Developing Army Cyber Officers as Operational Commanders

By LTC Justin Considine and CPT Blake Rhoades

The views expressed in this article are those of the authors and do not reflect the official policy position of the 780th MI BDE, United States Military Academy, Department of the Army, Department of Defense, Department of Treasury, or the U.S. Government

Given the rising number of military cyber activities between the United States and its adversaries over the last several years, it is increasingly clear that cyberspace is now an intrinsic part of the current operating environment. As the fifth warfighting domain, it is a space in which we fight and win battles, and its criticality to mission success is becoming more and more apparent with time. As Admiral Rogers recently stated, "(military) leaders must expect that cyber units will sometimes assume the role of main effort when facing U.S. adversaries, as well as a supporting role." Cyber leaders are thus charged with the task of assuming both supporting and supported roles in the cyber domain, which often entails coordinating cyber effects within the planning cycles of our maneuver counterparts.

As leaders of a nascent branch, Cyber Officers are currently in the process of transitioning into a maneuver mindset that is needed for the cyber force to be successful. Such transitions are complicated, however, as the vast majority of newly appointed cyber officers come from Operations Support backgrounds or with no operational background at all. The transitional dilemma poses numerous mission command challenges in the cyber force, threatening the Cyber Mission Force's ability to effectively dominate this crucial domain. This article highlights some of these leadership challenges and proposes a model for addressing problems that jeopardize the effectiveness of the force.

To say that Military Intelligence or Signal Corps officers are inexperienced as maneuver commanders is not a critique of Operations Support branches. Operations support is what these branches were designed to do; thus, these talented leaders have successfully enabled ground combat operations throughout their entire career. Without these branches, the Army would cease to function as it does today. Nonetheless, with the Cyber Corp's aspirational designation as an Operations branch, Army leaders must recognize and embrace that Cyber Officers must be trained and empowered as maneuver leaders who adopt an ethos, and demonstrate the ability and competence, to lead maneuver operations. Without this acknowledgement, Cyber Mission Force teams will be relegated solely to a supporting role.

Cyber leader development and culture must thus be fundamentally different than those of the Operations Support branches. Cyber leaders must be prepared to lead operations as the main effort, to deliver effects at the decisive point of operations, and to manage resources in support of those efforts. Given the carryover from their legacy branches, and the (necessarily) strong emphasis on technical versus tactical expertise, the vast majority of junior cyber officers are not currently prepared to assume such a role. In order for the cyber branch to embrace operations,

its leaders must focus on three areas of change to appropriately transition cyber officers from their role as Operations Support officers into operational leaders: (1) institutional change, (2) structural change, and (3) cultural change.

Institutional change is a major factor of success as the Cyber branch transitions from its legacy unit heritage(s). The Cyber Center of Excellence (CCoE) and school house are the executive agents for Cyber's efforts towards institutional change; both are based at Fort Gordon, GA. Cyber doctrine is an essential component of the CCOE's mission, and is derived from vision and experience. It not only informs the activities of cyber forces, but is vital to the integration of Cyber and Electronic Warfare capabilities into the larger operational force. Thus, doctrine is the foundation that will enable the integration of cyber elements, and thus the role of cyber leaders, into the Army at large.

Cyber branch education and training – also based out of Ft. Gordon - is another important piece of institutional change. Currently, the Cyber Officer's Basic Officer Leader's Course (CyBOLC), Cyber Officer Transition's course, and Captain's Career Course are being established under the auspices of the CCoE's mission, which has the responsibility to train and indoctrinate future cyber leaders in the Army. In the relatively short history of the Army's institutional cyber officer education, much of the curriculum has focused on increasing the technical adeptness for officers that are new to the domain. Unlike Army maneuver institutions, however, cyber leader curriculums do not train officers as supported commanders or operational leaders. There is no exercise at CyBOLC, for instance, which is reflective of the Infantry Officer's experience during their live fire exercises. While traditional maneuver branches train their officers by placing them in supported or supporting command roles from day one, cyber branch is currently focusing on individual skill training to prepare officers for their operational role.

To better prepare Cyber Officers to assume their combat roles, these leaders must be given opportunities to understand the significance of such responsibilities within an academic and training environment. Such opportunities include "live fire" exercises, wherein officers are repeatedly assigned the mission of either supported or supporting operational role. For cyber officers, such exercises would occur between cyber elements conducting Offensive Cyberspace Operations (OCO) and Defensive Cyberspace Operations (DCO) in various supporting and supported roles. They would also consist of Cyber Mission Force elements supporting units from other branches of the Army (i.e. infantry, field artillery, air defense artillery, etc.), and vice versa.

In order for these exercises to occur successfully and for Cyber leaders to be fully integrated into the maneuver force, however, cyber units must first be resourced like other maneuver units. As Table of Distribution and Allowances (TDA) units, they do not receive the full complement of command and staff personnel to be fully mission capable or the equipment necessary to be fully compatible with other maneuver units. Resourcing the cyber force as a maneuver branch, wherein mission capacity is judged by its resourcing status, is a critical factor

to integrating cyber operations with those of its sister branches, both in exercises and "real-world" operations.

In addition to institutionalization of Cyber leaders as operational leaders, command and control relationships within the Army's Cyber force must be engineered to reflect operational leadership and responsibility. Army Cyber unit commanders must not merely act as "force providers" to the future cyber force, wherein unit commanders do not have an operational role. Despite their heritage to Signals and Military Intelligence branch units, Cyber units cannot mimic their Operations Support command and control models. While the "force provider" role (often referred to as the "ADCON" or Administrative Control responsibility) serves a functional purpose in Operations Support units where commanders are tasked primarily with training and readiness, Cyber unit commanders of the future must be tactical experts that are capable of coordinating the efforts of their subordinate efforts. The term "dual-hatted" leader – in which officers lead both an operational effort and Soldier readiness – does not exist within the Operations mentality; combat leaders are the single points of failure for everything the unit does and fails to do. In an environment of persistent cyber conflict, Cyber leaders will need to embrace this role so that they are capable of adequately balancing the priorities of the mission with the welfare and training of the soldiers. These are not and should not be separate roles.

Finally, the Army's Cyber force, and the Army itself, must adapt a culture that supports the concept of Cyber officers as operational Leaders. Like Infantry or Armor officers, Cyber officers must believe and prove themselves to be capable and willing to engage our adversaries at decisive points within the operational environment. Maneuver competence is a key factor that contributes to both the culture of the cyber branch, and its integration into the larger profession of arms. Internal to the cyber units, senior commanders must fully embrace principals of Mission Command, enabling and trusting subordinate leaders to take disciplined initiative to conduct missions.

In order to achieve this level of trust, Cyber Officers must maintain high standards and the branch must have high thresholds for candidate selection. This latter principal is critically important to cyber branch's external efforts to fit in to the existing army culture. Specifically, Cyber Officers must be competent professionals that can earn the trust of leaders from other Operations Branches, and prove themselves capable of delivering decisive effects in support of the other branches as the supported commander. Thus, despite the technical nature of the Cyber branch, it is the principals of Leadership and Mission Command that continue to be cornerstones of effective operations and are ideas that must be central to warfighting in the cyber domain.

This article skims the surface of issues that are currently being address by Army leaders and its cyber leadership. At the Army Cyber Institute, researchers are currently exploring these concepts in depth to support the Army's effort to more efficiently conduct talent management of cyber officers. Such initiatives shape and inform ongoing efforts to assess, recruit, develop and retain a world class cyber force that is capable of fighting and winning our nation's wars in

cyberspace. These Soldiers and Department of the Army Civilians work diligently in the Army's cyber operational units like the 780th Military Intelligence Brigade and the Cyber Protection Brigade. This article advocates operational doctrine, structure, and culture suited to the mission of gaining and maintaining freedom of action in cyberspace and denying the same to our adversaries.

Author Biographies:

LTC Justin Considine is a US Army cyberspace officer currently commanding the 781st Military Intelligence Battalion (Cyber). From 2011 to the present, he has served in cyber assignments from the technical and tactical to the policy and national level, to include Chief of the Army Remote Operations Center, Mission Commander, and Joint Staff Cyberspace Operations Branch Chief in the Deputy Directorate for Global Operations.

CPT Blake Rhoades is a member of the Army Cyber Institute and an Instructor of International Relations in the Department of Social Sciences. From 2012-2013, he was the company commander of the Army's first Cyber National Mission Team at the 780th MI Brigade in Ft. Meade, MD, and has deployed twice as a signals intelligence platoon leader in support of Operation Iraqi Freedom. He holds an M.S. in Information Security Policy and Management from Carnegie Mellon University and a B.A. (Political Science) from the University of Alabama. He was recently selected as a 2016 Madison Policy Forum cybersecurity fellow.