KCS Group Europe

Codename TAO – The NSA's Mass Surveillance and Tailored Access Operations

July 2024

In this era of digital connectivity, privacy is a concept that is on the one hand prized, and on the other, severely compromised. The National Security Agency (NSA), known for being one of the largest intelligence gathering agencies in the world, has continuously found itself under intense scrutiny regarding its mass surveillance operations. Its mandate as of the middle of the last century, was to collect and disseminate foreign intelligence with restriction. However, following the atrocities of the 9-11 attacks, the agency was given unrestricted access, which expanded its reach significantly to include surveillance of US communications with foreign entities. This was done in the interests of national security, authorised by then President George W. Bush.

TAO – Tailored Access Operations

The extent of the NSA's capabilities became chillingly clear when senior NSA executive, Thomas Drake, blew the whistle on the illicit spending and activities of some of the agency's programs. Drake, who served with the NSA from 2001 to 2008, luckily avoided a severe prison term sentence under the Espionage Act.

Drake's leaks brought to light a secret special operations unit within the NSA known as Tailored Access Operations or TAO (now called CNA Computer Network Operations, and structured as S32), a group that specialises in acquiring the unobtainable. Consisting of 600 employees stationed in a Remote Operations Centre (ROC) within the NSA called S321, TAO are the world's best in the cyber sphere.

They are a “special forces” unit within the NSA, using extremely talented operatives to infiltrate, manipulate and sabotage any and all digitally connected devices worldwide. It is said that there is nothing they cannot hack.

TAO was again brought to the media’s attention following leaked documents by Edward Snowden’s revelations in 2013, which caused heated global discussion regarding the scope of the unit’s surveillance abilities. Snowden’s leaks also revealed details of the NSA’s PRISM program, which gave the agency direct access to emails, video chats and more from major tech companies. The public called for an inquiry as to what or who these units were monitoring and why.

Among TAO’s most notable abilities is the capacity to engage in what the NSA labels “Computer Network Exploitation” (CNE). They exploit networks and routers because this gives them access to all devices connected to a network, as opposed to just one. Exploits can be found at random by blue hat hackers hired to find vulnerabilities in client software or devices, or red hat hackers who sell their discoveries on the dark net to the highest bidder.

Soon after exploits are revealed, the software companies responsible provide patches and updates mending the compromises preventing further unwarranted access. It is rumoured that the NSA has its own comprehensive list of top secret zero-day exploits and TAO uses these exploits to compromise computer networks to either gather valuable information, disable systems, or destroy data. TAO is believed to have not only targeted terrorist organisations – its sole purpose – but has been implicated in commercial espionage and surveillance of foreign leaders and business interests.

The hunt for Bin Laden

A notable revelation about the effectiveness of the NSA’s TAO unit came from its contribution to the high-profile counter-terrorism activities surrounding the hunt for Osama Bin Laden. TAO agents were directed to hack into the mobile phones of Al-Qaeda operatives living within Bin Laden’s network and track their movements.

The abilities of the unit and the fact they were able to pinpoint key figures that eventually led to their capture and the assassination of one of the world's most wanted terrorists demonstrated the double-edged sword of its surveillance power. TAO does infringe on privacy, however, if orchestrated responsibly, it serves as an invaluable weapon in the global fight against terrorism.

NSA's secret catalogue

On top of the agency's covert operations, the extent of TAO's technological armoury has been a subject of much intrigue and, of course, concern. A leaked series of documents confirmed the existence of an NSA catalogue known to few as the ANT (Advanced Network Technology) catalogue, that lists a plethora of spy tools at TAO's disposal to conduct surveillance and data interception. The listed tools include hard and software devices that have the ability to capture signals without a target's knowledge. One such device is called the RAGEMASTER, a hardware device that hides within a VGA cable that can transmit what is displayed on a victim's screen to a remote viewer by reflecting radar waves.

Operations revealed

Local and international entities thought to have been targeted by TAO include China's Northwestern Polytechnical University, the Organization of the Petroleum Exporting Countries (OPEC), and Mexico's Secretariat of Public Security.

TAO is also alleged to have compromised global communications including the tapping of the SEA-ME-WE 4, a submarine communications cable line that connects multiple countries across Asia, including Singapore and India, the Middle East and Europe.

QUANTUM - a known TAO software hacking network - was given access to the fibre-optic links of Försvarets radioanstalt (FRA) in Sweden, to enhance the unit's surveillance capabilities. This QUANTUM INSERT technology developed by TAO has also been shared with UK intelligence services.

The Government Communications Headquarters (GCHQ) has also used QUANTUM as part of the Five Eyes agreement to infiltrate networks such as Belgacom and various GPRS roaming exchange (GRX) providers, including Comfone and Syniverse.

It has also been reported that TAO has intercepted laptops purchased online under the instruction of the CIA and FBI. The equipment is redirected to covert facilities where they are compromised with spyware and hardware before being forwarded to the unsuspecting buyer.

Is it right or wrong?

The implications - both ethical and moral - of employing such surveillance is complicated. There is the need to monitor digital communications in the battle against terror attacks and cyber threats, yet, there remains the issue of how this profound ability is policed in terms of non-state security critical threat use in the commercial sector.

By its very nature, TAO operates in the greyest of areas. Its activities cannot be accessed without the highest levels of authority, and this means that the governing frameworks that control its activities are not easily comprehended by the public. Naturally, such secrecy fosters a platform for abuse with little to no accountability. Many argue that this unit could bring significant implications for civil liberties.

TAO's operations have also strained international relations as several countries have expressed outrage on learning that their subjects have been targeted by US surveillance units. These incidents forced the US government to reconsider its surveillance policies, although the extent of these considerations is unknown.

Domestic and international calls for transparency and the regulation of the NSA have been abundant, with some suggesting reforms by way of an international treaty on surveillance and cyber-attacks to set global standards and norms. Given the geopolitical tensions and cold war environment of today, significant changes are unlikely to occur anytime soon. However, the ongoing debate over individual privacy will continue.

The efforts of special unit entities like TAO might be a pivotal asset in the fight to protect national security, but the potential for its abuse is a contentious issue.

Conclusion

The revelations of the NSA's Tailored Access Operations (TAO) unit provide insight into the intricate balance between national security priorities and the value of individual privacy. Although TAO's pivotal role in missions like bringing Osama Bin Laden to justice demonstrates an unquestionable value in the fight against terror, its participation in intercepting private laptops and penetrating global communication lines, highlights serious mass surveillance privacy concerns.