Defense One

Cybersecurity Outlook

As the Pentagon boosts cyber spending, it's also grappling with new challenges and mandates.

By Stephanie Gaskell and Aliya Sternstein

Maksim Kabakou/Shutterstock.com

In late January, for the second year in a row, Director of National Intelligence James Clapper told Congress that cyberattacks were the top threat to United States national security. For the military, the challenge remains: staff up, train up and get ahead of the curve of the ever-growing cybersecurity threat.

Gen. Keith Alexander, the outgoing head of the National Security Agency and U.S. Cyber Command, warned last year that cyber threats are an increasing threat to the United States. "When you look at the strategic landscape from our perspective, it's getting worse," Alexander said during congressional testimony in March. New technologies—and new threats—emerge almost daily.

While the Pentagon faces a variety of budget threats in the New Year, officials have pledged to protect cyber programs. There's also growing concern that a cyber threat could lead to real conflict. And 2014 will see the controversial Alexander, who was on the hot seat much of the year over the Edward Snowden leaks, exit his dual post in March. On Jan. 30, the Pentagon announced that Vice Adm. Michael Rogers, currently commander of the U.S. Navy's 10th Fleet and U.S. Fleet Cyber Command, would be nominated to replace Alexander.

As the Defense Department boosts cyber spending, it faces a series of challenges, ranging from controlling cyberweapons to assessing whether to set up a cyber militia to protect critical networks.

BIGGER BUDGET

Early this year, Congress approved a fiscal 2014 spending package that includes $447 million for the Pentagon component that launches cyber weapons and deflects hacks against civilian and military networks. That's more than a two-fold increase over Cyber Command's fiscal 2013 budget of $191 million.

The funding jump is mostly attributed to the growth of cyber mission forces, Pentagon officials said. In March 2013, about 834 active duty military and civilian personnel were on staff, Alexander told lawmakers at the time. The goal is to grow cyber forces by 2,000 personnel annually, until 2016.

The boundary where the military takes over network defense from the Homeland Security Department is unclear, since cyberspace is not demarcated by geographic lines. For example, Cyber Command is bulking up "national mission forces" that will thwart incoming digital threats to American power, health care and other critical infrastructure sectors. Homeland Security is responsible for "leading a coordinated national response to significant cyber incidents," a DHS spokesman said last year.

DHS and Defense workforces are straining to protect Americans from disruptive hacks and cyberspying, government officials say.

The number of cyber incidents federal agencies and all other sectors reported to DHS increased by 42 percent between fiscal 2011 and fiscal 2012, to a total of 153,043 cases, according to the most recent assessment of the government's compliance with federal cyber legislation.

CONTROLLING CYBERWEAPONS

Under military legislation passed late last year, federal agencies must work together on guidelines for controlling the trade of cyberwar technology.

In programming, a cyberweapon often refers to malicious code that takes advantage of a software glitch unknown to developers, called a "zero day," to insert itself and manipulate data. For example, Stuxnet, an alleged U.S-Israeli cyberweapon, upended Iranian's nuclear program by exploiting a flaw in the country's centrifuge systems.

The concern in Congress is that war worms, let loose in the black market, are being sold to the public and overseas aggressors.

The 2014 National Defense Authorization Act requires that federal departments, with input from industry, devise "intelligence, law enforcement and financial sanctions" mechanisms to "suppress the trade in cyber tools and infrastructure that are or can be used for criminal, terrorist, or military activities while preserving the ability of governments and the private sector to use such tools for legitimate purposes of self-defense."

THE CONCERN IN CONGRESS IS THAT WAR WORMS, LET LOOSE IN THE BLACK MARKET, ARE BEING SOLD TO THE PUBLIC AND OVERSEAS AGGRESSORS.

The U.S. defense authorization package calls on the administration to craft "principles for controlling the proliferation of cyberweapons that can lead to expanded cooperation and engagement with international partners."

By fall 2014, federal agencies must deliver recommendations for damping the proliferation of cyberweapons, including a draft statement of principles and a review of applicable legal authorities.

CYBER MILITIA

Congress also has mandated that Defense Secretary Chuck Hagel evaluate the practicality of hiring part-time nonmilitary employees to help the National Guard thwart cyberattacks.

Some states and other nations, including Estonia, already have volunteer netwarfare squads poised to protect networks controlling oil reserves, subways and other critical infrastructure in times of crisis.

The corps outlined in the 2014 National Defense Authorization Act would recruit "non-dual technicians," or National Guard personnel who are not required to deploy overseas. Dual-status employees must be uniformed military members and maintain their Defense Department ranks and assignment units.

The authorization measure calls for "an assessment of the appropriateness of hiring on a part-time basis non-dual status technicians who possess appropriate cybersecurity expertise for purposes of assisting the National Guard in protecting critical infrastructure and carrying out cyber missions."

Last year, House and Senate members from both parties introduced legislation that would stand up a National Guard "Cyber and Computer Network Incident Response Team"—or Cyber Guard—in every state. Officials with the National Guard Association of the United States have said they back the proposals, but note Defense officials have argued the teams might sap resources from departmental cyber activities.

IF YOU DON'T KNOW US, YOU SHOULD.

We are General Dynamics Advanced Information Systems.

Through our unique blend of mission understanding, domain expertise and technical agility, General Dynamics Advanced Information Systems delivers enduring cybersecurity solutions, products and services to advance your mission across the full spectrum of cyber operations.

- We defend your network against dynamic threats
- We build to your evolving offensive mission requirements
- We support your critical systems infrastructure operations
- We integrate information assurance into your entire enterprise

GENERAL DYNAMICS
Advanced Information Systems

www.gd-ais.com/cyber