https://firstlook.org/theintercept/2015/02/10/nsa-iran-developing-sophisticated-cyber-attacks-learning-attacks/

NSA Claims Iran Learned from Western Cyberattacks

By *Glenn Greenwald*

2/10/2015

The U.S. Government often warns of increasingly sophisticated cyberattacks from adversaries, but it may have actually contributed to those capabilities in the case of Iran.

A top secret National Security Agency document from April 2013 reveals that the U.S. intelligence community is worried that the West's campaign of aggressive and sophisticated cyberattacks enabled Iran to improve its own capabilities by studying and then replicating those tactics.

The NSA is specifically concerned that Iran's cyberweapons will become increasingly potent and sophisticated by virtue of learning from the attacks that have been launched against that country. "Iran's destructive cyber attack against Saudi Aramco in August 2012, during which data was destroyed on tens of thousands of computers, was the first such attack NSA has observed from this adversary," the NSA document states. "Iran, having been a victim of a similar cyber attack against its own oil industry in April 2012, has demonstrated a clear ability to learn from the capabilities and actions of others."

The document was provided to *The Intercept* by NSA whistleblower Edward Snowden, and was prepared in connection with a planned meeting with Government Communications Headquarters, the British surveillance agency. The document references joint surveillance

successes such as "support to policymakers during the multiple rounds of P5 plus 1 negotiations," referring to the ongoing talks between the five permanent members of the U.N. Security Council, Germany and Iran to forge an agreement over Iran's nuclear program.

The document suggests that Iran has become a much more formidable cyberforce by learning from the viruses injected into its systems—attacks which have been linked back to the United States and Israel.

In June 2012, *The New York Times* reported that from "his first months in office, President Obama secretly ordered sophisticated attacks on the computer systems that run Iran's main nuclear enrichment facilities, significantly expanding America's first sustained use of cyberweapons, according to participants in the program." As part of that plan, the U.S. and Israel jointly unleashed the Stuxnet virus on Iranian nuclear facilities, but a programming error "allowed it to escape Iran's Natanz plant and sent it around the world on the Internet." Israel also deployed a second virus, called Flame, against Iran.

Obama ordered cyberattacks despite his awareness that they would likely unleash a wholly new form of warfare between states, similar to the "first use of atomic weapons in the 1940s, of intercontinental missiles in the 1950s and of drones in the past decade," according to the *Times* report. Obama "repeatedly expressed concerns that any American acknowledgment that it was using cyberweapons—even under the most careful and limited circumstances—could enable other countries, terrorists or hackers to justify their own attacks."

The NSA's concern of inadvertently aiding Iran's cyberattack capabilities is striking given the government's recent warning about the ability of adversaries to develop more advanced viruses. A top official at the Pentagon's Defense Advanced Research Projects Agency's (DARPA) appeared on *60 Minutes* this Sunday and claimed that cyberattacks against the U.S. military are becoming more potent. "The sophistication of the attacks is increasing," warned Dan Kaufman, director of DARPA's Information Innovation Office.

The NSA document suggests that offensive cyberattacks on other states do not merely provoke counterattacks—those attacks can teach adversaries how to launch their own. "Iran continues to conduct distributed denial-of-service (DDOS) attacks against numerous U.S. financial institutions, and is currently in the third phase of a series of such attacks that began in August 2012," the document says. "SIGINT indicates that these attacks are in retaliation to Western activities against Iran's nuclear sector and that senior officials in the Iranian government are aware of these attacks."

This would not be the first time the U.S. has inadvertently assisted Iran's attack capabilities. Last month, former CIA officer Jeffrey Sterling was convicted of multiple felony counts for telling *New York Times* reporter James Risen about an agency program designed to feed Iran false data about nuclear engineering in order to create setbacks, but which instead may have provided useful information the Iranians were able to exploit to advance their nuclear research.

As of 2013, the NSA said that while it had no indications "that Iran plans to conduct such an attack against a U.S. or UK target, we cannot rule out the possibility of such an attack, especially in the face of increased international pressure on the regime."

The NSA "can't comment or speculate on the motivations of those who aim to harm the United States or our allies," a spokesperson for the agency said. "The National Security Agency works with foreign partners to protect our interests and citizens in cyberspace."