Leaked documents expose secret contracts between NSA and tech companies

Thomas Gaist
20 October 2014

Internal National Security Agency documents published by the *Intercept* earlier this month provide powerful evidence of active collaboration by the large technology corporations with the US government's worldwide surveillance operations. The documents give a glimpse of efforts by the American state—the scale and complexity of which are astonishing—to penetrate, surveil and manipulate information systems around the world.

Reportedly leaked by whistleblower Edward Snowden, the documents catalogue a dizzying array of clandestine intelligence and surveillance operations run by the NSA, CIA and other US and allied security bureaucracies, including infiltration of undercover agents into corporate entities, offensive cyber-warfare and computer network exploitation (CNE), theoretical and practical aspects of encryption cracking, and supply chain interdiction operations that "focus on modifying equipment in a target's supply chain."

The trove of documents, made available in their original forms by the *Intercept* , are largely comprised of classification rubrics that organize NSA secrets according to a color-coded scale ranging from green (lowest priority secrets), through blue and red, to black (highest priority secrets).

The secret facts organized in the leaked classification guides supply overwhelming evidence that the NSA and Central Security Service (a 25,000-strong agency founded in 1972 as a permanent liaison between the NSA and US military intelligence) rely on cooperative and in some cases contractual relations with US firms to facilitate their global wiretapping and data stockpiling activities.

Blue level facts listed in the documents include:

* "Fact that NSA/CSS works with US industry in the conduct of its cryptologic missions"

* "Fact that NSA/CSS works with US industry as technical advisors regarding cryptologic products"

Red level facts include:

* "Fact that NSA/CSS conducts SIGINT enabling programs and related operations with US industry"

* "Fact that NSA/CSS have FISA operations with US commercial industry elements"

Black level facts include:

* "Fact that NSA/CSS works with and has contractual relationships with specific named US commercial entities to conduct SIGINT [signals intelligence] enabling programs and operations"

* "Fact that NSA/CSS works with specific named US commercial entities to make them exploitable for SIGINT"

* "Facts related to NSA personnel (under cover), operational meetings, specific operations, specific technology, specific locations and covert communications related to SIGINT enabling with specific commercial entities"

* "Facts related to NSA/CSS working with US commercial entities on the acquisition of communications (content and metadata) provided by the US service provider to worldwide customers; communications transiting the US; or access to international communications mediums provided by the US entity"

* "Fact that NSA/CSS injects 'implants' into the hardware and software of US companies to enable data siphoning"

Particularly damning are facts reported by a leaked classification schema detailing operation "Exceptionally Controlled Information (ECI) WHIPGENIE," described in the document's introduction as covering NSA "Special Source Operations relationships with US Corporate Partners."

According to the ECI WHIPGENIE document, unnamed "corporate partners" facilitate NSA mass surveillance as part of undisclosed "contractual relations," through which "NSA and Corporate Partners are involved in SIGINT 'cooperative efforts."'

Among the classified TOP SECRET items listed in the ECI WHIPGENIE document is the fact that "NSA and an unnamed Corporate Partner are involved in a 'cooperative effort' against cable collection, including domestic wire access collection."

As part of WHIPGENIE, the document further states, the FBI facilitates NSA partnerships with industry that are both "compelled and cooperative" in nature. In other words, the NSA carries out domestic wiretapping and "cable collection" operations with the cooperation of at least one US corporation.

These revelations are especially significant in light of persistent claims by the major tech and communications corporations that their involvement in the surveillance operations is strictly involuntary in nature.

Last year, a leaked NSA PowerPoint presentation titled "Corporate Partner Access" showed that the volume of data transferred to the agency by Yahoo, Google, and Microsoft during a single 5-week period was sufficient to generate more than 2,000 intelligence reports. The companies all defended their actions by claiming they were forced to furnish data by the government.

Other documents contained in the trove detail the NSA's development of sophisticated offensive cyber-warfare capabilities targeting the information systems of foreign corporations and governments. These programs highlight the threat of outbreaks of electronic warfare between competing capitalist elites, which could provide the spark for full-fledged shooting wars.

One document, titled "Computer Network Exploitation Classification Guide," states that NSA, CSS and the NSA's in-house hacker unit, the so-called Tailored Access Operations (TAO), engage in "remote subversion" as well as "off-net field operations to develop, deploy, exploit or maintain intrusive access."

Another classification guide, titled "NSA / CSS Target Exploitation Program," covers target exploitation operations (TAREX), which are said to "provide unique collection of telecommunication and cryptologic-related information and material in direct support of NSA / CSS."

TAREX also involves "physical subversion," "close access-enabling exploitation," and "supply chain enabling," the document shows, through which the surveillance agencies intervene directly to modify and sabotage the information systems of rival states.

TAREX operations are supported by outposts located in Beijing, China, South Korea, Germany, Washington DC, Hawaii, Texas and Georgia, and TAREX personnel are "integrated into the HUMINT [human intelligence] operations at CIA, DIA/DoD, and/or FBI," according to the document.

On top of the electronic surveillance, infiltration and cyber-warfare operations themselves, the intelligence establishment has launched a slate of secondary operations designed to protect the secrecy of its various initiatives, as shown in another leaked document, titled "Exceptionally Controlled Information Listing."

These include:

* AMBULANT, APERIODIC, AUNTIE—"Protect information related to sensitive SIGINT Enabling relationships"

* BOXWOOD—"Protects a sensitive sole source of lucrative communications intelligence emanating from a target"

* CHILLY—"Protects details of NSA association with and active participation in planning and execution of sensitive Integrated Joint Special Technical Operations (IJSTO) offensive Information Warfare strategies"

* EVADEYIELD—"Protects NSA's capability to exploit voice or telephonic conversations from an extremely sensitive source"

* FORBIDDEN—"Protects information pertaining to joint operations conducted by NSA, GCHQ, CSE, CIA, and FBI against foreign intelligence agents"

* FORBORNE—"Protects the fact that the National Security Agency, GCHQ, and CSE can exploit ciphers used by hostile intelligence services"

* OPALESCE —"Protects Close Access SIGINT collection operations, which require a specialized sensor, positioned in close physical proximity to the target or facility"

* PENDLETON—"Protects NSA's investment in manpower and resources to acquire our current bottom line capabilities to exploit SIGINT targets by attacking public key cryptography as well as investment in technology"

* PIEDMONT—"Provides protection to NSA's bottom line capabilities to exploit SIGINT targets by attacking the hard mathematical problems underlying public key cryptography as well as any future technologies as may be developed"

* And others…

The number and character of the NSA's "protection" programs gives an indication of the scope of its activities.

The latest round of leaked NSA documents underscores the absurdity of proposals aimed at "reforming" and "reigning in" the mass surveillance programs, which, propelled by the explosive growth of social inequality and the rise of a criminal financial oligarchy, have enjoyed a tropical flourishing since the 1970s, acquiring an extravagant scale and diversity.