Edward Snowden exposes NSA spying against Chinese telecom firm Huawei

Tom Carter
24 March 2014

Documents released by National Security Agency (NSA) whistleblower Edward Snowden and published in the *New York Times* over the weekend confirm that the US spy agency has been engaged for years in a campaign of industrial espionage against Huawei, the giant Chinese telecommunications firm. The documents expose a broad range of espionage activities, from spying on company executives to creating "back doors" into the company's servers, routers and switches.

The documents, which date from 2010, reveal that a major spying operation against Huawei had been underway since at least 2007 under the codename "Shotgiant." While the *Times* reported the existence of the program and published some of the PowerPoint slides provided by Snowden, the *Times* has "withheld technical details of the operation at the request of the Obama administration, which cited national security concerns." The "newspaper of record" has once again bowed to the demands of the military-intelligence apparatus.

The NSA issued a statement claiming that the release of the PowerPoint slides "is detrimental to the security of the United States and our allies—and places at risk those we are sworn to protect." Reuters reported the response of Huawei's global cyber security officer John Suffolk: "If the actions in the report are true, Huawei condemns such activities that invaded and infiltrated into our internal corporate network and monitored our communications."

In 2012, Huawei became the world's largest telecommunications equipment maker. Its products are in use in as many as 145 countries. For years, Washington has termed Huawei a "national security" concern, alleging that Huawei grants the Chinese government unauthorized access to its telecommunications infrastructure (i.e., exactly what the American telecommunications companies allow the NSA to do).

The *Times* quoted Huawei executive William Plummer as saying, "The irony is that exactly what they are doing to us is what they have always charged that the Chinese are doing through us."

One PowerPoint slide released by Snowden and titled "Why We Care" explains that the NSA hacks into Huawei's infrastructure in order to spy on its products' users. "Many of our targets communicate over Huawei produced products, [so] we want to make sure that we know how to exploit these products—we also want to ensure that we retain access to these communication lines, etc."

Notes accompanying another slide include a list of "what we are trying to accomplish." One of the items on this list is to "[d]etermine if Huawei is doing SIGINT [signals intelligence, spying] for PRC [China]." In other words, the NSA's own internal documents make clear that the NSA does not have any evidence that Huawei is engaged in the conduct for which American political functionaries routinely denounce the company.

The documents name the NSA's "high priority targets" as "Iran, Afghanistan, Pakistan, Kenya, [and] Cuba." The NSA PowerPoint slide defines "success" as the following: "Obtaining actionable intelligence of Huawei's (and potentially PRC's) leadership plans and intentions" and "Enabl[ing] SIGINT collection through CNE tools."

"CNE" or "Computer Network Exploitation" refers to the legion of malware programs with which the NSA has infected more than 50,000 computer networks around the world. (See: "New Snowden document reveals NSA's international malware operation .") These malware programs allow the NSA to take

over networks and computers and use them to spy on their users.

The recently released PowerPoint slides feature the now-familiar concept of “intelligence gaps.” As far as the NSA is concerned, if anyone anywhere in the world is engaged in any kind of activity and the NSA does not know about it, then this represents an “intelligence gap” the spy agency is determined to close.

In the final analysis, the NSA spying campaign against Huawei has two fundamental purposes. First, Huawei (unlike the American telecommunications companies) does not allow the NSA free access to its infrastructure to conduct spying on its products’ users. Accordingly, as part of its mission of spying on the entire world’s population, the NSA hacked into Huawei’s systems in order to gather information traveling through its infrastructure.

Second, the spying campaign against Huawei is part of broader efforts to protect the profits and interests of American telecommunications companies at the expense of Huawei. This is the purpose of the NSA’s particular interest in Huawei’s executives and their “leadership plans and intentions.”

Indeed, the latest Snowden revelations cast fresh light on the US government’s repeated interventions around the world to undermine Huawei’s business. In 2008, the United States blocked Huawei’s participation in the purchase of 3Com Corporation, citing “national security” concerns. In 2012, the US government intervened in Australia to block Huawei from constructing a broadband network there. (See:“Australian government bars Chinese telco on ? security’ grounds.”) Also in 2012, Symantec ended a four-year partnership with Huawei under pressure from the US government, which threatened to cut off Symantec’s access to classified information. US Vice President Joseph Biden personally intervened in South Korea in 2013 to block Huawei from building a broadband telecommunications network in Seoul.

According to *Der Spiegel*, the German news magazine, the fruits of the NSA spying program against Huawei included a list of 1,400 of the firm’s clients, as well as internal engineering documents. One of the documents released by Snowden reads, “If we can see how Huawei is marketing itself, and working to expand this will help us to understand the company’s plans and intentions.”

Among the PowerPoint slides just published, one sentence in particular stands out. Among the tasks the NSA is “hoping to accomplish” in its campaign against Huawei is to “[d]ocument processes to be used later for targeting other non-partnerable companies.” The description of Huawei as a “non-partnerable” company, together with the expressed intention of targeting other “non-partnerable” companies for spying, is full of significance.

Translated into plain English, what “non-partnerable” means is that Huawei does not “partner” with the NSA to carry out illegal spying. Companies that are “partnerable” are presumably those such as Microsoft, Apple, Google, Facebook, Yahoo!, AOL, Verizon, AT&T and others around the world, which are willing “partners” of the US government in its illegal spying on their users and customers.

The new revelation about Huawei is one of the many devastating exposures by Snowden of different features of the spying architecture that has been built up behind the backs of the American and world population. The cumulative effect of these disclosures is to paint a picture of a massive military-corporate-intelligence complex, totalitarian in its implications, loosed from all constitutional and democratic controls.

This apparatus—with the integral participation of its “partners” in the business and financial spheres—has for years been quietly working its tentacles into virtually every corner of the world. The purpose of this spying apparatus is to protect the profits and wealth of the American ruling class at any cost—from international rivals and, above all, from a movement from below.