HOW TO GROW A CAPABLE CYBER OFFICER

LT. COL. JUSTIN CONSIDINE

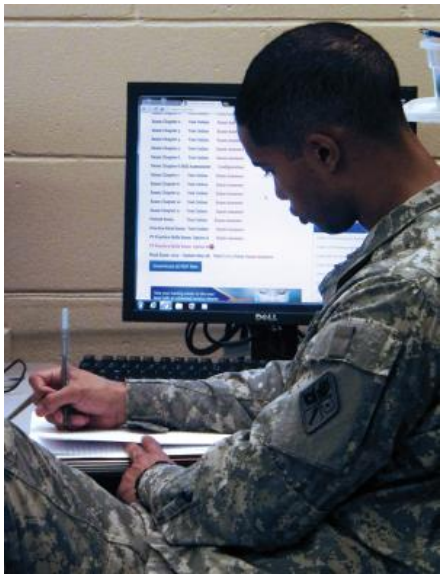
CAPT. BLAKE RHOADES

Tuesday, December 13, 2016

Given the rising number of military cyber activities between the U.S. 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 Adm. Michael S. Rogers, commander of U.S. Cyber Command, recently noted, military leaders should expect cyber units to be able to assume the main role as well as the supporting role when facing U.S. adversaries. This often entails coordinating cyber effects within the planning cycles of our maneuver counterparts.

As leaders of a nascent branch, cyber officers are 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 have no operational background at all. The transitional dilemma poses numerous Mission Command challenges in the cyber force, threatening its ability to effectively dominate this crucial domain.

To say Military Intelligence Corps and 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 careers. Without these branches, the Army would cease to function.



A student takes notes during a Cyber Basic Officer Leader Course at the U.S. Army Cyber Center of Excellence, Fort Gordon, Ga.

Nonetheless, with the cyber corps' 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 supporting roles.

Cyber leader development and culture must 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 prepared to assume such a role. 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: institutional change, structural change and cultural change.

Institutional Change

Institutional change is a major factor of success as the cyber branch transitions from various legacy unit heritages. The U.S. Army Cyber Center of Excellence and schoolhouse are the executive agents for cyber's efforts toward institutional change; both are based at Fort Gordon, Ga. Cyber doctrine, an essential component of the center's mission, is derived from vision and experience. It not only informs the activities of cyber forces but is also 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 the role of cyber leaders, into the Army at large.

ARTICLES FROM OUR LATEST ISSUE

Radical Change Is Coming: Gen. Mark A. Milley Not Talking About Just Tinkering Around the Edges

The Three Major Effects of Military Blogs

Take These Steps To Change Our Army

That's Edutainment: Connecting With the Youngest Generations of Soldiers

How to Grow a Capable Cyber Officer

On the Move With a Large Army Family

Command Climate Guidance Falls Short

January 2017 Reviews

Cyber branch education and training, also based at Fort Gordon, is another important piece of institutional change. Currently, the Cyber Basic Officer Leader Course, Cyber Operations Officer Course and Captain's Career Course are being established under the auspices of the Cyber Center of Excellence, 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 who are new to the domain.

Structural Change

Unlike Army maneuver institutions, however, cyber leader curriculums do not train officers as supported commanders or operational leaders. For example, there is no exercise at the Cyber Basic Officer Leader Course that reflects the infantry officer's experience during live-fire exercises. While traditional maneuver branches train officers by placing them in supported or supporting command roles from Day One, the cyber branch is currently focusing on individual skill training to prepare officers for an operational role.

To better prepare cyber officers to assume 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 and defensive cyberspace operations in various supporting and supported roles. They would also consist of Cyber Mission Force elements supporting units from other branches of the Army—for example, infantry, field artillery and air defense artillery—and vice versa.

An instructor reviews lessons with future cyber operations officers at Fort Gordon, Ga.

In order for these exercises to occur successfully and for cyber leaders to be fully integrated into the maneuver force, cyber units must first be resourced like other maneuver units. As table of distribution and allowances units, they do not receive the full complement of command and staff personnel to be fully mission capable. Nor do they receive 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 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 who are capable of coordinating the efforts of their subordinate efforts. The term “dual-hatted” leader, when 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 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.

U.S. Military Academy cadets participate in a cyber defense exercise.

Cultural Change

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 the culture of the cyber branch as well as 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.

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 the cyber branch's external efforts to fit in to the existing Army culture.

Specifically, cyber officers must be competent professionals who 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, the principles of leadership and Mission Command 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 addressed by Army leaders and the service's cyber leadership. For example, at the U.S. Military Academy's Army Cyber Institute, researchers are exploring these concepts in depth to support the Army's efforts 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.

Cyber

FOLLOW US

SHARE YOUR OPINION

Do you think the Army Combat Fitness Test is the right physical fitness assessment for the Army?

Yes

63% (15 votes)

No

13% (3 votes)

Bring back the Army Physical Fitness Test

25% (6 votes)

Total votes: 24

QUICK LINKS

- Find a Chapter
- Career Center
- Upcoming Events
- Podcasts
- Donate
- Shop

THE ASSOCIATION OF THE UNITED STATES ARMY

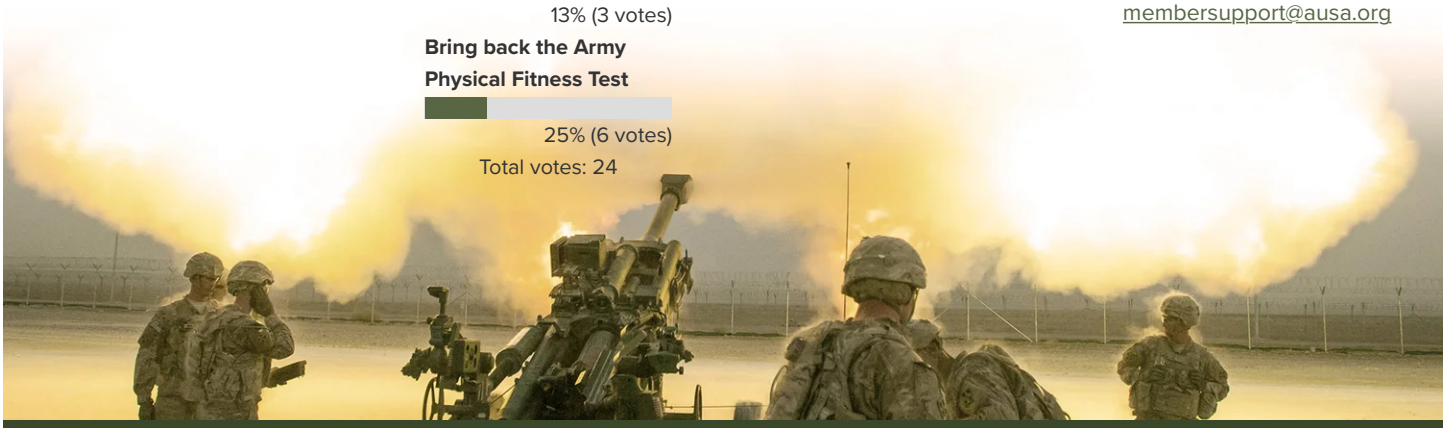
2425 Wilson Blvd.

Arlington, VA 22201

Phone: 703-841-4300

Member Services: 1-855-246-6269

Email: membersupport@ausa.org



 | Home | Work at AUSA | Privacy Policy