Marine Corps High Mobility Artillery Rocket System conducts dry-fire exercise during exercise Rim of the Pacific 2014 (U.S. Marine Corps/Aaron S. Patterson)

Cyber Security as a Field of Military Education and Study

By Eneken Tikk-Ringas, Mika Kerttunen, and Christopher Spirito

Information and communication technologies are acknowledged as enablers and the core arsenal of military capabilities, functions, and operations.[1] An increasing number of nations pursue improved fluency and agility of armed forces personnel in information and communication technology, its contemporary uses, and relevant defense and security implications. Underdeveloped terminology and concepts, combined with recognized functional needs and national ambitions to control the relatively new battlespace and domain, create ambiguity and even anxiety among the current generation of planners and leaders. Particularly challenging is the balance between technical in-depth knowledge requirements and strategic understanding of the cyber domain desirable for joint planners, field commanders, and senior decisionmakers.

Several conceptual and practical questions must be resolved by military education institutions through cyber security and defense as a field of study and education. Based on empirical observations on joint and senior-level education, this article addresses the problems of conceptual confusion and contextual diversity in military cyber education.[2] It offers views on curriculum development and tentative ways to address the problems and develop both content and methods of education with emphasis on officer career courses at military academies and defense and war colleges.

Dr. Eneken Tikk-Ringas is a Senior Fellow for Cyber Security at the International Institute for Strategic Studies–Middle East. Dr. Mika Kerttunen is the Director of the Department of Leadership at the Baltic Defence College. Christopher Spirito is the International Cyber Lead at The MITRE Corporation.

Key Problems

Students and decisionmakers find it difficult to understand the term *cyber*. Cyber security and defense referring to and dealing with tangible concepts such as computers, networks, and information assurance are understandable; however, alternatively *cyber* is used to cover anything based on Internet protocol (IP) traffic, comprising the users as part of the definition, or being coterminous with electricity or electromagnetic spectrum.[3]

The essence of education easily remains blurred as key concepts are either undefined or incommensurably defined by different epistemic communities or administrative entities. One only need ask: what is the relation of "cyber security" and "cyber defense"; how does a "cyber attack" relate to "cyber warfare"; or does "cyber war" actually mean anything, or is it an intentionally constructed flickering illusion?[4] Indeed, it remains to be seen if *cyber* as a term survives or will be rejected over time, not least because of the conceptual confusion that remains even within Western countries as to what it means.

Terminological and conceptual confusion is aggravated by the lack of taxonomy and missing links between allied and national doctrines. One need also critically examine whether or which 2,000-, 200-, or 20-year-old theories of war and operational concepts translate into the age of information and precision. Clausewitzian concepts such as hatred, center of gravity, or the superiority of defense over offense might appear different, even outdated, in the cyber era and space. Contemporary armed forces need to possess situational awareness beyond their immediate tasks and duties. For example, the Schmitt test to determine if an incident meets the threshold of use of force or armed attack requires competence often not belonging to an officer's area of expertise or available within and from the domain immediately under their command.[5] The speed and stealth of cyber maneuvers and effects intensify the presented challenges.

These inconsistencies make it difficult to make officer cohorts understand cyber as a concept and address it in a constructive manner, yet they should not be seen as diminishing the need to grasp the role of advanced technology in the current and future role of armed forces. Any contemporary operation or mission and up-to-date combat, combat support, and combat support service function is likely to involve cyber components or capabilities and therefore require a fundamental understanding of technology and a developed understanding of its use.

Right now, the level of awareness of cyber as an environment and as a tool typically is low among the audience, making it difficult to introduce more sophisticated and complex issues and to design far-reaching education and training strategies. However, it must be noted that the lack of general understanding is a generational issue, and the problem of current leadership not having proficiency in or even a basic understanding of the cyber domain should be to some extent resolved within the next decade.

National requirements sent to cyber warriors and cyber-savvy officers vary from country to country. Usually in smaller countries, officers are educated as generalists expected to cover broad fields of expertise during their service. They are often required to perform functions up to two levels above their rank. Similarly, national and cultural values and habits are reflected in command and control and leadership functions. One only needs to compare the Nordic interpretation of mission command emphasizing the independence of the subordinate to the U.S. Army interpretation focusing on the control aspect to realize the different educational preferences.[6] The diverse background of joint or international officer courses and varying levels of prior knowledge of students further underline the educational and conceptual challenge of creating lectures and discussions to match the requirements and target audience's justified expectations.

In leader education, the questions of autonomous decisionmaking and independent thinking and action are paramount. Since the cyber domain and cyber operations require agility, adaptability, and creative and critical thinking, students with a common military mentality and an expectation of clear concepts, templates, and orders-based execution that previously served them well may find they are not thinking out of the box but operating out of their comfort zone.[7]

Observations on Curricula

Comprehensive cyber defense and cyber security curricula for military education are still works in progress. Many professional military educational institutions tend to offer either tactical/technical (information assurance and security) or strategic/conceptual (policy and doctrine) level training and education, whereas joint and operational studies remain in the background as difficult to compile and deliver.[8]

However, understanding available cyber capabilities and assets and their potential use as well as threats is essential for service and joint level staff officers and commanders. Officers, regardless of their rank or position, must be able to assess their operational environments from a cyber perspective and be aware of the basic platforms and cyber capabilities. Field commanders are required to actively pursue cyber options in their missions and within their area of operations. They need to understand how to deliver a cyber effect and know the potential political and legal consequences of the decisions and actions—for example, wiping out all local communications— and especially relating to third party infrastructure. Commanders must be able to estimate when it is safe to assume or accept a cyber risk. Without such a skill, officer students cannot qualify as commanders, planners, or decisionmakers. Furthermore, it is important to be able to implement footprint control—that is, to assess electronic exhaust and determine how much one leaves behind or gives away. Commanders need to ask about IP security, patching, or radio frequency identification attacks against their own systems as they need to be aware of casualties, consumption, or morale. Joint and senior level cyber curricula must discuss appropriate levels of decisionmaking. This discussion of responsibilities and cyber rules of engagement easily returns to a conceptual jargon-talk; thus, tangible field examples must be found or developed.

Elements and aspects of cyber security and defense form an important part of higher level education. "Cyber capabilities and their use in war and peacekeeping" and "planning the use of cyber capabilities" should constitute the core themes of any joint and senior level officer course. Recognizing mutual spectrum co-dependency in a conflict provides two parallel perspectives on cyber operations that officers must grasp: how to defend against attacks and how to exploit spectrum dependency to execute attacks.[9]

Currently, due to the lack of prior systematic cyber security and defense education, the joint and senior level audience is often required to work through weeks of learning and study material in a few days or even hours. However, it could be estimated that to combine the required cadet, service, joint, and strategic level studies, cyber security and defense themes would easily add up to 5 to 6 weeks of intensive studies.[10] Any curricular planning should therefore focus on the full cycle of officer education rather than attempt to revisit the same items at all level of studies.

The Baltic Defence College's model reference curriculum on cyber security and cyber defense forms a matrix between the four levels of officer education—cadet/junior officer, intermediate/service, joint operational, and senior—and four identified interdisciplinary core study areas—fundamentals, capabilities, operations, and additional aspects—that seek to logically proceed from general to specific and from academic to military. At the first level of studies—cadet/junior officer education—the emphasis is on basic technical and scientific foundations and basic cyber hygiene as well as the individual contribution to cyber security and defense. At the service/joint operational levels, the emphasis is on service-specific and joint capabilities and the planning for and use of those capabilities in operations. At the senior level, strategy and policy formulation, international relations, diplomacy, and campaign design will be more thoroughly addressed. The reference curriculum is hoped to provide developed understanding of training and education needs as well as a solid foundation to develop a handbook on cyber defense.

Soldier connects with call manager during Cyber Endeavor, annual exercise designed for multinational operations in European theater (U.S. Army/Shawnon Lott)

Separating cyber as an area of studies should be seen as an interim solution on the way to treating the cyber domain and information and communication technologies as an essential and omnipresent aspect of all operations and functions. To create full cyber awareness, it is of utmost importance not to treat cyber themes as a separate area or discipline that one can enter and leave. As incoming students gradually become more competent and confident, more demanding and specific cyber security and cyber defense topics can be introduced into the curricula.

Educational Ways Forward

A simple solution to the above-described problem of basic computer and Internet illiteracy is to include competency tests and selected readings before lecture sessions. To create technical competency and make students comfortable with the domain, it would also be beneficial to have hands-on, engaging, and "fun-tech" courses before or between other classes. It is also preferable to decisively show what is gained from each element of study and how it is tied to particular requirements an officer actually needs to know, understand, and do.

To make cyber security and cyber defense more concrete and understandable, identifying relevant capabilities at small unit, larger brigade, air wing or corps size formations, and national levels is helpful. Investigating how these capabilities have been or can be used in the core functions of military operations such as command and control, intelligence, maneuver, interdiction, targeting and fire, logistics, and sustainment makes students comprehend cyber as an omnipresent and essential aspect.

Cyber defense and military cyber security need to be outlined in the context of the full spectrum of cyber security concerns reaching from basic cyber hygiene to civil-military cooperation and cyber diplomacy without overstretching the proportion of it. National strategies and service doctrines can be analyzed, compared, and critically scrutinized to understand different political and bureaucratic frameworks and factors and to appreciate different views and solutions to cyber operations and capabilities. Such an approach would integrate the notion of cyber to essential, concrete, and familiar concepts and practices; conceptual themes would become real and hopefully better appreciated and acknowledged.

We also advise distinguishing non-organic, reach-out cyber capabilities such as advanced intelligence from integrated, organic capabilities. Naturally, the focus and levels of learning at officer courses differ from those at technical and specialist courses. Whereas the latter focus is on hands-on, in-depth technical and tactical skills, officer education particularly at joint and senior levels aims to develop understanding of concepts, knowledge of the use of cyber capabilities in military operations, and the ability to design and define strategies, policies, and future capabilities.

A culture and mindset of reporting and individual responsibility similar to organic or delegated resources need to be created within cyber operations. Questions such as "what constitutes cyber in war?" and "who is considered a cyber warrior with what responsibilities in a particular organization and organizational culture?" must be addressed when preparing the curriculum.

Investigation of known incidents and modi operandi enables one to combine conceptual issues to real capabilities and operations; this will increase motivation to learn. There is a demand for well-researched, theoretically anchored, and thoroughly documented cyber case studies. Loose references to "Estonia," "Georgia," or "Stuxnet" that only support individual prejudice or organizational bias are not hallmarks of high-quality education.[11] Alongside truthful, credible accounts of the attacks and operations, speculative *what if* and normative *what should* questions both test students' competence and take discussions further. In this context, the demanding issue of civil-military roles, responsibilities, and interaction in the cyber domain can be addressed.[12]

There is a pressing need for comprehensive, well-referenced study materials to comprise the essentials of all levels of study and provide links to existing materials, concepts, and discourse. Such materials should link the concepts of cyber security and cyber defense to military theories and, more importantly, operationalize the theories, ideas, and concepts according to strategic, operational, and tactical levels and service and joint functions and operations.

It is plausible to conclude that officer cyber education must address and depart from the principal debates within cyber defense discourse. First is the education debate between a narrower focus of protecting and enabling one's own networks and network-based service and a wider interpretation, recognizing cyber as an asset by using those networks and services also to deliberately cause, enforce, and project hostile cyber effect on the adversary's systems and networks. Second, officer education needs to deal with the diverging views of the cyber element as an integral aspect or a separate function. As pointed out, demands of understanding and awareness of cyber concepts, capabilities, and threats do not fundamentally differ from the cognitive and educational requirements of mastering other operating environments, capabilities, and effects. Third, the interrelated roles and responsibilities between individuals, armed forces, and civilian society, including the private sector, must be examined and understood. Addressing these three debated and most practical areas would help to clear the terminological and conceptual fog of cyber as well as broaden and deepen understanding of cyberspace and the use of cyber capabilities. Finally, grasping cyber requires a broad set of educational methods. To be able to provide hands-on experience, thought-provoking readings and lectures, group discussions, debates, and exercises in which conceptual knowledge can be applied demands due consideration by military educational institutions of investments into the skills and competence of their directing staffs. Understanding the multifaceted nature of cyber security and defense and the broad requirements it sets for any military officer is the first step forward. JFQ

Notes

[1] See, for example, General Sir Nick Houghton observing that the British armed forces are critically deficient in the capabilities that enable the joint force, including intelligence, surveillance, and compatible communications. Richard Norton-Taylor, "Defence chief: UK armed forces have good equipment but not enough people," *The Guardian*, December 18, 2013, available at <www.theguardian.com/politics/2013/dec/18/defence-chief-uk-armed-forces-equipment-nick-houghton>.

[2] Our experience and observations are based on designing and implementing information assurance and cyber security and defense courses, modules, and workshops for joint and senior level officer and civil servant courses as well as for targeted national authorities and external customers in the Nordic-Baltic region, Gulf region, and the United States.

[3] The use of the term *cyber* derives from U.S. diplomatic culture and has been implemented into U.S. military doctrine as a domain control ambition involving nonstate actors as potential adversaries and targets. In contrast, North Atlantic Treaty Organization (NATO) doctrine restricts the use of *cyber* to protection of networks and strategic information assurance. See NATO, "Defending the Networks: The NATO Policy on Cyber Defense," 2011, available at <www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefense.pdf>.

[4] See, for example, Martin C. Libicki, "Don't Buy the Cyberhype: How to Prevent Cyberwars from Becoming Real Ones," *Foreign Affairs*, August 14, 2013, available at <www.foreignaffairs.com/articles/139819/martin-c-libicki/dont-buy-the-cyberhype>.

[5] Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," *Columbia Journal of Transnational Law* 37 (1998/1999), 890–937.

[6] On the concepts of mission command and command and control, see, for example, Field Manual 6-0, *Mission Command: Command and Control of Army Forces* (Washington, DC: Headquarters Department of the Army, 2003); and Marine Corps Doctrinal Publication 6, *Command and Control* (Washington, DC: Headquarters Department of the Navy, 1996).

[7] On the cognitive and intellectual challenges at joint and senior level officer education, see, for example, Joan Johnson-Freese, *Educating America's Military* (London: Routledge, 2013).

[8] Observations based on study visits to several U.S. and all Nordic defense and war colleges.

[9] James P. Farwell and Rafal Rohozinski, "The New Reality of Cyber War," *Survival* 54, no. 4 (August–September 2012), 107–120.

[10] An estimate based on the work on the Reference Curriculum on Cyber Security and Defense to be mentioned later.

[11] On the demands of proper case study methodology, see Robert K. Yin, *Case Study Research: Design and Methods* (London: Sage, 2014).

[12] As examples of national cyber security strategies emphasizing interagency cooperation, see *The National Cyber Security Strategy* (The Hague: Ministry of Security and Justice, 2011); and *Finland's Cyber Security Strategy* (Helsinki: Secretariat of the Security Committee, January 24, 2013).