Snowden reveals massive National Security Agency hacking unit

Robert Stevens
31 December 2013

The US National Security Agency (NSA) runs an Office of Tailored Access Operations (TAO), described by Germany's *Der Spiegel* as the "NSA's top operative unit—something like a squad of plumbers that can be called in when normal access to a target is blocked."

A report published Sunday based on documents released by whistleblower Edward Snowden states that the TAO operates as a vast hacking unit on behalf of the US government.

Based in San Antonio, Texas and formed in 1997, the TAO, "are involved in many sensitive operations conducted by American intelligence agencies. TAO's area of operations ranges from counterterrorism to cyber attacks to traditional espionage. The documents reveal just how diversified the tools at TAO's disposal have become—and also how it exploits the technical weaknesses of the IT industry, from Microsoft to Cisco and Huawei, to carry out its discreet and efficient attacks."

In 2008, the TAO unit had 60 specialists the magazine said—a number set to escalate to 270 by 2015. The TAO's duties according to the NSA are based on "Getting the ungettable."

A document seen by *Der Spiegel* cites a former head of the TAO who comments that it had collected "some of the most significant intelligence our country has ever seen" and has "access to our very hardest targets."

The remit of the TAO is enormous, with the former head stating it "needs to continue to grow and must lay the foundation for integrated Computer Network Operations."

In a statement that reveals how the mass surveillance operations of the NSA are intimately tied to the drive by US imperialism to dominate its rivals internationally, the former head states that the TAO must "support Computer Network Attacks as an integrated part of military operations."

Outlining its future role, she said the TAO would have to acquire "pervasive, persistent access on the global network."

Der Spiegel reports that this is precisely what has been achieved. "During the middle part of the last decade, the special unit succeeded in gaining access to 258 targets in 89 countries—nearly everywhere in the world," *Der Spiegel* notes. "In 2010, it conducted 279 operations worldwide."

Through their hacking operations the TAO has "directly accessed the protected networks of democratically-elected leaders of countries" states *Der Spiegel*. It notes in passing, "Workers at NSA's target selection office…had Angela Merkel in its sights in 2002 before she became [German] chancellor…"

Der Spiegel states that the TAO "infiltrated networks of European telecommunications companies and gained access to and read mails sent over Blackberry's BES email servers, which until then were believed to be securely encrypted."

The global reach of the TOA is vast, with *Der Spiegel* reporting that the "San Antonio office handles attacks against targets in the Middle East, Cuba, Venezuela and Colombia, not to mention Mexico, just 200 kilometers (124 miles) away, where the government has fallen into the NSA's crosshairs."

One of the presentation slides states that a critical TAO goal is to "subvert endpoint devices." These include the many main devices that make up modern communication technologies including "servers, workstations, firewalls, routers, handsets, phone switches, SCADA systems, etc."

Der Spiegel explains, "SCADAs are industrial control systems used in factories, as well as in power plants" and notes that the "most well-known and notorious use

of this type of attack was the development of Stuxnet, the computer worm whose existence was discovered in June 2010. The virus was developed jointly by American and Israeli intelligence agencies to sabotage Iran's nuclear program, and successfully so."

The TAO has developed various means to gain access to the PCs of Internet users. One slide reveals that TAO is able to gain "passive access" to a machine via Microsoft's automated PC crash reports. *Der Spiegel* notes, "even this passive access to error messages provides valuable insights into problems with a targeted person's computer and, thus, information on security holes that might be exploitable for planting malware or spyware on the unwitting victim's computer."

TAO operatives even created an internal graphic, for their own amusement, which replaced Microsoft's original error message with one reading, "This information may be intercepted by a foreign sigint system to gather detailed information and better exploit your machine."

Sigint is the acronym for "signals intelligence", meaning the gathering of intelligence by interception of signals.

Another document reveals that among the TAO's "most productive operations" is the direct interception of new PCs and other computer accessories ordered by individuals targeted by the NSA.

In a process named "interdiction", the goods are rerouted from the supplier to one of the TAO's secret workshops. *Der Spiegel* states that TAO agents then "carefully open the package in order to load malware onto the electronics, or even install hardware components that can provide backdoor access for the intelligence agencies. All subsequent steps can then be conducted from the comfort of a remote computer."

Interdiction allows the TAO to exploit networks "around the world," said the document.

The information on the TAO was published just days after Edward Snowden broadcast an "alternative" Christmas Day television message for Britain's *Channel 4*, to contrast with that given by the Queen. Speaking from his forced exile in Moscow, Snowden said the world's population have recently "learned that our governments, working in concert, have created a system of worldwide mass surveillance, watching everything we do."

He added that "the conversation occurring today will determine the amount of trust we can place both in the technology that surrounds us and the government that regulates it. Together, we can find a better balance."

His message followed an interview with the *Washington Post* December 24 in which he said of the revelations he has made available, "For me, in terms of personal satisfaction, the mission's already accomplished... Because, remember, I didn't want to change society. I wanted to give society a chance to determine if it should change itself."

Snowden has exposed a state intelligence apparatus of genuine totalitarian dimensions, which spies on the entire world's population and his courage and dedication to the preservation of basic democratic rights are admirable. However, if he believes that "a better balance" can now be found, he is mistaken.

Michael Hayden, former director of the National Security Agency, said Sunday that he had thought of Snowden as a "defector," but is now "drifting in the direction of perhaps more harsh language...such as 'traitor.' I think there's an English word that describes selling American secrets to another government, and I do think it's treason."

Earlier this month John Bolton, US ambassador to the United Nations during the George W. Bush administration, said, "My view is that Snowden committed treason, he ought to be convicted of that, and then he ought to swing from a tall oak tree."

Similarly, former CIA director James Woolsey declared that Snowden "should be prosecuted for treason. If convicted by a jury of his peers, he should be hanged by his neck until he is dead."