NSA tapping vast majority of cell phone networks worldwide

Thomas Gaist
5 December 2014

Electronic surveillance programs run by the US National Security Agency have compromised the great majority of the world's cell phone networks, according to newly released NSA documents leaked by Edward Snowden and published on *The Intercept.*

The NSA's operation AURORAGOLD, exposed by the new Snowden documents, has already established an institutional and technological framework through which the spy agency can achieve direct access to all data traversing the world's cellular networks.

Run by at least two secret NSA spy units, referred to in the documents as the Wireless Portfolio Management Office and the Target Technology Trends Center, AURORAGOLD encompasses a range of surveillance and electronic infiltration activities against cell phone networks on every continent.

The agency had established some level of electronic surveillance presence within 701 of the estimated 985 global cell phone networks as early as May 2012, the leaked documents reveal.

The main purposes of AURORAGOLD, the slides in the documents indicate, are:

* to “maintain data about international GSM/UMTS [cell phone] networks”

* to “forecast the evolution" of global cellular networks in support of the agency's "imperative to Know the Future”

* to develop intelligence on and surveillance operations against “GSM/UMTS infrastructure,” “voice data convergence,” “technology migration,” and “technology deployments”

As part of AURORAGOLD, the slides show that NSA agents engage in:

* installing electronic backdoors in encryption systems deployed to protect cell phone networks

* gathering intelligence on and predicting the future development of cell phone security systems

* cracking new encryption technologies before they have even been deployed on live cellular networks

Information gathered by AURORAGOLD is widely shared within the intelligence agencies of the US and its allies, the slides show.

“Coincident beneficiaries of this mission are, among others, other NSA SIGDEV elements, protocol exploitation elements, and Five-Eyes Partner SIGDEV organizations," one slide states. The Five Eyes network is comprised of the United States, Canada, Britain, Australia and New Zealand.

The leaked slides include a color-coded map showing that the NSA has tapped into 100 percent of existing cellular networks in numerous countries, including the majority of countries in Africa, as well as Mexico, Saudi Arabia, the Philippines, Venezuela, Poland and Indonesia.

The NSA has tapped a large majority of cell phone networks in China, Russia, Turkey, Iran and Spain, the map shows, and is running cellular network surveillance operations inside the US, the UK, Australia, New Zealand, Germany and France.

Making clear that the NSA is seeking to establish a regime of total information awareness even in relation to its corporate partners, one slide reads, “We monitor the industry” and demands “visibility into changing standards and practices for: Roaming, Signaling, Billing, Interoperability.”

The agency systematically spied on the content of emails sent from more than 1,000 email accounts run by key offices within the global telecommunications network.

One of the NSA's main targets was a British-based global trade group called the GSM Association, which maintains ties to hundreds of telecommunications and

tech companies around the world. NSA operations against GSM sought to intercept “IR.21 documents” passed between companies via GSM. The IR.21 documents contain information about cell phone networks that the NSA uses to penetrate their security systems.

The NSA and its British counterpart GCHQ worked together to crack the so-called “A 5/3” encryption algorithm as part of a program called WOLFRAMITE, the documents show.

The documents also shed light on the role of NSA in supporting the geopolitical machinations of US imperialism. One document shows that the NSA received orders to hack Libyan cellphone networks from the Pentagon’s Africa Command (AFRICOM) in March 2011.

“AFRICOM IKD-OPS requires information concerning the SMS Gateway domains for: Libyana mobile (libyans.ly) and Al Madar Al Jadid (almadar.ly),” one slide reads.

A slide boasting of the agency's “Notable Successes” claims that the NSA has achieved “IR 21 collection from 67 high-priority networks,” including “recent IR 21s from Egypt,” and “IR 21 collection related to a possible new Chinese network.”

The latest documents make a mockery of the countless lies advanced by the Obama administration and the intelligence establishment in defense of the US government's warrantless surveillance programs.

Rather than being limited to telephone metadata, or to “foreign intelligence” threats, the NSA's surveillance machine has direct access to the bulk of cell phone traffic worldwide, including traffic that is supposedly protected by encryption.

Responding to the latest revelations, NSA spokeswoman Vanee Vines reassured the public that the spy agency “collects only those communications that it is authorized by law.”

In a sense, it is true that the surveillance programs have been “authorized by law.”

With the emergence of the Foreign Intelligence Surveillance Court in 1978, a secret surveillance judiciary has was established that presides over the development of a panoply of unconstitutional spying operations by the US intelligence establishment.

This process has complete support from the Republican and Democratic parties in Congress and the last several presidential administrations, which have adopted a series of executive orders authorizing mass surveillance.

The entire US government, including the Congress, has endorsed practices which clearly violate the Fourth Amendment to the US Bill of Rights. It is the military and intelligence agencies that call the shots in Washington, in alliance with Wall Street, not Senators, congressmen and even presidents, who serve as willing accomplices.

Defending the worldwide cell network tapping programs, NSA spokesperson Vines argued that the use by “terrorists” of cellular networks justifies total access by the US agency to global cellular data. “Terrorists, weapons proliferators, and other foreign targets often rely on the same means of communication as ordinary people,” Vines said.

These words express the fact that as far as the NSA is concerned, Internet and telephone users have no democratic rights. Under the pretext of spying on “terrorists” lurking in every corner of the globe, the NSA is aggressively pursuing its openly stated objectives: “Collect it All; Process it All; Exploit it All; Partner it All; Sniff it All; Know it All.”

Terrorists also breath the same air, drink the same water, eat the same food and travel the same roads as ordinary people. Apparently this brings every necessity of human life under the jurisdiction of the US military-intelligence apparatus.

The favorite arguments of right-wing dictatorships are now continually invoked by the leaders of the US bourgeois state. The NSA spokesperson’s comments are a textbook application of the authoritarian legal theories developed by Nazi jurists, which call for the executive power to free itself from all legal constraints in response to a “state of emergency.”

The Obama administration has fully embraced authoritarian legal doctrine that the government the government can spy arbitrarily on any target that its agents select.