CRS INSIGHT

Information Warfare: DOD's Response to the Islamic State Hacking Activities

May 10, 2016 (IN10486)

Related Policy Issues

- Cybersecurity
- Terrorism and Counterterrorism Policy

Related Author

- Catherine A. Theohary

Catherine A. Theohary, Coordinator, Specialist in National Security Policy and Information Operations (ctheohary@crs.loc.gov, 7-0844)
Kathleen J. McInnis, Analyst in International Security (kmcinnis@crs.loc.gov, 7-1416)
John W. Rollins, Specialist in Terrorism and National Security (jrollins@crs.loc.gov, 7-5529)

The Islamic State (IS) has pursued a strategy of accessing U.S. government computer systems for a variety of purposes. IS pursues five primary categories of activity when targeting U.S. computer systems: defacement, distributed denial of service, data theft, disabling websites, and data breaches. The Department of Defense (DOD) is pursuing a number of activities aimed at detecting, deterring, and thwarting IS hacking activities.

In May 2015, FBI Director James Comey stated, "ISIS is 'waking up' to the idea of using sophisticated malware to cyberattack critical infrastructure in the U.S." and "logic tells me it's coming," and the terror group is "looking into" developing an advanced cyberattack capability. Some government officials have stated that IS has already undertaken attacks against computers that manage U.S. critical infrastructure processes. In October 2015, Caitlin Durkovich, Assistant Secretary for Infrastructure Protection at the Department of Homeland Security, stated at a conference focused on energy sector issues that "ISIL is beginning to perpetrate cyberattacks" on the nation's critical infrastructure. At the same conference, Special Agent John Riggi, Section Chief of the FBI's Cyber Division, stated that while IS has "strong intent (to undertake a cyberattack), thankfully, (they have) low capability."

The "Cyber Caliphate," a group of pro-Islamic State hackers also known as the "Islamic Cyber Army" (ICA) or "Islamic State Hacking Division," has a history of conducting a variety of operations within the information environment. The Department of Homeland Security and the Federal Bureau of Investigation issued a joint statement in December 2014 warning members of the U.S. military that the Islamic State may be mining social media to create "kill lists" of human

targets or to identify potential sympathizers for recruitment. In 2015, the U.S. Central Command's social media sites such as Twitter and Facebook were taken over for a short period of time by hackers claiming to be affiliated with the Islamic State. While this hack may have caused no damage to Central Command's operations, it was apparently designed to create a perception of vulnerability and weak U.S. national security capabilities. Most recently, a pro-ISIS group claims to have hacked the State Department's website, stolen data, and released a kill list of U.S. government officials. In addition, defacing government websites and redirecting web traffic allow the Islamic State to project its power online. Its use of encrypted communication has often enabled the Islamic State to plan and carry out strikes undetected.

The U.S. military has responded to these activities with defensive and offensive cyber operations. The U.S. Cyber Command is building a national cyber mission force composed of three teams, one of which assists combatant commanders in the field with planning and operations. These teams may, for example, target and dismantle violent extremist websites that present an operational threat to troops on the ground. According to Deputy Secretary of Defense Robert Work, the military is "dropping cyber bombs" in order to disrupt the ability of the Islamic State to propagate its narrative, recruit new members, exercise command and control, and execute routine operations. In addition, instead of shutting down the accounts, hacking prominent ISIS members can yield information on their whereabouts, allowing the military to capture or kill key figures in the command structure. The military has also conducted cyber operations to disrupt the Islamic State's use of encrypted communications.

Assessing the potential response to extremists' use of social media websites entails balancing interests. On the one hand, intelligence agencies may desire to know how individuals or groups might use Internet-based communication technologies to recruit, radicalize, and incite to violence prospective members. On the other hand, information contained on social media may suggest an immediate danger to troops that requires the website to be shut down. The tension between a website's threat level and its intelligence value is known as the intelligence gain/loss calculation.

Offensive cyber operations are a tactical component of the strategic concept of Information Warfare. Another component, Information Operations (IO), is defined by the Department of Defense as "the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own." A component of IO is Military Information Support Operations (MISO), formerly known as Psychological Operations, which are planned operations to convey selected information and indicators to foreign audiences to influence the emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. MISO focuses on the cognitive element of the information environment where its target audience includes not just potential and actual adversaries, but also friendly and neutral populations.

One such program, the U.S. Special Operations Command's Trans-Regional Web Initiative, established a series of websites that highlight positive aspects of regional and host country counterterrorism efforts, as well as the negative impact of adversaries' actions. The initiative, which was criticized in a 2013 GAO report on MISO, was effectively canceled by a provision of the Fiscal Year 2014 National Defense Authorization Act. Many other programs are classified and operate in concert with traditional military operations.

The U.S. experience countering the Islamic State in the information environment may have important implications for its future operations. As the 2015 National Military Strategy notes, state and non-state actors with similar interests are aligning themselves against U.S. interests, blurring the lines between irregular and conventional conflict (which scholars describe as "grey zone" or "hybrid" warfare). The information environment is a key domain in which this can occur. For example, some maintain that information and cyber operations against Kiev, including "digital propaganda, denial-of-service campaigns, website defacements ... cutting-edge cyber espionage malware ... and cyberattacks targeting Ukraine's energy grid—critical civilian infrastructure," constituted a major component of Russia's sponsorship of proxies in eastern Ukraine.

As part of its "Goldwater-Nichols at 30" defense reform deliberations, as well as its overall consideration of military policies, Congress may consider what kinds of capabilities the DOD will need to better engage adversaries in the cyber domain. Toward this end, one proposed step in H.R. 4909, the National Defense Authorization Act for Fiscal Year 2017, is to elevate United States Cyber Command, a sub-unified command under U.S. Strategic Command, to a unified

combatant command. Another suggestion by observers is to create a U.S. "cyber service." Nevertheless, cyber operations are but one component of the broader information environment in which U.S. adversaries appear to be operating. Congress may therefore consider whether the proposed DOD steps are appropriate to meet these emerging "grey zone" and "hybrid warfare" challenges.