GlobalResearch
Center for Research on Globalization

US Cyber Command's Plan X: Pentagon Launching Covert Cyber Attacks

By Tom Burghardt
Global Research, October 03, 2013
Antifascist Calling

Theme: Militarization and WMD, US NATO War Agenda

In 2008, the *Armed Forces Journal* published a prescient piece by Colonel Charles W. Williamson III, a staff judge advocate with the Air Force Intelligence, Surveillance and Reconnaissance Agency at Lackland Air Force Base in Texas, the National Security Agency listening post focused on intercepting communications from Latin America, the Middle East and Europe.

Titled "Carpet bombing in cyberspace," Col. Williamson wrote that "America needs a network that can project power by building an af.mil robot network (botnet) that can direct such massive amounts of traffic to target computers that they can no longer communicate and become no more useful to our adversaries than hunks of metal and plastic. America needs the ability to carpet bomb in cyberspace to create the deterrent we lack."

While Williamson's treatise was fanciful (a DDoS attack can't bring down an opponent's military forces, or for that matter a society's infrastructure), he had hit upon a theme which Air Force researchers had been working towards since the 1980s: the development of software-based weapons that can be "fired" at an adversary, potentially as lethal as a bomb dropped from 30,000 feet.

Two years later, evidence emerged that US and Israeli code warriors did something far more damaging.

Rather than deploying an "af.mil" botnet against Iran's civilian nuclear infrastructure at Natanz, they unleashed a destructive digital worm, Stuxnet. In the largest and most sophisticated attack to date, more than 1,000 centrifuges were sent spinning out of control, "no more useful" to Iranian physicists "than hunks of metal and plastic."

A line had been crossed, and by the time security experts sorted things out, they learned that Stuxnet and its cousins, Duqu, Flame and Gauss, were the most complex pieces of malware ever designed, the opening salvo in the cyberwar that has long-guided the fevered dreams of Pentagon planners.

'Plan X'

Today, that destructive capability exists under the umbrella of US Cyber Command (USCYBERCOM), one which has the potential of holding the world hostage.

Last year the Pentagon allocated $80 million dollars to defense giant Lockheed Martin for ongoing work on the National Cyber Range (NCR), a top secret facility that designs and tests attack tools for the government.

Under terms of the five year contract, Lockheed Martin and niche malware developers have completed work on a test-bed housed in a "specially architected sensitive compartmented information facility with appropriate security protocols" that "emulates the public internet and other networks, and provides for the modeling of cyber attacks."

Originally developed by the Defense Advanced Research Projects Agency (DARPA), the Pentagon's geek squad, NCR has gone live and was transitioned last year to the Office of the Secretary of Defense, federal contracts uncovered by *NextGov* revealed.

As *Antifascist Calling* reported back in 2009, "NCR will potentially serve as a new and improved means to bring America's rivals to their knees. Imagine the capacity for death and destruction implicit in a tool that can . . . cause an adversary's chemical plant to suddenly release methyl isocynate (the Bhopal effect) on a sleeping city, or a nuclear power plant to go supercritical, releasing tens of billions of curies of radioactive death into the atmosphere?"

NextGov also reported that the "Pentagon is seeking technology to coordinate and bolster cyberattack capabilities through a funding experiment called 'Plan X,' contract documents indicate."

A notice from DARPA's Information Innovation Office (I2O) informs us that "Plan X is a foundational cyberwarfare program to develop platforms for the Department of Defense to plan for, conduct, and assess cyberwarfare in a manner *similar to kinetic warfare*. Towards this end the program will bridge cyber communities of interest from academe, to the defense industrial base, to the commercial tech industry, to user-experience experts." (emphasis added)

Although DARPA claims "Plan X will not develop cyber offensive technologies or effects," the program's Broad Agency Announcement, DARPA-BAA-13-02: Foundational Cyberwarfare (Plan X), explicitly states: "Plan X will conduct novel research into the nature of cyberwarfare and support development of fundamental strategies needed to dominate the cyber battlespace. Proposed research should investigate innovative approaches that enable revolutionary advances in science, devices, or systems."

The document also gives notice that DARPA will build "an end-to-end system that enables the military to understand, plan, and manage cyberwarfare in real-time" as an "open platform architecture for integration with government and industry technologies."

The *Military & Aerospace Electronics* web site reported that DARPA has "chosen six companies so far to define ways of understanding, planning, and managing military cyber warfare operations in real-time, large-scale, and dynamic networks."

Collectively worth some $74 million, beneficiaries of taxpayer largesse include "Data Tactics Corp. in McLean, Va.; Intific Inc. in Peckville Pa.; Raytheon SI Government Solutions in Arlington, Va.; Aptima Inc. in Woburn Mass.; Apogee Research LLC in McLean, Va.; and the Northrop Grumman Corp. Information Systems segment in McLean, Va."

Additional confirmation of US government plans to militarize the internet were revealed in top secret documents provided by former NSA contractor-turned-whistleblower Edward Snowden. Those documents show that the Pentagon's goal of "dominating cyberspace" are one step closer to reality; a nightmare for privacy rights and global peace.

Such capabilities, long suspected by security experts in the wake of Stuxnet, are useful not only for blanket domestic surveillance and political espionage but can also reveal the deepest secrets held by commercial rivals or geostrategic opponents, opening them up to covert cyber attacks which *will* kill civilians if and when the US decides that critical infrastructure should be been switched off.

Before a cyber attack attack can be launched however, US military specialists must have the means to tunnel through or around security features built into commercial software sold to the public, corporations and other governments.

Such efforts would be all the easier if military specialists held the keys that could open the most secure electronic locks guarding global communications. According to Snowden, NSA, along with their corporate partners and private military contractors embarked on a multiyear, multibillion dollar project to defeat encryption through the subversion of the secure coding process.

Media reports published by *Bloomberg Businessweek*, *The Wall Street Journal* and *The Washington Post*, also revealed that US intelligence agencies are employing "elite teams of hackers" and have sparked "a new arms race" for cyberweapons where the "most enticing targets in this war are civilian–electrical grids, food distribution systems, any essential infrastructure that runs on computers," *Businessweek* noted.

Confirming earlier reporting, *The Washington Post* disclosed that the US government "carried out 231 offensive cyber-operations in 2011, the leading edge of a clandestine campaign that embraces the Internet as a theater of spying, sabotage and war, according to top-secret documents" provided by Snowden to the *Post*.

Since its 2009 stand-up as a "subordinate unified command" under US Strategic Command (USSTRATCOM), whose brief includes space operations (military satellites), information warfare (white, gray and black propaganda), missile defense, global command and control, intelligence, surveillance and reconnaissance (ISR), as well as global strike and strategic deterrence (America's first-strike nuclear arsenal), Cyber Command has grown from 900 personnel to a force that will soon expand to more than "4,900 troops and civilians," *The Washington Post* reported earlier this year.

Under the USSTRATCOM umbrella, the organization is comprised of "Army Cyber Command (ARCYBER); Air Forces Cyber (AFCYBER); Fleet Cyber Command (FLTCYBERCOM); and Marine Forces Cyber Command (MARFORCYBER)."

"The Command," according to a 2009 Defense Department Fact Sheet, "is also standing up dedicated Cyber Mission Teams" that "conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries."

The Defense Department Memorandum authorizing it's launch specified that the Command "must be capable of synchronizing warfighting effects across the global security environment as well as providing support to civil authorities and international partners."

In written testimony to the Senate Armed Services Committee during 2010 confirmation hearings, NSA head General Keith Alexander agreed, and *The New York Times* reported that Cyber Command's target list would "include civilian institutions and municipal infrastructure

that are essential to state sovereignty and stability, including power grids, banks and financial networks, transportation and telecommunications."

But what various "newspapers of record" still fail to report is that the deliberate targeting of civilian infrastructure are *war crimes* that cause catastrophic loss of life and incalculable suffering, as US attacks on the former Yugoslavia, Iraq and more recently, Libya, starkly demonstrate.

In a portrait of Alexander published earlier this summer by *Wired*, James Bamford noted that for years the US military has "been developing offensive capabilities, giving it the power not just to defend the US but to assail its foes. Using so-called cyber-kinetic attacks, Alexander and his forces now have the capability to physically destroy an adversary's equipment and infrastructure, and potentially even to kill."

While the specter of a temporary "interruption of service" haunt modern cities with blackout or gridlock, a directed cyberattack focused on bringing down the entire system by inducing widespread technical malfunction would transform "the vast edifices of infrastructure" into "so much useless junk," according to urban geographer Stephen Graham.

In *Cities Under Siege*, Graham discussed the effects of post-Cold War US/NATO air bombing campaigns and concluded that attacks on civilian infrastructure were not accidental; in fact, such "collateral damage" was consciously designed to inflict maximum damage on civilian populations.

"The effects of urban de-electrification," Graham wrote, "are both more ghastly and more prosaic: the mass death of the young, the weak, the ill, and the old, over protracted periods of time and extended geographies, as water systems and sanitation collapse and water-borne diseases run rampant. No wonder such a strategy has been called a 'war on public health,' an assault which amounts to 'bomb now, die later'."

A further turn in US Cyber Command's brief to plan for and wage aggressive war, was telegraphed in a 2012 Defense Department Directive mandating that autonomous weapons systems and platforms be built and tested so that humans won't lose control once they're deployed.

There was one small catch, however.

According to Deputy Secretary of Defense Ashton Carter, a former member of the Board of Trustees at the spook-connected MITRE Corporation, the Directive explicitly states it "does not apply to autonomous or semi-autonomous cyberspace systems for cyberspace operations."

Presidential Policy Directive 20: Authorizing 'Cyber-Kinetic' War Crimes

We now know, based on documents provided by Edward Snowden, that President Barack Obama "has ordered his senior national security and intelligence officials to draw up a list of potential overseas targets for US cyber-attacks," according to the 18-page top secret Presidential Policy Directive 20 published by *The Guardian*.

Though little commented upon at the time due to the avalanche of revelations surrounding dragnet domestic surveillance carried out by NSA, in light of recent disclosures by *The Washington Post* on America's bloated $52.6 billion 2013 intelligence budget, PPD-20

deserves close scrutiny.

With Syria now in Washington's crosshairs, PPD-20 offers a glimpse into Executive Branch deliberations before the military is ordered to "put steel to target."

The directive averred that Offensive Cyber Effects Operations (OCEO) "can offer unique and unconventional capabilities to advance US national objectives around the world with little or no warning to the adversary or target and with potential effects ranging from subtle to severely damaging."

These are described in the document as "cyber effects," the "manipulation, disruption, denial, degradation, or destruction of computers, information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon."

To facilitate attacks, the directive gives notice that "cyber collection" will entail "Operations and related programs or activities conducted by or on behalf of the United States Government, in or through cyberspace, for the primary purpose of collecting intelligence–including information that can be used for future operations–from computers, information or communications systems, or networks with the intent to remain undetected."

Such clandestine exercises will involve "accessing a computer, information system, or network without authorization from the owner or operator of that computer, information system, or network or from a party to a communication or by exceeding authorized access."

In fact, PPD-20 authorizes US Cyber Command to "identify potential targets of national importance where OCEO can offer a favorable balance of effectiveness and risk as compared with other instruments of national power."

Indeed, the "directive pertains to cyber operations, including those that support or enable kinetic, information, or other types of operations . . . that are reasonably likely to result in 'significant consequences'" to an adversary.

We are informed that "malicious cyber activity" is comprised of "Activities, other than those authorized by or in accordance with US law, that seek to compromise or impair the confidentiality, integrity, or availability of computers, information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon."

In other words, if such activities *are* authorized by the President acting as Commander-in-Chief under the dubious "Unitary Executive" doctrine, like Richard Nixon, Obama now claims that "when the President does it that means that it is not illegal," a novel reading of the US Constitution and the separation of powers as it pertains to declaring and waging war!

"Military actions approved by the President and ordered by the Secretary of Defense authorize nonconsensual DCEO [Defensive Cyber Effects Operations] or OCEO, with provisions made for using existing processes to conduct appropriate interagency coordination on targets, geographic areas, levels of effect, and degrees of risk for the operations."

This has long been spelled out in US warfighting doctrine and is fully consistent with the Pentagon's goal of transforming cyberspace into an offensive military domain. In an Air

Force planning document since removed from the web, theorists averred:

> Cyberspace favors offensive operations. These operations will deny, degrade, disrupt, destroy, or deceive an adversary. Cyberspace offensive operations ensure friendly freedom of action in cyberspace while denying that same freedom to our adversaries. We will enhance our capabilities to conduct electronic systems attack, electromagnetic systems interdiction and attack, network attack, and infrastructure attack operations. Targets include the adversary's terrestrial, airborne, and space networks, electronic attack and network attack systems, and the adversary itself. As an adversary becomes more dependent on cyberspace, cyberspace offensive operations have the potential to produce greater effects. (Air Force Cyber Command, "Strategic Vision," no date)

Those plans were made explicit in 2008, when the Air Force Research Lab issued a Broad Agency Announcement entitled Dominant Cyber Offensive Engagement and Supporting Technology, BAA-08-04-RIKA.

Predating current research under "Plan X" to build "an end-to-end system that enables the military to understand, plan, and manage cyberwarfare in real-time," the earlier notification solicited bids from private military contractors to build cyberweapons.

We learned that the Air Force, now US Cyber Command, the superseding authority in the realm of cyberweapons development, a mandate made explicit in PPD-20, was "interested in technology to provide the capability to maintain an active presence within the adversaries information infrastructure completely undetected. Of interest are any and all techniques to enable stealth and persistence capabilities on an adversaries infrastructure."

"This could be a combination of hardware and/or software focused development efforts."

"Following this," the solicitation read, "it is desired to have the capability to stealthily exfiltrate information from any remotely-located open or closed computer information systems with the possibility to discover information with previously unknown existence."

While the United States has accused China of carrying out widespread espionage on US networks, we know from information Snowden provided the *South China Morning Post*, that NSA and US Cyber Command have conducted "extensive hacking of major telecommunication companies in China to access text messages"; carried out "sustained attacks on network backbones at Tsinghua University, China's premier seat of learning"; and have hacked the "computers at the Hong Kong headquarters of Pacnet, which owns one of the most extensive fibre optic submarine cable networks in the region."

China isn't the only target of US industrial espionage.

Earlier this month, *O Globo* disclosed that "one of the prime targets of American spies in Brazil is far away from the center of power–out at sea, deep beneath the waves. Brazilian oil. The internal computer network of Petrobras, the Brazilian oil giant partly owned by the state, has been under surveillance by the NSA, the National Security Agency of the United States."

Top secret documents mined from the Snowden cache revealed that NSA employees are trained "step-by-step how to access and spy upon private computer networks–the internal

networks of companies, governments, financial institutions–networks designed precisely to protect information."

In addition to Petrobras, "other targets" included "French diplomats–with access to the private network of the Ministry of Foreign Affairs of France–and the SWIFT network, the cooperative that unites over ten thousand banks in 212 countries and provides communications that enable international financial transactions. All transfers of money between banks across national borders goes through SWIFT," *O Globo* disclosed.

The 2008 Air Force solicitation stressed that the service was interested in "any and all techniques to enable exfiltration techniques on both fixed and mobile computing platforms are of interest. Consideration should be given to maintaining a 'low and slow' gathering paradigm in these development efforts to enable stealthy operation."

The Air Force however, was not solely interested in defense or industrial spying on commercial rivals; building offensive capabilities were viewed as a top priority. "Finally," the solicitation reads, "this BAA's objective includes the capability to provide a variety of techniques and technologies to be able to affect computer information systems through Deceive, Deny, Disrupt, Degrade, Destroy (D5) effects."

As *Bloomberg Businessweek* reported in 2011, recipients of that Broad Agency Announcement may have included any number of "boutique arms dealers that trade in offensive cyber weapons. Most of these are 'black' companies that camouflage their government funding and work on classified projects."

"Offensive Cyber Effects Operations" will be enhanced through the development and deployment of software-based weapons; the Obama administration's intent in PPD-20 is clear.

The US government "shall identify potential targets of national importance where OCEO can offer a favorable balance of effectiveness and risk as compared with other instruments of national power, establish and maintain OCEO capabilities integrated as appropriate with other US offensive capabilities, and execute those capabilities in a manner consistent with the provisions of this directive."

Evidence has since emerged these programs are now fully operational.

On the Attack: Economic, Political and Military 'Exploits'

Despite diplomatic posturing and much handwringing from the "humanitarian intervention" crowd, the Obama administration's itchy trigger finger is still poised above the attack Syria button.

The conservative *Washington Free Beacon* web site reported recently that US forces "are expected to roll out new cyber warfare capabilities during the anticipated military strike on Syria," and that the targets of "cyber attacks likely will include electronic command and control systems used by the Syrian military forces, air defense computers, and other military communications networks."

Whether or not that attack takes place, NSA and US Cyber Command are ramping-up their formidable resources and would not hesitate to use them if given the go-ahead.

This raises the question: what capabilities have *already* been rolled out?

"Under an extensive effort code-named GENIE, *The Washington Post* disclosed, "US computer specialists break into foreign networks so that they can be put under surreptitious US control."

According to top secret budget documents provided by Snowden, the *Post* revealed the "$652 million project has placed 'covert implants,' sophisticated malware transmitted from far away, in computers, routers and firewalls on tens of thousands of machines every year, with plans to expand those numbers into the millions."

"Of the 231 offensive operations conducted in 2011," the *Post* reported, "nearly three-quarters were against top-priority targets, which former officials say includes adversaries such as Iran, Russia, China and North Korea and activities such as nuclear proliferation. The document provided few other details about the operations."

As other media outlets previously reported, the *Post* noted that US secret state agencies "are making routine use around the world of government-built malware that differs little in function from the 'advanced persistent threats' that US officials attribute to China."

One firm featured in *Bloomberg Businessweek's* cyberwar exposé is Endgame Systems, which first gained notoriety as a result of the 2011 HBGary Federal hack by Anonymous.

The shadowy firm has received extensive funding from venture capitalists such as Bessemer Venture Partners, Columbia Capital, Kleiner Perkins Caufield & Byers and the intelligence-connected Paladin Capital Group.

Endgame is currently led by CEO Nathaniel Flick, previously the CEO of the "nonpartisan" Center for a New American Security (CNAS), a warmongering Washington think tank focused on "terrorism" and "irregular warfare."

Flick replaced Christopher Rouland, Endgame's founder and CEO in December 2012. A former hacker, Rouland was "turned" by the Air Force during the course of a 1990 investigation where he was suspected of breaking into Pentagon systems, *Businessweek* reported.

The Board of Directors is currently led by Christopher Darby, the President and CEO of the CIA's venture capital arm, In-Q-Tel. Earlier this year, the firm announced that Kenneth Minihan, a former NSA Director and managing partner at Paladin Capital had joined the Board.

According to *Businessweek*, Endgame specializes in militarizing zero-day exploits, software vulnerabilities which take months, or even years for vendors to patch; a valuable commodity for criminals or spooks.

"People who have seen the company pitch its technology," *Businessweek* averred, "say Endgame executives will bring up maps of airports, parliament buildings, and corporate offices. The executives then create a list of the computers running inside the facilities, including what software the computers run, and a menu of attacks that could work against those particular systems."

While the United States has accused the Technical Reconnaissance Bureau of China's

People's Liberation Army of launching attacks and stealing economic secrets from US networks, American cyberoperations involve "what one budget document calls 'field operations' abroad, commonly with the help of CIA operatives or clandestine military forces, 'to physically place hardware implants or software modifications,'" according to *The Washington Post*.

"Endgame weaponry comes customized by region–the Middle East, Russia, Latin America, and China–with manuals, testing software, and 'demo instructions.'"

"There are even target packs for democratic countries in Europe and other US allies," *Businessweek* noted.

Readers will recall that Snowden documents have exposed how NSA has carried out widespread economic and political espionage against erstwhile "friends and allies" such as Brazil, France, Germany, India, the European Union and the United Nations.

Add to that list, Endgame exploits which are solely military in nature; in all probability these have been incorporated into NSA and US Cyber Command's repertoire of dirty tricks.

"Maui (product names tend toward alluring warm-weather locales) is a package of 25 zero-day exploits that runs clients $2.5 million a year," *Businessweek* reported. "The Cayman botnet-analytics package gets you access to a database of Internet addresses, organization names, and worm types for hundreds of millions of infected computers, and costs $1.5 million."

"A government or other entity could launch sophisticated attacks against just about any adversary anywhere in the world for a grand total of $6 million. Ease of use is a premium. It's cyber warfare in a box."

Sound familiar?

"An implant is coded entirely in software by an NSA group called Tailored Access Operations (TAO)," Snowden documents revealed. "As its name suggests, TAO builds attack tools that are custom-fitted to their targets," according to *The Washington Post*.

"The implants that TAO creates are intended to persist through software and equipment upgrades, to copy stored data, 'harvest' communications and tunnel into other connected networks" the *Post* disclosed.

"This year TAO is working on implants that 'can identify select voice conversations of interest within a target network and exfiltrate select cuts,' or excerpts, according to one budget document. In some cases, a single compromised device opens the door to hundreds or thousands of others."

This does much to explain why NSA's parallel, $800 million SIGINT Enabling Project stresses the importance of obtaining total global access and "full operating capacity" that can "leverage commercial capabilities to remotely deliver or receive information."

With "boutique arms dealers" and others from more traditional defense giants along for the ride, NSA and US Cyber Command hope their investment will help "shape the global network to benefit other collection accesses and allow the continuation of partnering with commercial Managed Security Service Providers and threat researchers, doing

threat/vulnerability analysis."

"By the end of this year," the *Post* noted, "GENIE is projected to control at least 85,000 implants in strategically chosen machines around the world. That is quadruple the number–21,252–available in 2008, according to the US intelligence budget."

The agencies are now poised to expand the number of machines already compromised. "For GENIE's next phase, according to an authoritative reference document," the *Post* disclosed, "the NSA has brought online an automated system, code-named TURBINE, that is capable of managing 'potentially millions of implants' for intelligence gathering 'and active attack'."

It should be clear, given what we have learned from Edward Snowden and other sources, that the US government views the internet, indeed the entire planet, as a battlespace.

In congressional testimony earlier this year, General Alexander told the House Armed Services Committee that "Cyber offense requires a deep, persistent and pervasive presence on adversary networks in order to precisely deliver effects."

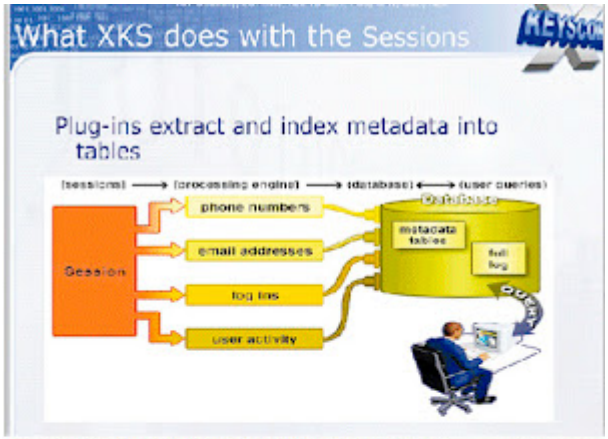
"We maintain that access, gain deep understanding of the adversary, and develop offensive capabilities through the advanced skills and tradecraft of our analysts, operators and developers."

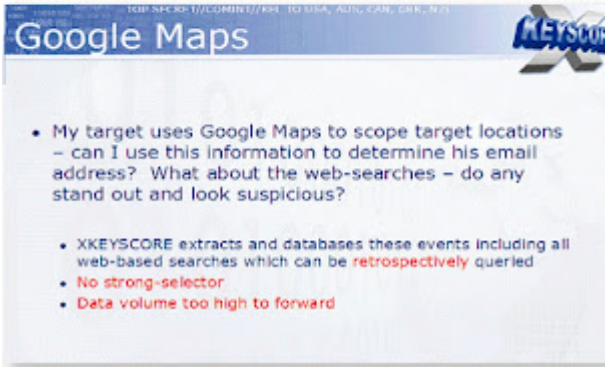
With US Cyber Command fully funded and mobilized, those "offensive capabilities" are only a mouse click away.

Posted by Antifascist at 3:55 PM No comments:
Labels: Cyber War, Encryption, NSA, Obama, Pentagon, Private Military Contractors, Secret State, Spying on Americans, Spying on the World, Surveillance, US Cyber Command, Whistleblowing

Sunday, July 28, 2013

'Big Data' Dynamo: How Giant Tech Firms Help the Government Spy on Us and Gut Privacy





As the secret state continues trawling the electronic communications of hundreds of millions of Americans, lusting after what securocrats euphemistically call "actionable intelligence," a notional tipping point that transforms a "good" citizen into a "criminal" suspect, the role played by telecommunications and technology firms cannot be emphasized enough.

Ever since former NSA contractor Edward Snowden began leaking secrets to media outlets about government surveillance programs, one fact stands out: The *zero probability* these privacy-killing projects would be practical without close (and very profitable) "arrangements" made with phone companies, internet service providers and other technology giants.

Indeed, a top secret NSA Inspector General's report published by *The Guardian*, revealed that the agency "maintains relationships with over 100 US companies," adding that the US has the "home field advantage as the primary hub for worldwide telecommunications."

Similarly, the British fiber optic cable tapping program, TEMPORA, referred to telcos and ISPs involved in the spying as "intercept partners." The names of the firms were considered so sensitive that GCHQ "went to great lengths" to keep their identities hidden, fearing exposure "would cause 'high-level political fallout'."

With new privacy threats looming on the horizon, including what CNET described as ongoing efforts by the FBI and NSA "to obtain the master encryption keys that Internet companies use to shield millions of users' private Web communications from eavesdropping," along with new government demands that ISPs and cell phone carriers "divulge users' stored passwords," can we trust these firms?

And with Microsoft and other tech giants, collaborating closely with "US intelligence services to allow users' communications to be intercepted, including helping the National Security Agency to circumvent the company's own encryption," can we afford to?

Hiding in Plain Sight

Ever since retired union technician Mark Klein blew the lid off AT&T's secret surveillance pact with the US government in 2006, we know user privacy is *not* part of that firm's business model.

The technical source for the Electronic Frontier Foundation's lawsuit, *Hepting v. AT&T* and the author of *Wiring Up the Big Brother Machine*, Klein was the first to publicly expose how NSA was "vacuuming up everything flowing in the Internet stream: e-mail, web browsing, Voice-Over-Internet phone calls, pictures, streaming video, you name it."

We also know from reporting by *USA Today*, that the agency "has been secretly collecting the phone call records of tens of millions of Americans" and had amassed "the largest database ever assembled in the world."

Three of those data-slurping programs, UPSTREAM, PRISM and X-KEYSCORE, shunt domestic and global communications collected from fiber optic cables, the servers of Apple, Google, Microsoft and Yahoo, along with telephone data (including metadata, call content and location) grabbed from AT&T, Sprint and Verizon into NSA-controlled databases.

But however large, a database is only useful to an organization, whether its a corporation or a spy agency, if the oceans of data collected can be searched and extracted in meaningful ways.

To the growing list of spooky acronyms and code-named black programs revealed by Edward Snowden, what *other* projects, including those in the public domain, are hiding in plain sight?

Add Google's BigTable and Yahoo's Hadoop to that list. Both are massive storage and retrieval systems designed to crunch ultra-large data sets and were developed as a practical means to overcome "big data" conundrums.

According to the Mountain View behemoth, "BigTable is a distributed storage system for managing structured data that is designed to scale to a very large size: petabytes of data across thousands of commodity servers." Along with web indexing, Google Earth and Google Finance, BigTable performs "bulk processing" for "real-time data serving."

Down the road in Sunnyvale, Yahoo developed Hadoop as "an open source Java framework for processing and querying vast amounts of data on large clusters of commodity hardware." According to Yahoo, Hadoop has become "the industry *de facto* framework for big data processing." Like Google's offering, Hadoop enable applications to work with thousands of computers and petabytes of data simultaneously.

Prominent corporate clients using these applications include Amazon, AOL, eBay, Facebook, IBM, Microsoft and Twitter, among many others.

'Big Data' Dynamo

Who might *also* have a compelling interest in cataloging and searching through very large data sets, away from prying eyes, and at granular levels to boot? It should be clear following Snowden's disclosures, what's good for commerce is also a highly-prized commodity among global eavesdroppers.

Despite benefits for medical and scientific researchers sifting through mountains of data, as *Ars Technica* pointed out BigTable and Hadoop "lacked compartmentalized security" vital to spy shops, so "in 2008, NSA set out to create a better version of BigTable, called Accumulo."

Developed by agency specialists, it was eventually handed off to the "non-profit" Apache Software Foundation. Touted as an open software platform, Accumulo is described in Apache literature as "a robust, scalable, high performance data storage and retrieval system."

"The platform allows for compartmentalization of segments of big data storage through an approach called cell-level security. The security level of each cell within an Accumulo table can be set independently, hiding it from users who don't have a need to know: whole sections of data tables can be hidden from view in such a way that users (and applications) without clearance would never know they weren't there," *Ars Technica* explained.

The tech site *Gigaom* noted, Accumulo is the "technological linchpin to everything the NSA is doing from a data-analysis perspective," enabling agency analysts to "generate near real-time reports from specific patterns in data," *Ars* averred.

"For instance, the system could look for specific words or addressees in e-mail messages that come from a range of IP addresses; or, it could look for phone numbers that are two degrees of separation from a target's phone number. Then it can spit those chosen e-mails or phone numbers into another database, where NSA workers could peruse it at their leisure."

(Since that *Ars* piece appeared, we have since learned that NSA is now conducting what is described as "three-hop analysis," that is, *three degrees of separation* from a target's email or phone number. This data dragnet "could allow the government to mine the records of 2.5 million Americans when investigating one suspected terrorist," the *Associated Press* observed).

"In other words," *Ars* explained, "Accumulo allows the NSA to do what Google does with your e-mails and Web searches–only with everything that flows across the Internet, or with every phone call you make."

Armed with a "dual-use" program like Accumulo, the dirty business of assembling a user's political profile, or shuttling the names of "suspect" Americans into a national security index, is as now easy as downloading a song from iTunes!

And it isn't only Silicon Valley giants cashing-in on the "public-private" spy game.

Just as the CIA-funded Palantir, a firm currently valued at $8 billion and exposed two years ago as a "partner" in a Bank of America-brokered scheme to bring down WikiLeaks, profited from CIA interest in its social mapping Graph application, so too, the NSA spin-off Sqrrl, launched in 2012 with agency blessings, stands to make a killing off software its corporate officers helped develop for NSA.

Co-founded by nine-year agency veteran Adam Fuchs, Sqrrl sells commercial versions of Accumulo and has partnered-up with Amazon, Dell, MapR and Northrop Grumman. According to published reports, like other start-ups with an intelligence angle, Sqrrl is hoping to hook-up with CIA's venture capital arm In-Q-Tel.

Its obvious why the application is of acute interest to American spy shops. Fuchs told *Gigaom* that Accumulo operates "at thousands-of-nodes scale" within NSA data centers.

"There are multiple instances each storing tens of petabytes (1 petabyte equals 1,000 terabytes or 1 million gigabytes) of data and it's the backend of the agency's most widely used analytical capabilities."

Accumulo's analytical functions work because of its ability to perform lightning-quick searches called "graph analysis," a method for uncovering unique relationships between people hidden within vast oceans of data.

According to *Forbes*, "we know that the NSA has successfully tested Accumulo's graph analysis capabilities on some huge data sets–in one case on a 1200 node Accumulo cluster with over a petabyte of data and 70 trillion edges."

Considering, as *Wired* reported, that "on an average day, Google accounts for about 25 percent of all consumer internet traffic running through North American ISPs," and the Mountain View firm allowed the FBI and NSA to tap directly into their central servers as *The Washington Post* disclosed, the negative impact on civil rights and political liberties when systems designed for the Pentagon are monetized, should be evident.

Once fully commercialized, how much more intrusive will employers, marketing firms, insurance companies or local and state police with mountains of data only a mouse click away, become?

Global Panopticon

The sheer scope of NSA programs such as UPSTREAM, PRISM or X-KEYSCORE, exposed by the Brazilian daily, *O Globo* should give pause.

A crude illustration (at the top of this post), shows that all data collected in X-KEYSCORE "sessions" are processed in petabyte scale batches captured from "web-based searches" that can be "retrospectively" queried to locate and profile a "target."

This requires enormous processing power; a problem the agency *may* have solved with Accumulo or similar applications.

Once collected, data is separated into digestible fragments (phone numbers, email addresses and log ins), then reassembled at lightning speeds for searchable queries in graphic form. Information gathered in the hopper includes not only metadata tables, but the "full log," including what spooks call Digital Network Intelligence, i.e., user content.

And while it may not *yet* be practical for NSA to collect and store each single packet flowing through the pipes, the agency is *already* collecting and storing vast reams of data intercepted from our phone records, IP addresses, emails, web searches and visits, and is doing so in much the same way that Amazon, eBay, Google and Yahoo does.

As the volume of global communications increase each year at near exponential levels, data storage and processing pose distinct problems.

Indeed, Cisco Systems forecast in their 2012 Visual Networking Index that global IP traffic will grow three-fold over the next five years and will carry up to 4 exabytes of data per day,

for an annual rate of 1.4 zettabytes by 2017.

This does much to explain why NSA is building a $2 billion Utah Data Center with 22 acres of digital storage space that can hold up to 5 zettabytes of data and expanding already existing centers at Fort Gordon, Lackland Air Force Base, NSA Hawaii and at the agency's Fort Meade headquarters.

Additionally, NSA is feverishly working to bring supercomputers online "that can execute a quadrillion operations a second" at the Multiprogram Research facility in Oak Ridge, Tennessee where enriched uranium for nuclear weapons is manufactured, as James Bamford disclosed last year in *Wired*.

As the secret state sinks tens of billions of dollars into various big data digital programs, and carries out research on next-gen cyberweapons more destructive than Flame or Stuxnet, as those supercomputers come online the cost of cracking encrypted passwords and communications will continue to fall.

Stanford University computer scientist David Mazières told CNET that mastering encrypted communications would "include an order to extract them from the server or network when the user logs in–which has been done before–or installing a keylogger at the client."

This is *precisely* what Microsoft has already done with its SkyDrive cloud storage service "which now has 250 million users worldwide" and exabytes of data ready to be pilfered, as *The Guardian* disclosed.

One document "stated that NSA already had pre-encryption access to Outlook email. 'For Prism collection against Hotmail, Live, and Outlook.com emails will be unaffected because Prism collects this data prior to encryption'."

Call the "wrong" person or click a dodgy link and you might just be the lucky winner of a one-way trip to indefinite military detention under NDAA, or worse.

What should also be clear since revelations about NSA surveillance programs began spilling out last month, is not a single ruling class sector in the United States–including corporations, the media, nor any branch of the US government–has the least interest in defending democratic rights or rolling-back America's emerging police state.

Articles by: Tom Burghardt
http://antifascist-calling.blogspot.com/