THE HILL

The U.S. government's cyber-go-round

By Patrick G. Eddington

February 17, 2015

Official Washington's response to perceived major crises generally follows a pattern: a serious security threat is proclaimed that requires vast new resources and legal authorities to defeat. A "czar" may be appointed to help coordinate the federal response, or even an entirely new military command will be established to meet the challenge. When those efforts fail, a reorganization of the national security apparatus will be the next proposed step. The end result is usually more bureaucratic and policy failure.

The U.S. government has effectively done all of these things in response to the increase in online threats, hacking, and "cyber warfare." The latest episode in the ongoing cyber-drama occurred this week, when White House official Lisa Monaco announced that the administration would soon create a "Cyber Threat Intelligence Integration Center."

Countering cyber threats is already the fragmented responsibility of the Departments of Homeland Security and Defense, as well as the FBI. And given the fact that the head of Cyber Command also happens to be the Director of the National Security Agency, the national security establishment's dominance of the cyber arena is already well advanced—a situation that prompted the resignation of then-National Cyber Security Center director Rod Beckstrom in 2009.

In his resignation letter to then-DHS Secretary Janet Napolitano, Beckstrom stated:

NSA effectively controls DHS cyber efforts through detailees, technology insertions, and the proposed move of NPPD and the NCSC to a Fort Meade NSA facility. NSA currently dominates most national cyber efforts. While acknowledging the critical importance of NSA to our intelligence efforts, I believe this is a bad strategy on multiple grounds. The intelligence culture is very different than a network operations or security culture. In addition, the threats to our democratic processes are significant if all top level government network security and monitoring are handled by any one organization (either directly or indirectly).

In light of NSA's well-documented mass surveillance and storage of data on millions of Americans, Beckstrom's concerns about concentrating government cyber-powers in any single entity seem well founded.

According to Bloomberg, the new cyber threat center will have a budget of $35 million and employ roughly 50 people. Cyber Command alone has at least 3000 staff at present and is seeking to double that number by the end of 2015. In Washington, unless an entity has lots of money and lots of people, it rarely has significant power. That is particularly true in the national security arena. There is little reason to believe at this point that the proposed cyber threat center will not be dominated by NSA and Cyber Command—either directly (through the latter's superior budget and personnel clout) or indirectly (by the former being heavily reliant on detailees and support staff from the two existing agencies).

Monaco indicated that the CTIIC would be modeled on the National Counterterrorism Center (NCTC), as if that model has somehow proven to be a blazing success. As the Senate Intelligence Committee found in the "underwear bomber" case, NCTC proved to be part of the problem.

Indeed, the CTIIC's proposed parent entity, the Office of the Director of National Intelligence (DNI)—was created specifically in the wake of the 9/11 attacks to fix the "failure to connect the dots" problem identified by both the Congressional Joint Inquiry and the 9/11 Commission. The aforementioned "underwear bomber", the Ft. Hood shooter, the Boston Marathon bombers, and even the Charlie Hebdo attackers—all were known to various U.S. government agencies as potential threats before they struck. Our government's problem in countering threats is rarely the result of information deficits, but instead of pulling all relevant threat information together, analyzing it correctly, and disseminating it before disaster strikes.

And if the civil liberties concerns and organizational pitfalls surrounding this latest proposal are not enough to worry you, consider the larger conceptual problem: the federal government is once again attempting to centralize a response to a problem that demands a decentralized solution.

By its very nature, the internet is a vast, distributed system—its infrastructure and users spread literally across the planet. Individuals and organizations who utilize it vary in their level of knowledge of and commitment to practicing sound cyber "hygiene." That is not a problem the federal government can fix, no matter how much money it tries to throw at the problem. And while the U.S. government should be taking the necessary steps to protect its own systems, there is no reason to believe that the creation of yet another federal cyber-related entity is one of them.

Eddington is a policy analyst for Homeland Security and Civil Liberties at the Cato Institute.