Sony hacking allegations used to push antidemocratic “cybersecurity” laws

Tom Carter
10 January 2015

While the US government has employed allegations about the hacking of Sony Pictures Entertainment to intensify its aggressive policy towards North Korea, domestically these allegations are being utilized to push for anti-democratic “cybersecurity” legislation.

In the language of official Washington, “cybersecurity” means further expanding the activities of the state’s repressive apparatus with respect to the Internet, integrating that apparatus with the largest American corporations and the private telecommunications infrastructure, and maintaining American domination over cyberspace internationally.

The 114th US Congress opened on January 3, and its first week was marked by widespread demands for “information sharing” cybersecurity legislation. The phrase “information sharing” refers to the practice of corporations collecting private information about individuals and then turning that information over to the government.

In one form or another, “information sharing” legislation has been the subject of proposals in Congress since the 1990s. However, previous attempts to pass such legislation have been blocked on the grounds that they would violate the privacy rights of individuals.

The Senate’s failed “Cybersecurity Information Sharing Act of 2014,” for example, was the fourth time in four years that Congress unsuccessfully attempted to pass cybersecurity legislation.

The Electronic Frontier Foundation (EFF) described the proposed legislation as “a dangerous bill that would grant companies more power to obtain ‘threat’ information (for example, from private communications of users) and to disclose that data to the government without a warrant—including sending data to the National Security Agency. It also gives companies broad immunity to spy on—and even launch countermeasures against—potentially innocent users.”

“Cybersecurity bills aim to facilitate information sharing between companies and the government,” the EFF warned, “but they always seem to come with broad immunity clauses for companies, vague definitions, and aggressive spying powers.”

Now, efforts are underway to exploit the Sony hacking allegations to finally ram through this antidemocratic legislation.

Homeland Security Chairman Michael McCaul announced on Monday that he would make it a priority to “better prevent, detect, and respond to [hacking] and to remove any unnecessary legal barriers for the private sector to share cyber threat information.”

Leading Republican Senator John McCain (Arizona) has similarly called on Congress to “finally pass long-overdue comprehensive cybersecurity legislation.” Senator Lindsey Graham (South Carolina), another leading Republican, made the following “tweet” last month: “Modernizing cyber-security laws & working to protect national interests against cyber-terrorism should be a top priority 4 Congress in 2015.”

Calls for “information sharing” legislation have not been limited to the Republican Party, which now enjoys substantial majorities in both houses of Congress. Outgoing Senate Intelligence Committee chair Dianne Feinstein, a Democrat from California, referred to the Sony hacking allegations last month as “only the latest example of the need for serious legislation to improve the sharing of information between the private sector and the government.” She added, “We must pass an information sharing bill as quickly as possible next year.”

White House Cybersecurity Coordinator Michael Daniel—known as Obama’s “cyber czar”—gave a press conference last Tuesday in which he announced that the administration would expand its cybersecurity efforts in the private sector.

“One of the things you can look for from us is continued effort to identify places where we can take executive action.” He added, “We will be looking for all the cases where we can potentially take some executive action to further things like information sharing and improving cybersecurity. Another big area you should look for us to do

is continue pressing on legislation … like information sharing …"

On December 19, Obama himself used a year-end press conference to urge Congress to pass "information sharing" legislation. "One of the things in the new year that I hope Congress is prepared to work with us on is strong cybersecurity laws that allow for information sharing across private-sector platforms, as well as the public sector, so that we are incorporating best practices and preventing these attacks from happening in the first place."

As National Security Agency whistleblower Edward Snowden revealed last year, the American military and intelligence apparatus is already deeply integrated into the boardrooms of the largest corporate and financial institutions, as well as into the physical infrastructure of the internet.

While the various factions in Congress may quibble over particulars, any "information sharing" legislation that is passed will only add to the stockpile of data that government entities such as the NSA are compiling about the activities, political interests, and personal lives of ordinary individuals all around the world.

The issue of "information sharing" has nothing to do with the actual hacking of Sony Pictures Entertainment. "It is unlikely that information sharing would have prevented the Sony hack," Robyn Greene, policy counsel for New America Foundation's Open Technology Institute, told *The Hill*. "Eighty to ninety percent of all attacks are the result of poor cyber hygiene and internal system monitoring." In other words, the Sony hacking allegations are simply being employed as a pretext to further expand and codify domestic spying on the population.

The Sony hacking scandal involves the release on November 24 of a large volume of internal information from the company, including internal emails and unreleased films. The hackers responsible, calling themselves the "Guardians of Peace," allegedly demanded the cancellation of the release of the film *The Interview*, a comedy featuring the assassination of North Korean leader Kim Jong-un. (See: "The latest blockbuster from CIA Pictures: *The Interview*")

On December 19, the Obama administration directly accused the North Korean state of responsibility for the hacking, and the Federal Bureau of Investigation released a report that purported to substantiate these allegations. However, over recent weeks, the foundation for these accusations has steadily deteriorated. (See: "Cybersecurity investigators raise doubts about North Korean responsibility for Sony hack")

On Wednesday, cybersecurity expert Jeffrey Carr added his voice to the growing number of skeptics. The Obama administration's accusations, Carr wrote on his blog, are based on the "myth" of a "closed" North Korean internet.

"The FBI, the NSA, and the private security companies upon which they rely for information believe that any attack linked to a North Korean IP address must be one that is government sanctioned since North Korea maintains such tight control over its Internet and Intranet," Carr wrote, calling this assumption the FBI's "single point of failure." According to Carr, access to North Korean servers "is relatively easy if you go in through China, Thailand, Japan, Germany or other countries where North Korea has strategic connections."

State Department spokeswoman Jen Psaki, pressed by reporters at a press conference Tuesday, refused to release additional data to back up the government's case. "There is a certain amount of evidence that the FBI made public; there is a certain amount they did not, that we're not going to do. But they remain confident and we remain confident in their findings."

It goes without saying that if the FBI had direct proof that North Korea was behind the Sony hacking, that proof would be aired around the clock on all the major news channels. Psaki's lame plea—"trust us"—comes from a government that has repeatedly been caught lying about subjects as diverse as torture, domestic spying, and "affordable health care." The response of any rational person who hears "trust us" from the Obama administration should be to immediately assume that whatever is being said is false.

Nevertheless, the Obama administration's "cybersecurity" initiatives continue to echo throughout the political establishment. Federal Trade Commission Chairwoman Edith Ramirez made a point of referring to "cybersecurity" in a speech on Tuesday. That same day, the FBI and Fordham University hosted an "International Conference on Cybersecurity." On Wednesday, the US Air Force announced new cybersecurity measures.

According to an article Sunday in the Washington DC newspaper *The Hill* (which focuses on the politics, business and lobbying around the US Congress), other cybersecurity-related proposals afloat in Congress include "offensive cyber tactics, cyber crime laws and the international community's definition of cyber warfare, to name a few."

The author also recommends:

US stokes conflict with North Korea over Sony hacking
[19 December 2014]