WAR ON THE ROCKS

The Challenge of Educating the Military on Cyber Strategy

Erica Borghard, Mark Montgomery, and Brandon Valeriano

June 25, 2021

Malicious cyber activity is ranked by some as the primary threat to international security. The strategic implications of cyberspace are particularly salient in the military context. From an offensive perspective, the military has developed concepts for the use of cyber capabilities as an independent instrument of military power, as well as their use as part of shaping activities to enable conventional operations on the battlefield. From a defensive perspective, the U.S. Department of Defense is as vulnerable to cyber threats to its networks and critical warfighting capabilities as the rest of U.S. society, if not more so. Yet there are significant gaps in how the military educates the officer corps as a community about the nature and practice of cyber strategy and operations.

The professional military education system faces several challenges in how it teaches future leaders practicing the profession of arms in the cyber domain. Cyber strategy programs are inconsistent across the services, are often under threat of funding cuts, and can be altered capriciously in the absence of clear guidance on what needs to be taught. Moreover, some core professors in the cyber security field have limited practical experience, while others have limited academic background in teaching cyber strategy. Military reading curriculums more often feature fictional takes on cyber security than rigorous empirical accounts of the domain. War colleges and service schools have significant room to improve how they educate the officer corps to understand the cyber and information environment, including the core concepts and legal authorities critical to the domain.

The Cyberspace Solarium Commission was tasked with evaluating U.S. national cyber strategy and promoting the conditions to harness U.S. power in the cyber domain. In the context of improving U.S. military capabilities in cyberspace, the commission found that it would not be sufficient to just grow the cyber force or improve acquisition authorities. Rather, it is essential for military leaders across the services — beyond those directly engaged in planning and implementing cyber operations — to have a fundamental understanding of the role of the cyber domain in military operations and strategy. The commission's March 2020 report contains a specific recommendation to enhance support for education on cyber strategy within the professional military education system. Specifically, the commission recommended that the war colleges and service schools establish permanent teaching and research faculty (sometimes called "Title 10 professors" at these institutions) "to communicate and investigate cyber strategy and policy at the national level as it affects the armed forces." This recommendation was intended to institutionalize cyber strategy education in professional military education institutions.

However, as the commission staff began to work on the implementation of the recommendation, we recognized that simply creating positions for professors would not address the full scope of the problem. Rather, the U.S. military should establish standardized and institutionalized *programs* — not just professors of cyber strategy — across the services to ensure an appropriate level of military cyber education.

Implementing Cyber Security Education in Professional Military Education

On the modern battlefield, warfare will inevitably involve cyber operations integrated or in tandem with conventional operations. Divergent opinions about the utility of modern technology on the battlefield are exacerbated by a lack of understanding about the applications of technology to modern strategy. Therefore, U.S. military officers should be trained to understand how technologies like cyber operations are integrated into modern warfare, including an exploration of the history of emergent technology and its impact on the military. The military education community should seek understanding of how the deployment of modern capabilities allows new considerations in strategy formation and practice. Cyber specialists have a requirement to understand the implications of cyber tools because it is their core expertise. However, it is also valuable for warfighting officers (e.g., Navy "unrestricted line" or Army "combat arms") to have an advanced understanding of the role of cyber operations. From a defensive perspective, for example, sensitizing non-cyber specialists to how adversaries may exploit the cyber vulnerabilities of the weapon systems and equipment they operate can promote the resilience of those systems, particularly in a combat environment. From an offensive perspective, better appreciating the role of cyber effects on the battlefield can improve how different capabilities work together — just as infantry and artillery officers are more effective when they understand how their respective movements and maneuvers contribute to achieving the overall objective.

Three military education programs stand out as promising for their focus on cyber security education and research, often providing unique degrees and certificates not available in civilian education. First, the National Defense University's College of Information and Cyberspace has traditionally taken the lead on cyber education. It plays the role of coordination center for the Department of Defense University Consortium for Cybersecurity, and serves as coordinator for the National Centers of Academic Excellence for Cybersecurity. The College of Information and Cyberspace could continue to provide overarching guidance to the broader Department of Defense effort — provided critical gaps are remedied. The continued existence of the College of Information and Cyberspace has been under threat from the Department of Defense for some time, which has reduced capacity through the attrition of personnel due to funding reductions.

Second, the Naval Postgraduate School plays a critical role in the military's cyber education system. Its longstanding Cyber Academic Group provides technical expertise unique in the professional military education system. Supported by the National Security Affairs and Defense Analysis departments, the school offers courses in cyber strategy through the Cyberspace Operations Fundamentals course. Through the Institute for Security Governance, the Naval

Postgraduate School is also building cyber courses that focus on cyber strategy, policy, and operations.

Finally, the Air Force Cyber College, a new entrant in the system, has rethought how to teach disruptive technologies to student bodies. The college offers professional cyber education to the Air Force and is developing a master of arts program in cyber strategy. Of specific interest is the course titled Cyberspace and Strategic Competition, which prepares students for "strategic level military and government service through the study of national security strategies and statecraft with a focus on cyberspace." The Air Force Cyber College is also preparing a cyber leadership certificate in coordination with the National Security Agency, which provides 12-credit distance learning certificates to Air Force officers who have a cyber consideration in their billets. The faculty is interdisciplinary and comprises Ph.D.s, J.D.s, and reservists who instruct the officer corps, providing a unique diversity of knowledge and experience.

The three programs described above serve as exemplars in the professional military education system and should be enhanced and institutionalized, so they are not at risk with each change of command or changes in leadership at the national level. With institutionalization would come clear standards and collaboration across units to achieve parity.

It is also important to note that the service academies (West Point, Naval Academy, Air Force Academy, Coast Guard Academy, and Merchant Marine Academy) also offer important cyber security education to the incoming commissioned officer corps. Gaining a foundation in cyber strategy and operations at the beginning of an officer's military career is beneficial. However, this is taught prior to individuals having developed the tactical and operational perspective that is important for understanding how to integrate cyber operations into operational planning. Therefore, while these programs certainly provide value, they should not preclude the development of more robust programs at the mid-career point, particularly given the dynamism of the cyber field and the operational and command responsibilities of more-senior officers.

Of course, there are other groups in the defense enterprise that conduct cyber research. For example, the Naval War College hosts the Cyber and Innovation Policy Institute and the Army Cyber Institute is located at West Point. Both institutes produce useful cyber research and academic work, but neither has clear teaching or training responsibilities (with the exception of academic instruction to the Corps of Cadets, in the case of West Point). Our focus here is on educating the warfighting officer corps — particularly at the senior O-3 level and above — to meet the challenges of cyber competition, rather than on research.

Therefore, to address gaps in existing programs, we recommend that Congress should direct the Department of Defense to conduct an in-depth study of its cyber strategy education offerings and provide a recommendation on the design of a comprehensive education program. This sort of comprehensive effort is not that far out of reach. First, each of the services should be offering significant programs in cyber strategy at their war colleges. The Air Force Cyber College sets a strong example of what this could look like. Moreover, the services should ensure that this effort is integrated across all of their professional military education programs, to include each service's specific planner school (e.g., school of advanced warfighting, school of advanced military studies). Second, the degree granting programs in development at Air Cyber and Naval Postgraduate School should be offered to the entire joint force, as these programs remain ahead in terms of both the quality of instruction and their focus on cyber strategy and operations. Third, each service academy should continue its efforts to introduce the topic of cyber strategy to future officers and efforts should be enhanced to make this topic available in reserve officer training programs, as well. Finally, the College of Information and Cyberspace program at National Defense University should provide the overall direction and offer advice to each service as they expand offerings to their respective officer corps.

To operate in new domains the military education community should develop new ways of thinking about organizations and processes to develop and implement strategy. Simply hiring professors to teach cyber strategy will not address the full scope of educating military leaders. Therefore, the Department of Defense should focus to gather the limited talent available to train future leaders, otherwise superficial offerings will only do a disservice.

Institutionalizing the Solutions

Additionally, institutionalizing a cyber education requirement in U.S. code is important to ensure the longevity of these programs. Therefore, in addition to maturing existing professional military education cyber programs, Congress should revise U.S. code, which sets joint professional military education standards, to include cyber and information operations strategy as core requirements. Currently, 10 U.S. Code § 2151(a) outlines joint professional military education requirements but makes no mention of educating the force about planning operations in the cyber domain. Instead, it refers to “joint planning at all levels of war.”

The language in U.S. code that establishes these standards is vague by design, which will still provide the services with considerable latitude to interpret that requirement. However, absent specific references to the cyber domain in U.S. code, competing requirements may crowd out a focus on cyber security and strategy as curriculum and leadership change. Amending U.S. code is not an insurmountable hurdle: it was recently revised to include “operational contract support.” Therefore, on its face, there is little reason to deny similar adjustments to other emerging domains as they become necessary to improve the ability of the profession of arms to understand the evolving impact of technology on combat.

That said, amending U.S. code is not a panacea, especially given how the language in law is broadly construed. Therefore, additional measures, such as establishing common cyber education standards in the chairman of the Joint Chiefs of Staff’s *Officer Professional Military Education Policy*, which provides professional military education guidance across the services, can help institutionalize and refine cyber curriculum standards. This guidance is also more adaptable, as the environment — and the resulting operational needs and challenges — evolves.

Without meaningful change and investment in professional military cyber education, service efforts will likely remain in a state of flux and uncertainty. The potential consequences of maintaining the status quo are significant. For instance, academic research on military innovation has shown that military organizations adapt poorly to modern technology when they are not sufficiently educated on the dynamics of change. Budget cuts are a fact of life in the military community, but so are cyber and information operations. In the absence of strong educational foundations, the military is at risk of being unprepared to engage in rigorous thought about the future application of technology on the battlefield.

Brandon Valeriano is a senior fellow at the Cato Institute and a senior adviser with the U.S. Cyberspace Solarium Commission.