THE CIVIL-MILITARY DIVIDE: THE ROLE OF THE MILITARY IN DOMESTIC CYBERSECURITY

DR. MAREN LEED, CIVIL-MILITARY FACULTY FELLOW

AUGUST 2021

It seems like every morning, someone can accompany their first cup of coffee by reading about the latest cyberattack. From the December 2020 breach of the SolarWinds information technology (IT) management software that exposed tens of thousands of clients' software, networks, and data to the June 2021 ransomware attack on Colonial Pipeline that sent gas prices soaring, international cyberattacks are increasingly common and of growing national attention.

If the military is supposed to protect the United States and its citizens from security threats, what is its role in defending America's public and private IT systems and data? While not all aspects of this question are fully resolved, Congress has been actively involved in clarifying the U.S. Department of Defense's (DOD) authorities, processes, and mechanisms for ensuring adequate oversight and transparency and in defining substantive limitations on military cyber operations. Much of the legislation has specified how the existing legal framework that has governed the conduct of traditional military activities applies to cyberspace.

While this is a rich and complex topic, there are two basic points useful to understand. First, the military is not in the lead. While DOD (primarily, though not exclusively, through U.S. Cyber Command) has a significant role in defending U.S. interests against cyberattacks, the U.S. Department of Homeland Security (DHS) is the lead responsible agency. Second, the military's plan is to play cyber defense with a strong offense. In 2018, with congressional encouragement, DOD issued a cyber strategy pledging to "defend forward to disrupt or halt malicious cyber activity at its source."

DOD's Supporting Role

Just like defending against physical attacks in the United States, DHS's Cybersecurity and Infrastructure Security Agency (CISA) is the lead federal agency for protecting U.S. critical infrastructure (e.g., the electric and power grids, even though they are privately owned, as well as a number of other critical sectors of the U.S. economy). The Fiscal Year 2021 National Defense Authorization Act also called for the creation of a National Cyber Director within the Executive Office of

the President to provide further coordination and guidance at the highest levels of government. DOD is responsible for protecting its own networks and supports DHS efforts to coordinate cyber protection of the Defense Industrial Base-the labs and private companies that research and build essential military capabilities. It also supports CISA by providing intelligence on cyber threats.

Defending Forward

The military also has clear authority to "defend forward," gaining access to adversary IT networks, watching their activities, and intervening or disrupting if there is a threat to the U.S. military or U.S. critical infrastructure, including election machines. An early example of the strategy in practice is when Cyber Command conducted a cyber attack against a Russian troll farm that was spreading false information about U.S. elections, taking it offline for several days during the election. It conducted additional attacks to help protect the 2020 elections, corrupting foreign malware used to steal financial data and conduct ransomware attacks. The congressionally-mandated and led Cyberspace Solarium Commission, charged with developing a consensus national security strategy, endorsed DOD's "defend forward" approach but called on it to be broadened by involving the tools available to other government agencies such as diplomacy and economic sanctions.

A Complex Policy Area

While Congress has been a very active and constructive partner in helping to advance U.S. cyber defenses, the growing intensity of cyber conflict makes clear that the work is not over. It also suggests that the military will continue to play an integral role in the national response under the authorities and constraints established by law.