, travel records, Web searches, G.P.S. equipment, and any other 'attributes' that an analyst might find useful in pinpointing 'the bad guys,'" writes Jane Mayer in the New Yorker magazine, based on her interviews with former NSA staff.
Unfortunately for the SARC team, ThinThread was vetoed by upper management at the NSA in August 2001. But after the September 11, 2001 attacks, the NSA is believed to have returned to the drawing board. Rumor has it that the project was restarted, stripped of any privacy controls.
Recently William Binney, a former NSA staffer who helped design ThinThread and has now become a whistleblower, says that the project was a mistake. "I should apologize to the American people," Binney who was once the technical director for the 6,000 employees of the NSA's World Geopolitical and Military Analysis Reporting Group told Mayer. "It's violated everyone's rights. It can be used to eavesdrop on the whole world."

In May 2005, Lundy was promoted to CEO of the company. Four months later – on September 21, 2005 – Glimmerglass Networks was awarded a no-bid contract of $769,600 for telecommunications support equipment for the U.S. Navy Sea Systems Command.

Lundy's experience managing data contracts for the U.S. Army in Europe would not have hindered the sale. Nor would the deep connections ofGlimmerglass board member Alan Rogers, a retired U.S. Air Force Major General, who had previously been in charge of planning for the Pentagon at the North Atlantic Treaty Organization (NATO) Supreme Headquarters Allied Powers Europe (SHAPE) headquarters in Brussels.

By 2010, Lundy had successfully expanded Glimmerglass' business by marketing "lawful interception systems" to seven international customers outside the U.S., which appear to include Germany, Israel and the UK as well as two unnamed countries in Asia.

"We've become as a result a gold standard in the intel and defense community … they're managing these optical signals so they can acquire, split, move and obtain the necessary information to protect the country," Lundy told Fierce Telecom, an industry blog, in an interview about global malware threats. "At their undersea landing locations, their major points of presence, on a selective basis they need to acquire and monitor those optical signals … rather than wait to get it off somebody's, when it hits a PC or cellphone."

Questions remain as to how well the Glimmerglass product works. Ed Loomis, who worked

on the NSA's ThinThread signal collection and monitoring project in the 1990s, (*see box: Eavesdropping On The Whole World*) told CorpWatch that the company claim that they can extract "actionable information" would be limited to little more than selecting from a customer-supplied list of phone numbers, IP addresses, and DNS email addresses.

"In order to replicate an analyst's deductive reasoning process to create an artificial intelligence equivalent requires an immense amount of cooperation by an analyst and an understanding of analytic processes by the programmer," said Loomis. "Unless the two have acquired years of experience in the intelligence production business, I doubt the 'target analytics' is as robust as Glimmerglass would have its clients believe."

Are Companies Helping Invade Privacy?

Civil liberties experts have denounced the practice of wholesale data collection. "By injecting the N.S.A. into virtually every crossborder interaction, the U.S. government will forever alter what has always been an open exchange of ideas," says Jameel Jaffer, the deputy legal director of the American Civil Liberties Union.

Such collection would also violate numerous legal principles that safeguard individual privacy. In addition to the fourth amendment to the U.S. constitution, human rights experts say that it would violate Article 8 of the European Convention on Human Rights and Article 12 of the Universal Declaration of Human Rights.

The big questions now are what role did the telecommunication companies play in the data interception and are intelligence contractors like Glimmerglass helping to design the collection and analysis system?

"Tempora would not have been possible without the complicity of these undersea cable providers," says Eric King, head of research at Privacy International. "What we, and the public, deserve to know is this: To what extent are companies cooperating with disproportionate intelligence gathering, and are they doing anything to protect our right to privacy?"

The Glimmerglass brochures can be downloaded here:

http://www.wikileaks.org/spyfiles/docs/glimmerglass/55_glimmerglass-cybersweep.html

and here:

http://www.wikileaks.org/spyfiles/docs/glimmerglass/275_transparent-signal-access-and-monitoring.html

---

Articles by: Pratap Chatterjee