FOREIGN POLICY RESEARCH INSTITUTE

E-NOTES

"A nation must think before it acts." - Robert Strausz-Hupé

FEBRUARY 2015

A NEW CYBER AGENCY IS BORN

By Lawrence Husick

Lawrence Husick is an FPRI Senior Fellow, Co-Chair of FPRI's Center for the Study of Terrorism, and Co-director of FPRI's Wachman Center project on Teaching about Innovation.

On February 10, 2015, Lisa Monaco, assistant to the president for homeland security and counterterrorism announced the formation of yet another agency under the aegis of the Director of National Intelligence: the Cyber Threat Intelligence Integration Center (CTIIC) will be modeled on the National Counterterrorism Center (NCTC) and will serve as a center of analysis for cyber threat and cyber protection for the United States.

"The cyberthreat is one of the greatest threats we face, and policymakers and operators will benefit from having a rapid source of intelligence," said Ms. Monaco. "It will help ensure that we have the same integrated, all-tools approach to the cyberthreat that we have developed to combat terrorism." Recent "hacks" against Anthem, JPMorgan Chase, Target, Home Depot, and Sony have highlighted the need for a rapid, cogent, and proactive strategy.

At present, a variety of agencies have overlapping responsibilities in the cyber domain. The Department of Homeland Security, the FBI and the National Security Agency all have cyber-operations centers, and the Air Force has its own CyberCommand, which is tasked with intelligence, offensive and defensive roles. Both the FBI and the NSA integrate threat information and pass it along to other agencies, as well as state, local and tribal officials, and the National Institute of Standards and Technology has been assigned the task of establishing voluntary cybersecurity frameworks for both the public and private sectors. Most of these roles are not expected to migrate to the CTIIC, and no reductions in budget or staff have been announced in any of the existing agencies.

Instead, the CTIIC will begin with a staff of about 50 and a budget of $35 million. If the early history of the NCTC is used as a guide, much of that funding will be used to secure office space and a state-of-the-art command center with dozens of large, bright video displays, reminiscent of NASA's Mission Control. If the organizational model of NCTC is used, much of the time of the staff will be spent in consultation with partner organizations including the Central Intelligence Agency, Defense Intelligence Agency, Department of Agriculture, Department of Defense, Department of Energy, Dept. of Health & Human Services, Department of Homeland Security, Department of Justice, Department of State, Department of the Treasury, Drug Enforcement Administration, Federal Bureau of Investigation, Nat'l Geospatial Intelligence Agency, Nuclear Regulatory Commission, National Security Agency, Transportation Security Administration, and the U.S. Capitol Police.[1]

While the organizational hurdles of establishing and running the new Center are great, the technical task list is not simply Herculean, it is Sisyphean. There are now more than 285 different antivirus programs for the Microsoft Windows environment, alone. As of today (February 10, 2015) computer security company Symantec catalogs 32,875,320 unique computer virus signatures. That number increased by 37 in the last 75 minutes. Computer virus attacks, however, are the proverbial tip of the iceberg. Flaws in operating systems, application software, embedded controllers, industrial systems, and chip microcode are a perhaps greater threat, and the human element - susceptibility to "social engineering" attacks such as phishing emails, popup websites, and poor "cyber hygiene" including sloppy password management threaten government and

[1] http://www.nctc.gov/partnerships.html

private computers and networks, alike. It should be clear that even the most adept 50 government cyberwizards can't and won't stay even modestly informed about the full range of danger facing our cyber-dependent economy, government, and world. Leaks from government and private information systems show that we have yet to implement a useful way to secure electronic information while making it available to those who legitimately must access and use it. These technologies exist (I have personally helped to patent some) but have been roundly ignored -- information security is not a "sexy" technology and not a high priority for most decision makers.

All of this should not be taken as a criticism of the impulse that brought today's announcement. The range and severity of cyberthreats is increasing, and the consequences of cyber disruption should not be underestimated. If we merely assume that our adversaries, regardless of whether they are criminal or state-sponsored, have capabilities that are similar to the catalog of NSA goodies published by Der Spiegel (http://en.wikipedia.org/wiki/NSA_ANT_catalog), then we should recognize that every electronic system is at risk for both data theft and disruption. Because the private sector in the United States has been notably lax in its response to these threats, more often covering up after attacks than spending the amounts necessary to install even a moderate level of protection, it is high time that government take real action.

Unfortunately, after repeated attempts by the President to get a cybersecurity bill through the US Senate were thwarted by holds and threatened filibusters, only a watered-down set of voluntary "frameworks" were proposed by NIST, and even these were criticized as government meddling in the business affairs of the private sector. It is likely that today's creation of a new Center does little to promote actual progress in national cyber defense - the task is too large, the established responses too fragmented, and the new effort, both too small and intrinsically subject to internecine turf wars.

The new Center must yoke gigantic information flows in time that is measured in nanoseconds, to enable responses to "zero day" vulnerabilities lurking in diverse systems built by millions of coders and engineers all over the world. One cannot help but envision the 50 new CTIIC employees, standing next to that brand new wall of video displays, frantically shoving their virtual fingers into millions of virtual holes in an electronic dike, unable to stem the approaching cyber tsunami. For the United States, which invented the Internet and leads the world in computer technologies, there must be a better way.