Snowden discusses US surveillance and cyber-warfare programs in interview with Wired

Thomas Gaist
15 August 2014

Wired magazine published an extended interview this week with former US intelligence agent and famed whistleblower Edward Snowden. Conducted in a hotel room somewhere in Russia, the interview included fresh revelations related to mass surveillance, cyber-warfare and information-grabbing operations mounted by the US National Security Agency (NSA).

The meat of the interview centered on a number of operations run by the surveillance and intelligence agencies, painting a picture of an American government engaged in ever-expanding cyber-machinations worldwide.

Snowden spoke about the NSA's MonsterMind program, an "autonomous cyber-warfare platform" which has been developed to launch cyber-attacks automatically against rival governments, without any need for human intervention. He noted that MonsterMind could easily be manipulated to provoke spasms of cyber-warfare between the US and its main rivals.

"These attacks can be spoofed. You could have someone sitting in China, for example, making it appear that one of these attacks is originating in Russia. And then we end up shooting back at a Russian hospital," Snowden said.

Far from restricting itself to cyber-defense, Snowden said, the US is constantly engaged in offensive hacking operations against China.

"It's no secret that we hack China very aggressively," Snowden said. "But we've crossed lines. We're hacking universities and hospitals and wholly civilian infrastructure rather than actual government targets and military targets."

Snowden offered new information about the role of the NSA in facilitating US imperialism's geopolitical agenda in the Middle East. In 2012, Snowden said, the NSA's Tailored Access Operations (TAO) hacking unit accidentally disabled large portions of Syria's Internet during an operation that sought to install information-capturing software on the routers of a main Syrian service provider.

Western media dutifully reported at the time that the Internet shutdown was ordered by the Assad regime, which was and remains a primary target for overthrow by US and European imperialism.

Describing "one of the biggest abuses we've seen," Snowden said that the US routinely transfers bulk communications data acquired from Palestinian and Palestinian- and Arab-American sources to Israeli intelligence in support of Israeli military operations targeting the Occupied Territories.

Moreover, a Snowden-leaked NSA document published earlier this month stated that through its collaboration with US intelligence and surveillance agencies, the Israeli regime "enjoys the benefits of expanded geographic access to world-class NSA crypto analytic and SIGINT engineering expertise, and also gains controlled access to advance US technology and equipment." During Israel's 2008-2009 military onslaught against Gaza, US and British intelligence provided Israel with reams of data captured from surveillance of Palestinian e-mail addresses and telephones, the document confirmed.

Speaking about the lies told by Director of National Intelligence (DNI) James Clapper during congressional testimony in the wake of the initial leaks, Snowden denounced the culture of deception and criminality that pervades the US government and ruling elite.

During the March 2013 hearing, DNI Clapper was asked, "Does the NSA collect any type of data at all on millions or hundreds of millions of Americans?"

In an absurd lie, repeated in one form or another by

numerous top officials including President Barack Obama, Clapper answered, “No sir, not wittingly.”

Snowden correctly noted that Clapper’s brazen lying was merely standard operating procedure for top US officials. “He [DNI Clapper] saw deceiving the American people as what he does, as his job, as something completely ordinary. And he was right that he wouldn’t be punished for it, because he was revealed as having lied under oath and he didn’t even get a slap on the wrist for it. It says a lot about the system and a lot about our leaders,” Snowden said.

The interview provided an outline of Snowden’s career prior to 2013, which included significant high-level work on behalf of the Central Intelligence Agency (CIA) and NSA as an intelligence and technology specialist. During his years of employment by the government, Snowden attended a secret CIA school for tech experts and worked for the CIA’s global communications division as well as for the NSA office at the Yokota Air Base near Tokyo.

Snowden later held a position with Dell as its head technologist in relation to the CIA’s account with the company.

While working for the NSA contractor Booz Allen, Snowden worked to seize data from foreign service and inject malware into computer systems around the globe, he said. It was during this period that he became aware that the NSA was capturing and archiving huge amounts of US data, and doing so “without a warrant, without any requirement for criminal suspicion, probable cause, or individual designation.”

Snowden stressed the all-invasive character of the surveillance programs, stating categorically that the surveillance programs violate the Fourth Amendment.

“The argument [made by the US government] is that the only way we can identify these malicious traffic flows and respond to them is if we’re analyzing all traffic flows. And if we’re analyzing all traffic flows, that means we have to be intercepting all traffic flows. That means violating the Fourth Amendment, seizing private communications without a warrant, without probable cause or even a suspicion of wrongdoing. For everyone, all the time,” Snowden said.

Responding to the interview, an official government statement reiterated the state’s longstanding demand for Snowden to return to the United States and face espionage charges in a US court.

“If Mr. Snowden wants to discuss his activities, that conversation should be held with the U.S. Department of Justice. He needs to return to the United States to face the charges against him,” the statement said.

During the interview, Snowden suggested that he might voluntarily accept a prison sentence as part of a deal with the US government allowing him to return home. While it is understandable that Snowden should seek every available means to avoid the fate of fellow whistleblower Pfc. Chelsea Manning, who was sentenced to 35 years in prison and abused for years prior to his trial, it is a dangerous delusion to believe that the US government can be negotiated with on this matter.

In compromising mass spying operations that are considered essential to the stability and security of the capitalist state, Snowden’s actions have provoked significant anxiety within ruling circles. As a result, the most powerful elements within the US establishment view Snowden as a hated and mortal enemy, and are determined to lock him up and throw away the key.