The NSA's cyber-surveillance technology

Infrastructure of a police state

Kevin Reed
25 June 2013

Edward Snowden's documentary exposure of secret NSA surveillance activities has brought to light details of the mass illegal collection of phone metadata and online transaction activity of both US citizens and individuals, organizations and governments around the world.

Following a classified Congressional intelligence briefing on June 11, US Representative Loretta Sanchez stated in a C-Span interview that Snowden's disclosures were "the tip of the iceberg." Indeed, with more revelations to come, Edward Snowden has courageously helped make the public aware of a vast spying conspiracy by the corporate-military-intelligence apparatus within the US.

Prior to Snowden's revelations, available published information about the NSA's signals intelligence systems has been limited. Much of what is presented here is derived from the work of James Bamford, journalist and intelligence expert and author of several books on the NSA including *The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America* (2008).

Bamford has conducted extensive interviews with former NSA employees and other whistleblowers. He is also the author of a March 2012 *Wired* magazine article entitled, *The NSA is Building the Country's Biggest Spy Center (Watch What You Say)* .

Background to NSA surveillance

In the early days of the cold war, the NSA developed "black" activities and began building up the infrastructure for secretly monitoring communications inside and outside the US. One of the first warrantless NSA surveillance operations—Project Shamrock—involved copying telegrams and passing them to US law enforcement and the military. There was no distinction between foreign and domestic communications; every telegram was being copied to microfilm.

Project Shamrock required collaboration between the NSA and the communications industry. Companies such as Western Union, RCA and ITT made secret agreements and turned over the telegrams to the NSA every night. The program was exposed in 1975 and became a subject of the Senate Intelligence Committee hearings of Frank Church that resulted in the FISA law of 1978.

With the growth of post-war satellite and microwave communications, a surveillance program called Echelon pioneered the interception, storage and analysis of trunk-line voice and data communications. To cover the entire globe, Echelon became a joint program of the so-called Five Eyes (US, UK, Australia, Canada and New Zealand) and utilized the most advanced satellite and software technologies of its time. Since only 1% of the world's telecommunications traffic passes through satellites today, it is believed that Echelon remains an aspect of signals intelligence that is otherwise dedicated to fiber optic cable networks.

In the 1990s, the Internet, World Wide Web and mobile phones transformed global communications. To keep pace, the NSA moved to transition its black operations to the new era of cyber-surveillance. Initially, due to residual concerns from the Nixon era about domestic spying, the NSA was restricted from taking widespread advantage of the technologies being developed by the emerging intelligence industry. However, after the attacks of the September 11, 2001, huge sums were pumped into surveillance budgets and NSA proposals and initiatives that were sitting on shelves for years were ramped up and brought online.

It is clear that the same political forces within the ruling class that utilized the hysteria over 9/11 to rapidly carry out war plans long in the making also moved swiftly to implement high-tech eavesdropping operations, especially within the US.

One such program was the Bush administration's Total Information Awareness (TIA) initiative run by the secret Office of Information Awareness (OIA), headed by former Iran-Contra conspirator John Poindexter, beginning in February 2002. TIA was the brainchild of J. Brian Sharkey, a deputy director of the Defense Advanced Research Projects Agency, who recognized early on the exceptional opportunities to "vacuum up" everyone's digital trail. Sharkey's concept was that bookstore visits, gas station fill-ups, phone data and Internet search activity could be processed with supercomputers and complex algorithms to automate the surveillance process.

Following the exposure of Poindexter's TIA/OIA operation in late 2002, the public was told that these illegal NSA activities would be suspended and funding terminated by congressional action. However, considered too valuable to scrap, these functions were moved deeper into the bowels of military intelligence and kept going by the Pentagon.

The Obama administration, far from reducing the activities of the NSA, has expanded illegal spying operations to staggering proportions. Along with the use of unmanned and remote controlled drones for "targeted assassinations," technological breakthroughs in high-speed optical communications and computer processing power, storage and decryption have been used to intensify spying.

Given the colossal scale of the technologies both in place and coming online soon, it is conceivable that the US government intends to intercept, store, catalog, and profile the activities of every single person with a cell phone or an Internet connection, i.e., more than two-thirds of the world's population, or about 4.5 billion people.

The NSA's structure

Centered at its city-sized headquarters in Fort Meade, Maryland, the NSA is engaged in communications monitoring program that includes many billions of exchanges per day. Tapping into the entirety of global

Internet and phone call data that passes through nodal points in the US and around the world, the NSA processes enormous volumes of information in real time.

What cannot be used today—due to the effectiveness of current encryption technologies, for example—is being stored and cataloged for future decryption and analysis. Additionally, in the Orwellian world of American intelligence, what may not be officially considered a "threat" today can turn into one tomorrow and the "evidence" put together from readily available databases.

The NSA has 40,000 employees, made up of administrators, code-breakers, intercept operators, crypto-linguists and area specialists. Increasingly, the NSA subcontracts work to private corporations such as Booz Allen Hamilton (Edward Snowden's former employer), Raytheon, Lockheed Martin, Northrop Grumman, and Science Applications International Corporation (SAIC). Although the NSA budget is classified, Bamford estimated it at $60 billion in 2008, with 70% being spent on subcontractors.

The NSA operates four geostationary satellite facilities around the world that monitor radio frequencies from satellite and microwave communications to cell phone and walkie-talkie signals. Within the US, the agency has a network of sites in Pennsylvania, California, Colorado, Texas, Georgia, Tennessee, and Hawaii. Some of these are either research facilities like Oak Ridge, Tennessee, or are sites that manage the communication intercepts into the network from different parts of the world.

Due to the interdependent nature of the worldwide telecommunications grid, the distinction between information that is specifically "foreign" versus that which is "domestic"—upon which much of the FISA wiretapping laws were drafted—has been rendered meaningless. Amongst the trillions of packets of information traversing the network each day, international and US-only data are entirely comingled.

Interception in gigabits

The system of undersea fiber optic cables carries 99 percent of international telecommunications. The NSA is not tapping the fiber network at the two-dozen cable landing stations in the US where overseas traffic enters the US. Instead, the agency has installed sophisticated "optical splitters" or data interceptors at major commercial exchange and switching hubs well within the shoreline. It is gathering vast amounts of information.

Bamford interviewed Mark Klein, an AT&T employee who exposed the NSA's tapping of the communications infrastructure in 2006. As early as 2003, Klein became aware of government monitoring at AT&T's San Francisco hub with the installation of a Narus intercept traffic analyzer, an advanced computer system that taps directly into the fiber optic lines. Klein said, "What I saw is that everything's flowing across the Internet to this government-controlled room. The physical apparatus gives them everything. A lot of this was domestic."

Narus initially specialized in high speed data filtering systems that differentiate email, chat, calendar appointments, draft folders, address books, etc., to calculate telecom processing fees. As Bamford explained, "Following the attacks on 9/11, Narus began modifying its system and selling it to intelligence agencies around the world, who used it not for billing purposes but for mass surveillance."

Today, as a subsidiary of Boeing, the latest generation of Narus systems is capable of "deep packet inspection," the ability to distinguish between different planes within the data flow, and examining Internet traffic as it passes through the 10-gigabit-per-second cables at the speed of light. According to former NSA intelligence official William Binney, the NSA has these systems installed at "10 or 20" switches around the country, and they are managed remotely from Fort Meade. Binney says the NSA is challenged with what to do with the 20 terabytes of intercepted data being captured each minute.

Storage in yottabytes

Presently, the NSA is building a facility called the Utah Data Center that is scheduled to open in September of this year. The $2 billion construction project in Bluffdale, 20 miles south of Salt Lake City, will be the largest cloud-based data storage facility in the world and the hub of the NSA's cyber-espionage operations. At more than 1 million square feet, the top-secret and self-sustaining complex will host servers capable of storing yottabytes of data. A yottabyte (1024 bytes) is 1 trillion terabytes.

The NSA is building the Utah data-mining facility—including four 25,000-square-foot data halls packed with high speed servers—in a mad attempt to keep pace with the exponential growth of communications traffic. It has been estimated that total data throughput on the Internet will quadruple from 2010 to 2015 to just under 1,000 exabytes per year (1 million exabytes = 1 yottabyte). A major aspect of the Utah Data Center's purpose is to penetrate and gather the data in the "deep web," i.e., password-protected information that is secure, private, and not available for public browsing.

The facility will have 900,000 square feet of technical support and administrative offices. According to Bamford, "Flowing through its servers and routers and stored in near-bottomless databases will be all forms of communication, including the complete contents of private emails, cell phone calls, and Google searches, as well as all sorts of personal data trails—parking receipts, travel itineraries, bookstore purchases, and other digital 'pocket litter.'"

Analysis in petaflops

One of the purposes of the center in Bluffdale is to develop the ability to break through standard encryption technologies that make it impossible to read the content of some intercepted data. The NSA plans to crack encryption with a combination of super-fast computers and "brute force" attacks on messages, going through a massive number of messages to analyze. According to Bamford, "The more messages from a given target, the more likely it is for the computers to detect telltale patterns, and Bluffdale will be able to hold a great many messages."

The processing aspect is being worked on as part of what is known as the High Productivity Computer Systems program at the NSA's research facility in Oak Ridge, Tennessee. The initial goal was to build the most powerful computer ever known and advance computational speeds beyond a quadrillion (1015) operations per second (petaflop). A flop is a measurement of mathematical floating-point calculations that a computer can process per second. A very fast desktop computer today can achieve speeds of 100 gigaflops or about one hundred thousand times slower than the NSA's goal.

Working with Cray, the supercomputer company as a $250 million contract partner, the NSA built a system code-named "Jaguar" that broke the petaflop barrier and officially became the world's fastest computer in 2009. In 2011, the Oak Ridge facility hit 2.33 petaflops but it ranked third in speed behind Japan's "K Computer," with an impressive 10.51

petaflops, and the Chinese Tianhe-1A system, with 2.57 petaflops. The next NSA goal is to complete a project code-named “Titan” that will hit speeds of 10 to 20 petaflops by 2013.

Threat of a police state

When considered within the context of the economic, social and political crisis of American capitalism, the unprecedented scale and scope of the NSA electronic eavesdropping on US citizens and others around the world has an ominous character to it. It is clear that such measures are being prepared for reasons other than those officially provided.

At the height of its power, the Nazi regime of Adolf Hitler used the most sophisticated analog information methods available to identify and track those whom it deemed undesirable. The 1933 census was used to establish the ethnic identity of the population and was conducted with the assistance of the computer punch card tabulation services invented by Herman Hollerith and provided by IBM. Years later, each one of the Nazi concentration camps had a three-digit Hollerith code number it used for paperwork purposes.

The explosive development of mobile and wireless devices and their ubiquity in the lives of the vast majority of the world’s population make it possible for sinister operations within the state to gather details about each individual’s everyday activities for repressive purposes.