12-28-2020

Government cyber breach shows need for convergence

Charles Suslowicz
United States Military Academy, charles.suslowicz@westpoint.edu

Jan Kallberg
Army Cyber Institute, jan.kallberg@westpoint.edu

Todd Arnold
Army Cyber Institute

Opinion

Government cyber breach shows need for convergence

Maj. Chuck Suslowicz , Jan Kallberg , and LTC Todd Arnold December 28, 2020

What does the latest government breach teach us about the interconnection between offensive and defensive cyber operations? (Thitichaya Yajampa/Getty Images)

The SolarWinds breach points out the importance of having both offensive and defensive cyber force experience.

The breach is an ongoing investigation, and we will not comment on the investigation. Still, in general terms, we want to point out the exploitable weaknesses in creating two silos — OCO and DCO.

The separation of OCO and DCO, through the specialization of formations and leadership, undermines broader understanding and value of threat intelligence. The growing demarcation between OCO and DCO also have operative and tactical implications. The Multi-Domain Operations (MDO) concept emphasizes the competitive advantages that the Army — and greater Department of Defense — can bring to bear by leveraging the unique and complementary capabilities of each service.

It requires that leaders understand the capabilities their organization can bring to bear in order to achieve the maximum effect from the available resources. Cyber leaders must have exposure to a depth and the breadth of their chosen domain to contribute to MDO.

Unfortunately, within the Army's operational cyber forces, there is a tendency to designate officers as either offensive cyber operations (OCO) or defensive cyber operations (DCO) specialists. The shortsighted nature of this categorization is detrimental to the Army's efforts in cyberspace and stymies the development of the cyber force, affecting all soldiers.

The Army will suffer in its planning and ability to operationally contribute to MDO from a siloed officer corps unexposed to the domain's inherent flexibility.

We consider the assumption that there is a distinction between OCO and DCO to be flawed. It perpetuates the idea that the two operational types are doing unrelated tasks with different tools, and that experience in one will not improve performance in the other. We do not see such a rigid distinction between OCO and DCO competencies. In fact, most concepts within the cyber domain apply directly to both types of operations.

The argument that OCO and DCO share competencies is not new; the iconic cybersecurity expert Dan Geer first pointed out that cyber tools are dual-use nearly two decades ago, and continues to do so. A tool that is valuable to a network defender can prove equally valuable during an offensive operation, and vice versa.

For example, a tool that maps a network's topology is critical for the network owner's situational awareness. The tool could also be effective for an attacker to maintain situational awareness of a target network. The dual-use nature of cyber tools requires cyber leaders to recognize both sides of their utility.

So, a tool that does a beneficial job of visualizing key terrain to defend will create a high-quality roadmap for a devastating attack. Limiting officer experiences to only one side of cyberspace operations (CO) will limit their vision, handicap their input as future leaders, and risk squandering effective use of the cyber domain in MDO.

An argument will be made that "deep expertise is necessary for success" and that officers should be chosen for positions based on their previous exposure. This argument fails on two fronts. First, the Army's decades of experience in officers' development have shown the value of diverse exposure in officer assignments. Other branches already ensure officers experience a breadth of assignments to prepare them for senior leadership.

Second, this argument ignores the reality of "challenging technical tasks" within the cyber domain. As cyber tasks grow more technically challenging, the tools become more common between OCO and DCO, not less common. For example, two of the most technically challenging tasks, reverse engineering of malware (DCO) and development of exploits (OCO), use virtually identical toolkits.

An identical argument can be made for network defenders preventing adversarial access and offensive operators seeking to gain access to adversary networks. Ultimately, the types of operations differ in their intent and approach, but significant overlap exists within their technical skillsets.

Experience within one fragment of the domain directly translates to the other and provides insight into an adversary's decision-making processes. This combined experience provides critical knowledge for leaders, and lack of experience will undercut the Army's ability to execute MDO effectively. Defenders with OCO experience will be better equipped to identify an adversary's most likely and most devastating courses of action within the domain. Similarly, OCO planned by leaders with DCO experience are more likely to succeed as the planners are better prepared to account for potential adversary countermeasures.

In both cases, the cross-pollination of experience improves the Army's ability to leverage the cyber domain and improve its effectiveness. Single tracked officers may initially be easier to integrate or better able to contribute on day one of an assignment. However, single-tracked officers will ultimately bring far less to the table than officers experienced in both sides of the domain due to the multifaceted cyber environment in MDO.

Maj. Chuck Suslowicz is a research scientist in the Army Cyber Institute at West Point and an instructor in the U.S. Military Academy's Department of Electrical Engineering and Computer Science (EECS). Dr. Jan Kallberg is a research scientist at the Army Cyber Institute at West Point and an assistant professor at the U.S. Military Academy. LTC Todd

Arnold is a research scientist in the Army Cyber Institute at West Point and assistant professor in U.S. Military Academy's Department of Electrical Engineering and Computer Science (EECS.) The views expressed are those of the authors and do not reflect the official policy or position of the Army Cyber Institute at West Point, the U.S. Military Academy or the Department of Defense.