GlobalResearch
Centre for Research on Globalization
globalresearch.ca / globalresearch.org

ECHELON Today: The Evolution of an NSA Black Program

By Tom Burghardt
Global Research, July 13, 2013

People are shocked by the scope of secret state spying on their private communications, especially in light of documentary evidence leaked to media outlets by former NSA contractor Edward Snowden.

While the public is rightly angered by the illegal, unconstitutional nature of NSA programs which seize and store data for retrospective harvesting by intelligence and law enforcement officials, including the content of phone calls, emails, geolocational information, bank records, credit card purchases, travel itineraries, even medical records–in secret, and with little in the way of effective oversight–the historical context of how, and why, this vast spying apparatus came to be is often given short shrift.

Revelations about NSA spying didn't begin June 5, 2013 however, the day when *The Guardian* published a top secret FISA Court Order to Verizon, ordering the firm turn over the telephone records on millions of its customers "on an ongoing daily basis."

Before PRISM there was ECHELON: the top secret surveillance program whose all-encompassing "dictionaries" (high-speed computers powered by complex algorithms) ingest and sort key words and text scooped-up by a global network of satellites, from undersea cables and land-based microwave towers.

Past as Prologue

Confronted by a dizzying array of code-named programs, the casual observer will assume the spymasters running these intrusive operations are all-knowing mandarins with their fingers on the pulse of global events.

Yet, if disastrous US policies from Afghanistan and Iraq to the ongoing capitalist economic meltdown tell us anything, it is that the American superpower, in President Nixon's immortal words, really is "a pitiful, helpless giant."

In fact, the same programs used to surveil the population at large have also been turned inward by the National Security State against itself and targets military and political elites who long thought themselves immune from such close attention.

Coupled with Snowden's disclosures, those of former NSA officer Russell Tice (first reported here [www.boilingfrogspost.com/2013/06/19/podcast-show-112-nsa-whistleblower-goes-on-record-reveals-new-information-names-culprits/] and here [www.corbettreport.com/interview-685-russ-tice-reveals-the-truth-about-nsa-spying/]), revealed that the agency–far in excess of the dirt collected by FBI spymaster J. Edgar Hoover in his "secret and confidential" black files–

has compiled dossiers on their alleged controllers, for political leverage and probably for blackmail purposes to boot.

While Tice's allegations certainly raised eyebrows and posed fundamental questions about who is really in charge of American policy–elected officials or unaccountable securocrats with deep ties to private security corporations–despite being deep-sixed by US media, they confirm previous reporting about the agency.

When investigative journalist Duncan Campbell first blew the lid off NSA's ECHELON program, his 1988 piece for *New Statesman* [cryptome.org/jya/echelon-dc.htm] revealed that a whistleblower, Margaret Newsham, a software designer employed by Lockheed at the giant agency listening post at Menwith Hill in North Yorkshire, England, stepped forward and told the House Permanent Select Committee on Intelligence in closed session, that NSA was using its formidable intercept capabilities "to locate the telephone or other messages of target individuals."

Campbell's reporting was followed in 1996 by New Zealand investigative journalist Nicky Hager's groundbreaking book, *Secret Power* [www.nickyhager.info/secret-power-new-zealands-role-in-the-international-spy-network/], the first detailed account of NSA's global surveillance system. A summary of Hager's findings can be found in the 1997 piece that appeared in *CovertAction Quarterly* [www.nickyhager.info/exposing-the-global-surveillance-system/].

As Campbell was preparing that 1988 article, a report in the *Cleveland Plain Dealer* alleged that arch-conservative US Senator Strom Thurman was one target of agency phone intercepts, raising fears in political circles that "NSA has restored domestic, electronic, surveillance programmes," said to have been dialed-back in the wake of the Watergate scandal.

Ironically enough, congressional efforts to mitigate abuses by the intelligence agencies exposed by the Church and Pike Committees in the 1970s, resulted in the 1978 creation of the Foreign Intelligence Surveillance Court. However, as *The New York Times* [www.nytimes.com/2013/07/07/us/in-secret-court-vastly-broadens-powers-of-nsa.html] reported July 7, that court "in more than a dozen classified rulings . . . has created a secret body of law giving the National Security Agency the power to amass vast collections of data on Americans," a "parallel Supreme Court" whose rulings are beyond legal challenge.

In an 88-page report on ECHELON published in 2000 by the Electronic Privacy Information Center (EPIC) [www.duncancampbell.org/menu/surveillance/echelon/EPIC_report.pdf] Newsham said that when she worked on the development of SILKWORTH at the secret US base, described as "a system for processing information relayed from signals intelligence satellites," she told Campbell and other reporters, including CBS News' *60 Minutes* [cryptome.org/echelon-60min.htm], that "she witnessed and overheard" one of Thurman's intercepted phone calls.

Like Thomas Drake, the senior NSA official prosecuted by the Obama administration under the 1917 Espionage Act, for information he provided *The Baltimore Sun* [articles.baltimoresun.com/2006-01-29/news/0601290158_1_saic-information-technology-intelligence-experts] over widespread waste, fraud and abuse in the agency's failed Trailblazer program, Newsham had testified before Congress and filed a lawsuit against Lockheed over charges of sexual harassment, "corruption and mis-spending on other US government 'black' projects."

A year earlier, in a 1999 on the record interview with the Danish newspaper *Ekstra Bladet* [www.mail-archive.com/kominform@lists.eunet.fi/msg00493.html], Newsham spoke to journalists Bo Elkjaer and Kenan Seeberg, telling them of her "constant fear" that "certain elements" within the US secret state would "try to silence her"; a point not lost on Edward Snowden today.

"As a result," the newspaper reported, "she sleeps with a loaded pistol under her mattress, and her best friend is Mr. Gunther–a 120-pound German shepherd that was trained to be a guard and attack dog by a good friend in the Nevada State Police."

"To me," the whistleblower said, "there are only two issues at stake here: right or wrong. And the longer I worked on the clandestine surveillance projects, the more I could see that they were not only illegal, but also unconstitutional."

"Even then," between 1974 and 1984 when she worked on ECHELON, it "was very big and sophisticated."

"As early as 1979 we could track a specific person and zoom in on his phone conversation while he was communicating," Newsham averred. "Since our satellites could in 1984 film a postage stamp lying on the ground, it is almost impossible to imagine how all-encompassing the system must be today."

When queried about "which part of the system is named Echelon," Newsham told the reporters: "The computer network itself. The software programs are known as SILKWORTH and SIRE, and one of the most important surveillance satellites is named VORTEX. It intercepts things like phone conversations."

Despite evidence presented in her congressional testimony about these illegal operations, "no substantive investigation took place, and no report was made to Congress," Campbell later wrote.

"Since then," the British journalist averred, "investigators have subpoenaed other witnesses and asked them to provide the complete plans and manuals of the ECHELON system and related projects. The plans and blueprints are said to show that *targeting of US political figures would not occur by accident, but was designed into the system from the start*." (emphasis added)

This would explain why members of Congress, the federal Judiciary and the Executive Branch itself, as Tice alleges, tread lightly when it comes to crossing NSA. However, as information continues to emerge about these privacy-killing programs it should also be clear that the agency's prime targets are not "terrorists," judges or politicians, but the American people themselves.

In fact, as Snowden stated in a powerful message published by WikiLeaks [wikileaks.org/Statement-from-Edward-Snowden-in.html]: "In the end the Obama administration is not afraid of whistleblowers like me, Bradley Manning or Thomas Drake. We are stateless, imprisoned, or powerless. No, the Obama administration is afraid of you. It is afraid of an informed, angry public demanding the constitutional government it was promised–and it should be."

How did we get here? Is there a direct line from Cold War-era programs which targeted the Soviet Union and their allies, and which now, in the age of capitalist globalization, the epoch of planet-wide theft and plunder, now targets the entire world's population?

ECHELON's Roots: The UKUSA Agreement

Lost in the historical mists surrounding the origins of the Cold War, the close collaboration amongst Britain and the United States as they waged war against Nazi Germany and Imperial Japan, by war's end had morphed into a permanent intelligence-military alliance which predated the founding of NATO. With the defeat of the Axis powers, a new global division of labor was in the offing led by the undisputed superpower which emerged from the conflagration, the United States.

Self-appointed administrator over Europe's old colonial holdings across Africa, Asia and the Middle East (the US already viewed Latin America as its private export dumping ground and source for raw materials), the US used its unparalleled position to benefit the giant multinational American firms grown larger and more profitable than ever as a result of wartime economic mobilization managed by the state.

By 1946, the permanent war economy which later came to be known as the Military-Industrial Complex, a semi-command economy directed by corporate executives, based on military, but also on emerging high-tech industries bolstered by taxpayer-based government investments, was already firmly entrenched and formed the political-economic base on which the so-called "American Century" was constructed.

While resource extraction and export market domination remained the primary goal of successive US administrations (best summarized by the slogan, "the business of government is business"), advances in technology in general and telecommunications in particular, meant that the system's overlords required an intelligence apparatus that was always "on" as it "captured" the flood of electronic signals coursing across the planet.

The secret British and US agencies responsible for cracking German, Japanese and Russian codes during the war found themselves in a quandary. Should they declare victory and go home or train their sights on the new (old) adversary–their former ally, the Soviet Union–but also on home grown and indigenous communist and socialist movements more generally?

In opting for the latter, the UK-US wartime partnership evolved into a broad agreement to share signals and communications intelligence (SIGINT and COMINT), a set-up which persists today.

In 1946, Britain and the United States signed the United Kingdom-United States of America Agreement (UKUSA), a multilateral treaty to share signals intelligence amongst the two nations and Britain's Commonwealth partners, Canada, Australia and New Zealand. Known as the "Five Eyes" agreement, the treaty was such a closely-guarded secret that Australia's Prime Minister was kept in the dark until 1973!

In 2010, the British National Archives [www.nationalarchives.gov.uk/ukusa/] released previously classified Government Communications Headquarters (GCHQ) files that provide an important historical overview of the agreement. Also in 2010, the National Security Agency followed suit and published formerly classified files [www.nsa.gov/public_info/declass/ukusa.shtml] from their archives. Accompanying NSA's release was a 1955 amended version [www.nsa.gov/public_info/_files/ukusa/new_ukusa_agree_10may55.pdf] of the treaty.

It's secretive nature is clearly spelled out: "It will be contrary to this Agreement to reveal its existence to any third party unless otherwise agreed by the two parties."

In 2005 [www.gwu.edu/%7Ensarchiv/NSAEBB/NSAEBB24/index.htm], 2009 [www.gwu.edu/%7Ensarchiv/NSAEBB/NSAEBB278/index.htm] and 2013 [www.gwu.edu/%7Ensarchiv/NSAEBB/NSAEBB424/], The National Security Archive [www.gwu.edu/%7Ensarchiv/index.html] published a series of previously classified documents obtained from NSA under the Freedom of Information Act that revealed agency thinking on a range of subjects, from global surveillance to cyberwar.

What we have learned from these sources and reporting by Duncan Campbell and Nicky Hager, are that the five agencies feeding the surveillance behemoth, America's NSA, Britain's GCHQ, Canada's Communications Security Establishment (CSE), Australia's Defence Signals Directorate (DSD) and New Zealand's Government Communications Security Bureau (GCSB), are subdivided into first and second tier partners, with the US, as befitting a hyperpower, forming the "1st party" and the UK, Australia, Canada and New Zealand forming "2nd party" partners.

Under terms of UKUSA, intelligence "products" are defined as "01. Collection of traffic. 02. Acquisition of communications documents and equipment. 03. Traffic analysis. 04. Cryptanalysis. 05. Decryption and translation. 06. Acquisition of information regarding communications organizations, procedures, practices and equipment."

"Such exchange," NSA informed us, "will be unrestricted on all work undertaken except when specifically excluded from the agreement at the request of either party and with the agreement of the other."

"It is the intention of each party," we're told, "to limit such exceptions to the absolute minimum and to exercise no restrictions other than those reported and mutually agreed upon."

This certainly leaves wide latitude for mischief as we learned with the Snowden disclosures.

Amid serious charges that "Five Eyes" were illegally seizing industrial and trade secrets from "3rd party" European partners such as France and Germany, detailed in the European Parliament's 2001 ECHELON report [www.duncancampbell.org/menu/surveillance/echelon/EU_resolution.pdf], it should be clear by now that since its launch in 1968 when satellite communications became a practical reality, ECHELON has evolved into a global surveillance complex under US control.

The Global Surveillance System Today

The echoes of those earlier secret programs reverberate in today's headlines.

Last month, *The Guardian* [www.guardian.co.uk/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa] reported that the "collection of traffic" cited in UKUSA has been expanded to GCHQ's "ability to tap into and store huge volumes of data drawn from fibre-optic cables for up to 30 days so that it can be sifted and analysed. That operation, codenamed Tempora, has been running for some 18 months."

Then on July 6, *The Washington Post* [www.washingtonpost.com/business/technology/agreements-with-private-companies-protect-us-

access-to-cables-data-for-surveillance/2013/07/06/aa5d017a-df77-11e2-b2d4-ea6d8f477a01_print.html] disclosed that NSA has tapped directly into those fiber optic cables, as AT&T whistleblower Mark Klein described to *Wired Magazine* in 2006 [www.wired.com/science/discoveries/news/2006/05/70944], and now scoops-up *petabyte scale* communications flowing through the US internet backbone. The agency was able to accomplish this due to the existence of "an internal corporate cell of American citizens with government clearances."

"Among their jobs documents show, was ensuring that surveillance requests got fulfilled quickly and confidentially."

Following up on July 10, the *Post* [www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/32801426-e8e6-11e2-aa9f-c03a72e2d342_story.html] published a new PRISM slide from the 41-slide deck provided to the paper by Edward Snowden.

The slide revealed that "two types of collection" now occur. One is the PRISM program that collects information from technology firms such as Google, Apple and Microsoft. The second source is "a separate category labeled 'Upstream,' described as accessing 'communications on fiber cables and infrastructure as data flows past'."

Recently, *Der Spiegel* [www.spiegel.de/international/world/secret-documents-nsa-targeted-germany-and-eu-buildings-a-908609-druck.html], reported that NSA averred the agency "does NOT target its 2nd party partners, nor request that 2nd parties do anything that is inherently illegal for NSA to do." This is an outright falsehood exposed by former Canadian Communications Security Establishment (CSE) officer Mike Frost.

In a 1997 *CovertAction Quarterly* exposé, Frost recounted how "CSE operated alone or joined with NSA or GCHQ to: intercept communications in other countries from the confines of Canadian embassies around the world with the knowledge of the ambassador; aid politicians, political parties, or factions in an allied country to gain partisan advantage; spy on its allies; spy on its own citizens; and perform 'favors' that helped its allies evade domestic laws against spying."

"Throughout it all," Frost insisted, "I was trained and controlled by US intelligence which told us what to do and how to do it."

Everyone else, *Der Spiegel* reports, is fair game. "For all other countries, including the group of around 30 nations that are considered to be 3rd party partners, however, this protection does not apply. 'We can, and often do, target the signals of most 3rd party foreign partners,' the NSA boasts in an internal presentation."

It should also be clear that targeting isn't strictly limited to the governments and economic institutions of "3rd party foreign partners," but extends to the private communications of their citizens. *Der Spiegel*, citing documents supplied by Snowden, reported that the agency "gathered metadata from some 15 million telephone conversations and 10 million Internet datasets." The newsmagazine noted that "the Americans are collecting from up to half a billion communications a month in Germany," describing the surveillance as "a complete structural acquisition of data."

Despite hypocritical protests by European governments, on the contrary, Snowden disclosed that those "3rd party" partners are joined at the hip with their "Five Eyes" cousins.

In a recent interview with *Der Spiegel* [www.spiegel.de/international/world/interview-with-whistleblower-edward-snowden-on-global-spying-a-910006-druck.html], Snowden was asked if "German authorities or German politicians [are] involved in the NSA surveillance system?"

"Yes, of course. We're in bed together with the Germans the same as with most other Western countries. For example, we tip them off when someone we want is flying through their airports (that we for example, have learned from the cell phone of a suspected hacker's girlfriend in a totally unrelated third country–and they hand them over to us. They don't ask to justify how we know something, and vice versa, to insulate their political leaders from the backlash of knowing how grievously they're violating global privacy."

Disclosing new information on how UKUSA functions today, Snowden told the German newsmagazine: "In some cases, the so-called Five Eye Partners go beyond what NSA itself does. For instance, the UK's General [sic] Communications Headquarters (GCHQ) has a system called TEMPORA."

"TEMPORA," the whistleblower averred, "is the signals intelligence community's first 'full-take' Internet buffer that doesn't care about content type and pays only marginal attention to the Human Rights Act. It snarfs everything, in a rolling buffer to allow retroactive investigation without missing a single bit."

"Right now," Snowden said, "the buffer can hold three days of traffic, but that's being improved. Three days may not sound like much, but remember that that's not metadata. 'Full-take' means it doesn't miss anything, and ingests the entirety of each circuit's capacity. If you send a single ICMP packet and it routes through the UK, we get it. If you download something and the CDN (Content Delivery Network) happens to serve from the UK, we get it. If your sick daughter's medical records get processed at a London call center . . . well, you get the idea."

We do; and thanks to Edward Snowden we now know that everyone is a target.