Players participate in Defend Forward: 2019 Critical Infrastructure War Game at U.S. Naval War College, July 25, 2019, Newport, Rhode Island (U.S. Navy/Tyler D. John)

Accelerating Cyber Leader Development

A Call to Action for Service War Colleges

By Alfredo Rodriguez III

Cyber leaders find their organizations under constant cyber attack from millions of daily intrusions disrupting everything from our electoral system to our social media feeds. The 2007 cyber attacks on Estonia, the set of cyber attacks on Iran's nuclear enrichment facility at Natanz, and the 2014 Sony Pictures data hack are a few headlines at the tip of the iceberg. Today, cyberspace provides both technological opportunity and vulnerability. Electronic banking, utilities, health care—everything seems increasingly dependent on a network of digital devices that store, process, and analyze data. The frightening reality is that the Nation is adrift in a dangerous cyberspace domain, a warfighting domain that stores, processes, and analyzes data under the uncertain eye of ill-prepared senior cyber leaders. This article is

Alfredo Rodriguez III is the Enterprise Cyber Workforce Program Manager at Headquarters, U.S. Marine Corps, Deputy Commandant for Information, Workforce Division.

Marines and civilians with Marine Corps Cyberspace Warfare Group and Marine Corps Cyberspace Operations Battalion compete in Cyber Flag 23-2, at undisclosed location, August 7, 2023 (U.S. Marine Corps/Brian Stippey)

squarely focused on a recommendation to deliberately develop senior cyber leaders within the Department of Defense (DOD) to win in this dangerous battlespace.

Despite robust defensive capabilities in this domain, attacks on the United States persist. The attackers operate on the digital battlefield without the worry of legal ramifications. In an era of strategic competition, Chinese operators push to steal intellectual property and continue to inch closer to economic and military parity with the United States. Russian operators and their proxies overtly damage public trust in the integrity of the U.S. election process and democratic institutions overall.[1] U.S. infrastructure is relentlessly probed, and criminals leverage global networks to steal assets from individuals and companies alike. This environment has the potential to mute the military instrument of power in its traditional sense. Those who understand how cyberspace shapes the world will adapt methodologies, doctrine, and practices to ensure their militaries can meet the challenges. The opening letter from Senator Angus King (I-ME) and Representative Mike Gallagher (R-WI) in the U.S. Cyberspace Solarium Commission highlighted what is at stake: "The status quo is inviting attacks on America every second of every day. The status quo is a slow surrender of American power and responsibility. We all want that to stop."[2]

Current Posture

The 2019 National Defense Authorization Act (NDAA) charted the first U.S. Cyberspace Solarium Commission to address cyberspace challenges. This commission was an initial step at the national level to define the strategic approach to defend the United States against cyber attacks of significant consequence.[3] The Solarium report discusses the implementation of national policies to recruit, develop, and retain cyber talent and deepen the range of candidates for government service. Similarly, the DOD Cyber Strategy states:

The Department will adapt its institutional culture so that individuals at every level are

knowledgeable about the cyberspace domain and can incorporate that knowledge into their day-to-day activities. Leaders and their staffs need to be "cyber fluent" so they can understand the cybersecurity implications of their decisions and are poised to identify opportunities to leverage the cyberspace domain to gain strategic, operational, and tactical advantages.[4]

Operations in cyberspace must be treated like operations in the other domains; that is, the Services must commit to the unique career fields for cyberspace officers. These officers will lead or advise on how cyberspace could help influence joint operations. There is a focus on providing highly trained, technically skilled personnel at the enlisted and warrant officer ranks, and the Services can do the same for cyberspace officer career development. Like the other domains, cyberspace requires joint officers who are developed across their careers to prepare them to lead at senior levels in command and staff assignments.[5] Current DOD cyber workforce publications seek to standardize the cyber workforce and establish the foundation on which operational forces will build. These publications are the authoritative DOD reference for coding cyber positions. They are also the foundation for enterprise qualifications for those who operate, support, and lead in the cyber domain. Services will now be accountable for the development and qualification of the employees covered by this DOD Cyber Workforce Framework (DCWF). Specifically, the publications codify the cyber work role for leaders and mandate their development.

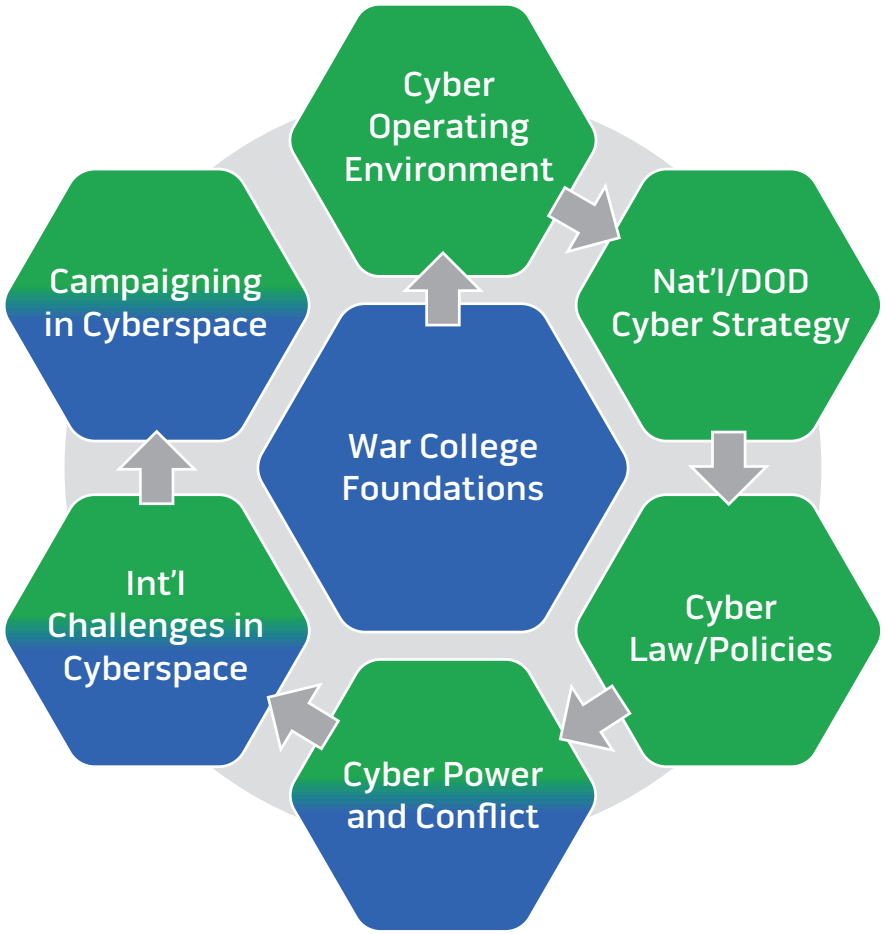
In pursuit of implementing the DCWF, how can DOD leverage the professional military education (PME) infrastructure to develop cyberspace senior military and civilian leaders? How do we prepare senior cyber leaders who will employ or advise on cyberspace and information-related capabilities in support of adaptive joint operations, strategy development, and other national security activities? These gaps prompted DOD to charter a RAND Corporation study to examine its educational institutional approach to cyberspace at the Joint PME Phase II and graduate levels.[6] The study, published just after my research into this article was concluded, recommended the same expansion this article argues for.

Service war colleges should implement a dedicated cyberspace strategic studies track aligned with the DOD Cyber Workforce Framework to develop cyberspace leaders. This pathfinder effort would shape joint PME and the future developmental ecosystem for cyberspace leaders. There must be alignment among our national and DOD strategies, joint PME guidance, and DOD cyberspace workforce directives to build such a program. This article introduces national perspectives on cyberspace, describes current DOD cyberspace workforce directives, and then details how the current joint PME apparatus is well suited to educate future cyber leaders. It concludes with a recommendation on how the Service war colleges can meet DOD requirements by instituting a cyberspace strategic studies track to help DOD succeed in the highly contested cyberspace warfighting domain.

The Cyberspace Leadership Challenge

National and DOD Perspectives. Global digital connectivity has brought us tremendous economic growth, technological dominance, and improved quality of life. The U.S. Cyberspace Solarium Commission report describes the vulnerabilities that come from people's increasing connections and the data they exchange. It notes that the cyber landscape requires a level of data security,

Figure. Cyberspace Strategic Studies Course Essentials Proposal



Note: Blue represents common course content. Green represents specialized course content. Created by author.

resilience, and trustworthiness that neither our government nor the private sector alone is equipped to provide.[7] This landscape offers adversaries unique instruments of coercion, sabotage, espionage, and extortion used for digital, economic, and social overmatch.

The power and reach of cyber operations are growing, and other nations or nonstate actors can pressure the United States without committing military force or declaring their intent. The Interim National Security Strategic Guidance describes this landscape as a "revolution in technology that poses both peril and promise"—a race by global powers to develop and deploy emergent technologies.[8] The Joint Operating Environment 2035 describes the future of science, technology, and engineering as the means to reach technological parity and the ways that allow adversaries to challenge U.S. interests.[9] Warfare in 2035 will be defined by the use of force to disrupt global commons and a contest for cyberspace. The Joint Concept for Operating in the Information Environment refines a central theme to address this challenge and achieve enduring strategic outcomes.[10]

To succeed, the joint force must build cyberspace into operational art to design operations that deliberately leverage the informational aspects of military activities.[11] Leaders must understand cyberspace and informational aspects of military activities and informational power, defined as to "acquire, process, distribute, and employ data to enhance combat power."[12] This understanding requires the Services to integrate physical and informational power into training

Airman 1st Class Aden Gonzales of 83rd Network Operations Squadron participates in 688th Cyberspace Wing's 4th annual tactical-level exercise "Savage Cerberus 23," in San Antonio, Texas, May 12, 2023 (DOD/Nadine Wiley De Moura)

and education pipelines, preparing cyber leaders as multidomain warriors. Innovation and the consistent integration of informational power in operational situations would provide commanders with a broader range of options that maximize military power.[13] The role of cyber leaders within this environment demands cognitive dedication to the fluid environment and its integration across all domains. Our current education of senior cyber leaders at Service war colleges must deliver on this demand signal.

Where We Stand Today. The Cyberspace Solarium clearly stated that the U.S. Government is poorly positioned to lead in cyberspace with the speed and agility needed to secure its interest.[14] The Solarium report suggests the government is weighed down by industrial-age bureaucracy, laws, and norms.[15] The insufficient number of cyber professionals in Federal service is hampering national efforts, and the report cites over 33,000 unfilled cyberspace positions in the U.S. Government.[16]

Difficulties in recruiting and retaining cyber talent are also impacting the Services. Retaining and developing personnel who employ cyberspace tools are so pivotal that the fiscal year 2022 (FY22) NDAA calls for DOD to assess its current cyber and information warfare curriculum across the joint education apparatus. The NDAA explicitly directs DOD to assess whether its current senior-level schools have the right curriculum and are the appropriate institutions for its delivery.[17] A new strategic posture is needed to position cyberspace as a warfighting domain with a commanding view of this rapidly evolving landscape.

The Solarium's key recommendation centered on the human capital dimension. Recommendation 1.5 states that the United States needs to recruit, develop, and retain a cyber workforce capable of building a defensible ecosystem and enabling the agile, effective deployment of all tools of national power in cyberspace.[18] Specific to this recommendation is the reinforcement of the National Institute of Standards and Technology role and the use of its National Initiative on Cybersecurity Education (NICE) workforce framework nationwide. The framework is the foundation for describing the tasks, knowledge, and skills required to perform cybersecurity work. It is also the cornerstone that enables organizations to develop their workforce to perform cybersecurity work and helps them determine the appropriate learning activities to advance their knowledge and skills. Specifically, the NICE framework is the organizing principle for the current DOD requirement to develop the cyber workforce, especially senior cyber leaders.

Today, none of the Services provides a dedicated program, beyond optional concentration studies and online certifications taken separately from PME, to meet this obligation at the place where most senior uniformed and civilian cyber officers are deliberately developed—the Service war colleges.

Current DOD Requirements. A recent National Cyber Strategy (2018) stresses the development of a superior cybersecurity workforce as a security advantage. It further states that the United States will "fully develop the vast American talent pool, while at the same time attracting the best and brightest among those abroad who share our values."[19] The strategy emphasizes that the Federal Government must use the NICE framework to standardize identifying, hiring, developing, and retaining a talented cybersecurity workforce. Success in the cyber domain will depend on the DOD ability to cultivate a high-quality workforce and develop leaders who can integrate new capabilities and adopt emergent approaches. At the time of its publication, there was no holistic DOD guidance that specifically addressed the scope of the cyberspace workforce beyond the information assurance sector.

So how does DOD develop its cyber talent and align with the NICE framework? Focus area one of the DOD cyberspace workforce strategy establishes a cohesive set of DOD-wide cyberspace workforce management issuances, the DOD 8140 publications. These publications address the demand to reevaluate staffing requirements, realign personnel within cyberspace work roles (codified in the DCWF), and retain qualified personnel. In cooperation with U.S. Cyber Command, DOD integrated a complete set of cyberspace work roles and qualification requirements into the overarching DCWF. The DOD 8140 publications are broken into the following three interrelated directives, instructions, and manuals:[20]

- DOD Directive 8140.01, *Cyberspace Workforce Management* (signed October 5, 2020)
  - authorizes the DOD Cyberspace Workforce Management Board
  - establishes elements in the cyber workforce
  - identifies roles and responsibilities within DOD
  - defines the cyberspace workforce.
- DOD Instruction 8140.02, *Identification, Tracking, and Reporting of Cyberspace Workforce Requirements* (signed December 21, 2021)
  - offers guidance for identification, tracking, and reporting of DCWF work roles
  - identifies military and civilian requirements
  - provides the foundation for developing enterprise baseline cyberspace workforce qualifications.
- DOD Manual 8140.03, *Cyberspace Workforce Qualification and Management Program* (signed February 15, 2023)
  - assigns responsibilities and procedures for qualification of the cyberspace workforce
  - describes foundational (knowledge), residential (capability), and continuous development/qualification requirements
  - includes military, civilian, and contracted personnel.

The DOD 8140 publications address the full spectrum of the cyber workforce. The cyberspace workforce comprises personnel who build, secure, operate, defend, and protect DOD and U.S. cyberspace resources; conduct related intelligence activities; enable future operations; and project power in or through cyberspace.

The DCWF represents a comprehensive standardized way to describe DOD cyber work with the intent to get the right people in the right positions. This framework allows Services to identify, track, and report cyberspace workforce personnel and their qualifications as required by the Federal Cybersecurity Workforce Assessment Act of 2015. The forthcoming DOD 8140 manual will list tasks and knowledge, skills, and abilities (KSAs) for 54 work roles within the DCWF. The DCWF features 54 work roles across 5 areas:

- cyber IT
- cybersecurity
- cyber effects
- cyber intelligence
- cyber enablers.[21]

Though the cyber leader work role is of great importance, future senior civilians and O6s may find themselves in the cyber policy and strategy planner role or any acquisition and project management role in support of major cyber and technology initiatives. Recently, the DCWF has been updated through a process known as DCWF Refresh and is codifying even more cyber leader roles for data and artificial intelligence.[22] These work roles are given three-digit codes, commonly referred to as "cyber coding."

Per DOD 8140 publications, cyber coding is intended to help identify, track, and report qualifications for personnel who perform cyberspace work roles using the authoritative personnel and manpower databases. The established codes will denote the work performed and corresponding proficiency level. This effort is ongoing, and the Services have achieved only the initial coding of the workforce. In 2021, over 120,000 military and civilian positions in DOD were cyber coded—and that does not count the military positions in the Army, U.S. Cyber Command, and a couple of others that were still working on completing military coding via their manpower systems.[23] Despite the missing data, the report is a good indicator of the size of the cyberspace workforce across DOD.

The DCWF and its cyber coding effort represent the DOD requirement to standardize cyber workforce management. Each cyber work role has a definition, a list of core and additional tasks, and KSAs that describe what is needed to execute critical functions and measure proficiency.[24] Cyber leaders are not exempt from the requirement. Extrapolating from the same DOD cyber coding report, the breakout of cyber positions coded as an "executive cyber leader" represents over 700 positions. The Army data, once complete, will raise those numbers considerably. The demand signal to ensure senior cyber leaders are fully qualified per DOD 8140 publications is apparent. Even without the final Army coding numbers, this represents a diverse and expanding number of senior cyber leader positions across DOD. Furthermore, in addition to using the DCWF to manage cyber workforce development and performance, the Services are directed to confirm compliance as an element of mission readiness.[25] The current apparatus for DOD leader development, joint PME, is tailored to meet this challenge.

Joint Education and Cyber. Joint PME is continuously refining the art and science of warfighting, particularly embracing technology and its integration to achieve mission success. The 2020 Joint Chiefs of Staff (JCS) vision and guidance for PME elaborates that changes in the character and conduct of war demand "continuous integration of national instruments of power and influence in support of national objectives . . . [and] a deeper understanding of the implications of disruptive and future technologies for adversaries and ourselves."[26]

Today's environment requires critical study of the information instrument of power, requisite cyber capabilities, and evolving technologies. To that end, the JCS vision lays out clearly that PME programs must provide graduates the knowledge and skills to prepare them for service as joint warfighting leaders, senior staff officers, and strategists who "anticipate and lead rapid adaptation and innovation during a dynamic period of acceleration in the rate of change in warfare under the conditions of Great Power competition and disruptive technology."[27] The DOD chief information officer (CIO) further echoes this task in his lines of effort (LOE) to meet the DOD Cyber Strategy. Of note is LOE 8—sustain a cyber workforce. This LOE has a specific objective to enhance the quality of the cyber education continuum across DOD. The LOE's relevant subobjectives include:

- 8-5-2: Enhance the cyberspace curriculum at joint PME schools by incorporating realistic and relevant case studies
- 8-5-3: Develop the concept for establishing a leadership-level cyber strategy development and planning framework into course curriculum at joint and Service-sponsored function courses
- 8-5-4: Incorporate cyber mission, roles, and responsibilities into required leadership training plans and curriculum.[28]

For the Service war colleges to execute this intent, their vector must coincide with the Chairman of the Joint Chiefs of Staff instruction on officer PME. The May 2020 release describes an outcomes-based approach across six joint learning areas (JLAs). The intent of the national and joint cyber visions and the DOD CIO LOEs can be translated across three of the six JLAs:

- JLA 3: The Continuum of Competition, Conflict, and War. The instruction describes joint leaders who use their knowledge of the nature and character of war to determine the challenges to U.S. national interests, evaluating the best use of the military instrument of power to achieve national security objectives.[29] Cyber technology contributes significantly to the evolution of war and global competition. Senior cyber leaders must shape the transition from the current cyber posture to a posture suited for the changing character of war. DOD Cyber Strategy LOE 8-5-2 is perfectly matched and can be met by this JLA.
- JLA 4: The Security Environment. The instruction describes the evaluation of innovative and technological

Marine Corps Corporal Joshua Mackaman, cyberspace warfare operator with Defensive Cyberspace Operations, Force Headquarters Group, Marine Forces Reserve, helps civilian with computer network analysis hacking game called "Packet Inspector" at DEF CON 31, Las Vegas, Nevada, August 11, 2023 (U.S. Marine Corps/Jonathan L. Gonzalez)

forces that pose threats, opportunities, and risks.[30] Senior cyber leaders are entrusted to lead and advise on cyber threats and opportunities. DOD Cyber Strategy LOE 8-5-2 and 8-5-4 can both be supported by this JLA because senior cyber leaders must understand their role in tackling the evolving security environment.

- JLA 5: Strategy and Joint Planning. The instruction describes joint officers who design all-domain plans across the spectrum of conflict.[31] Cyber is a warfighting domain per the numerous national and joint strategies previously discussed. Senior cyber leaders must account for this domain in all phases of planning. DOD Cyber Strategy LOE 8-5-3 fits in and can be met by this JLA because the cyber domain permeates strategy, operations, and tactics in all other domains.

The Chairman's instruction lists the National Defense University's College of Information and Cyberspace (CIC) as the only institution educating senior leaders in the cyberspace domain. This exclusivity matches neither the evolving security environment nor the cyber workforce per the DOD 8140 publications and recent coding data. The cyber domain has grown exponentially and, as noted before, permeates strategy, operations, and tactics in all domains.[32] Cyberspace cannot be taught at only one location for those few who were selected to attend CIC. Based on the 2021 RAND study, DOD covers an estimated 62 percent of the estimated yearly military demand for joint PME (JPME) II, resulting in officers in cyber and information roles likely to receive only general PME.[33] CIC is a modest, at best, proportion of the JPME II graduate population. To date, the U.S. Army War College, Air University, and Naval War College do not have a dedicated track to develop cyber leaders. By leveraging the JLAs, every Service war college can help meet the requirement to deliberately develop senior cyber leaders per the DOD cyber strategy and inform the DOD response to the FY22 NDAA assessment of cyber education at the Service war colleges. Cyber topics integrated into the general JPME II curriculum are no longer sufficient.

What Is a Cyber Leader? Recommendations

To adapt senior-level PME to meet the intent of the requirements established in national policy documents and framed in the DOD 8140 publications, the cyber leader work role must be defined. The current DCWF cyber leader work role summary is the foundation for the proposed recommendations. That is, the cyber leader executes decisionmaking authorities and establishes vision and direction for an organization's cyber and cyber-related policies, resources, and/or operations while maintaining responsibility for risk-related decisions affecting mission success.

A synthesis of the available KSAs for Federal cyber leader work roles and the recent CIC learning outcomes helps establish a baseline for the proposed cyberspace strategic studies track.[34] The following are recommended learning outcomes for this proposed track:

- evaluate the national security environment with an emphasis on the effect of cyberspace operations and related evolving technologies on all instruments of national power
- integrate joint doctrine perspectives into cyberspace operations and strategy
- analyze the critical aspects of cyberspace operations, technology, theories, laws, and policies in the development of national and Service strategies, joint operations, and other DOD activities
- evaluate and mitigate potential vulnerabilities of cyber capabilities, applications, and innovative and technological forces that pose threats, opportunities, and risks to joint operations
- apply principles of strategic leadership, decisionmaking, and ethical conduct regarding cyber capability employment.

As with any educational program, the challenge is to balance breadth and depth of knowledge. These learning outcomes set a path for success in balancing, on the one hand, the complementary set of essential KSAs to develop and defend the cyber environment with, on the other hand, strategic leadership underpinnings to influence departmental culture and military strategy.

This recommendation could be implemented with the help of the cyber resources and experts each Service has at its various educational institutions. Additionally, this recommendation positions CIC to reinvigorate its role as a "center of excellence" and support curriculum development, research opportunities, and Service war college partners—another shared conclusion with the RAND study.[35] The recommendation is both broad enough to allow for flexible implementation and detailed enough to allow for rapid implementation. There is no intent to swap or remove from an already crowded Joint Staff–directed curricula, only to use it as the foundational block in a dedicated track to narrow the focus on cyberspace and information. It parallels existing space, maritime, national security, and other differentiated tracks and shares the same intent: to prepare senior leaders in those areas demanding differentiated deliberate development.

The first step is establishing (or reestablishing) a cyber lead at each Service war college. This senior cyber leader will be a prominent on-staff advocate for cyber domain education while championing learning outcomes for senior cyber leaders, helping graduates meet DCWF cyber leader work role qualifications, and collaborating with intra-Service and inter-Service cyberspace educators. This track should include officers and civilians from cyber, information, space, acquisition, and information technology occupational specialties to bring in varying perspectives and prepare the full range of senior cyber leaders coded as such in the DCWF. This specialized track builds on the war colleges' current joint strategy and leadership curriculum by adding the unique perspectives and challenges cyberspace and information warfare present. It adds the origins of the cyberspace operational environment and national and DOD cyber strategies. It also seeks to incorporate curriculum on cyber technological capabilities, laws, policies, and data analytics. This could potentially include short trips to Service, DOD, and Department of Homeland Security cyber operations facilities, research laboratories, and industry partners. These trips and collaborative sessions with industry partners and other Federal agencies would prepare students to meet the NDAA requirement of expanded engagement outside DOD to explore different cyber capabilities and methods.[36]

Students in this track who are required by their Services to present research papers will focus on cyber and information domain challenges. The specialized track prepares students to provide cyber analysis and expertise during wargaming exercises, based on each of the war colleges' curricula. The proposed course essentials for the cyber strategic studies track are depicted in the figure and require further refinement from Service cyber institutions as well as recommendations from CIC. Adopting this recommendation ensures all learning objectives are met, and graduates will meet the DCWF Service requirements for the cyber leader work role.

Conclusion

Cyberspace has increasingly changed the way that war and global competition have evolved. The digital environment, initially designed to expand ideas and interaction, is now being used to circumvent U.S. sovereignty across all instruments of national power. It is an understatement to claim the introduction of cyberspace as a domain has had disruptive effects across the rest of the warfighting domains. Carl von Clausewitz warned that "all planning, particularly strategic planning, must pay attention to the character of contemporary war."[37] French academic and martyred World War II partisan Marc Bloch wrote of "theorists who were bogged down in errors engendered by the faulty teaching of history" and "the smell of decay rising from the Staff College," providing a harsh bridge from Clausewitz to modern criticisms from senior DOD officials.[38] DOD must adapt and innovate or find itself reacting to more attentive and agile actors.

The DOD cyber strategy LOEs and the 8140 publications set out the

requirement to establish governance and structure for management of the cyber workforce and provide the foundation for qualification and development. Paramount to this effort is the development of joint senior cyber leaders. This is so critical that the DCWF designated a specific cyber leader work role. Leaders set culture, and we must ensure senior cyber leaders are fluent in the technologies, risks, and strategic cyber applications across all domains. Service war colleges are positioned to lead the DOD effort to develop senior cyber leaders to meet directives and find solutions that could develop each new generation of cyberspace leaders to succeed in this transformational warfighting domain.

To accelerate the transition from the force we have to the one required to win in cyber competition and conflict, the joint force must look beyond the rapid acquisition of ships, tanks, and planes. It must demonstrate an unwavering and growing commitment to deliberately developing senior cyber leaders who will shape this warfighting domain that permeates strategic, operational, and tactical levels in all other domains. Service war colleges can lead the way by pathfinding a dedicated cyberspace strategic studies track. **JFQ**

Thanks to Colonel Mark D. Coggins, USAF, Ph.D., Dr. Carl J. Horn, and Professor Gene C. Kamena from the Air War College for their thoughtful comments and suggestions regarding themes and ideas for this article.

Notes

[1] Angus King and Michael Gallagher, co-chairs, *Cyberspace Solarium Commission Report* (Washington, DC: U.S. Cyberspace Solarium Commission, March 2020), 8, https://cybersolarium.org/wp-content/uploads/2022/05/CSC-Final-Report.pdf.

[2] Ibid., 1.

[3] Ibid.

[4] *Summary: Department of Defense Cyber Strategy* (Washington, DC: Department of Defense, 2018), 5, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

[5] Brett T. Williams, "The Joint Force Commander's Guide to Cyberspace Operations," *Joint Force Quarterly* 73 (2nd Quarter 2014), 14, https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-73/Article/577499/the-joint-force-commanders-guide-to-cyberspace-operations/.

[6] Quentin E. Hodgson et al., *Educating for Evolving Operational Domains: Cyber and Information Education in the Department of Defense and the Role of the College of Information and Cyberspace* (Santa Monica, CA: RAND, 2022), iii, https://doi.org/10.7249/RRA1548-1.

[7] *Cyberspace Solarium Commission Report*, 1.

[8] *Interim National Security Strategic Guidance* (Washington, DC: The White House, March 2021), 8, https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf.

[9] *Joint Operating Environment 2035: The Joint Force in a Contested and Disordered World* (Washington, DC: The Joint Staff, July 14, 2016), 3, https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joe_2035_july16.pdf?ver=2017-12-28-162059-917.

[10] *Joint Concept for Operating in the Information Environment* (Washington, DC: The Joint Staff, July 25, 2018), 8, https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf.

[11] Ibid.

[12] Ibid., viii.

[13] Ibid., 9.

[14] *Cyberspace Solarium Commission Report*, 16.

[15] Ibid., 15.

[16] Ibid., 16.

[17] National Defense Authorization Act for Fiscal Year 2022 (NDAA FY22), Pub. Law 117-81, 117th Cong., 1st sess. (December 27, 2021), 489.

[18] *Cyberspace Solarium Commission Report*, 43.

[19] *National Cyber Strategy of the United States of America* (Washington, DC: The White House, September 2018), 17, https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

[20] William Hess and Alfredo Rodriguez III, "USMC DOD 8140 OPT Presentation," USMC DOD 8140 Working Group, Headquarters Marine Corps, Washington, DC, June 14, 2021, 4.

[21] "DOD CIO Cyber Workforce Management," Defense Workforce Council presentation, Pentagon, Washington, DC, August 2021, 3.

[22] "DOD CIO Cyber Workforce News," *Defense.gov*, October 2020, https://dodcio.defense.gov/Portals/0/Documents/Cyber/WorkforceNewsletterOctober2020.pdf.

[23] Patrick Johnson, chief, Workforce Management Directorate, DOD-CIO, email to author, October 7, 2021; Department of Defense Inspector General (IG), *Audit of the Department of Defense Recruitment and Retention of the Civilian Cyber Workforce (DODIG-2021-110)* (Washington, DC: Government Publishing Office, August 2, 2021), i, 2, 8, 11–12, 26, 28. The IG report redacted the numbers. Mr. Johnson provided releasable numbers in the email.

[24] Department of Defense Instruction 8140.02, *Identification, Tracking, and Reporting of the Cyberspace Workforce Requirements* (Washington, DC: Department of Defense, December 21, 2021), 9.

[25] Ibid., 6.

[26] *Developing Today's Joint Officers for Tomorrow's Ways of War: The Joint Chiefs of Staff Vision and Guidance for Professional Military Education and Talent Management* (Washington, DC: The Joint Staff, May 1, 2020), 3, https://www.jcs.mil/Portals/36/Documents/Doctrine/education/jcs_pme_tm_vision.pdf?ver=2020-05-15-102429-817.

[27] Ibid., 4.

[28] "DOD CIO Cyberspace Strategy Lines of Effort, LOE 8 Summary," Department of Defense CIO, October 4, 2019, 3.

[29] Chairman of the Joint Chiefs of Staff Instruction 1800.01F, *Officer Professional Military Education Policy* (Washington, DC: The Joint Staff, May 15, 2020), 26.

[30] Ibid., 25.

[31] Ibid.

[32] Joshua A. Sipper, "It's Not Just About Cyber Anymore: Multidisciplinary Cyber Education and Training Under the New Information Paradigm," *Joint Force Quarterly* 100 (1st Quarter 2021), 53, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2497154/its-not-just-about-cyber-anymore-multidisciplinary-cyber-education-and-training/.

[33] Hodgson et al., *Educating for Evolving Operational Domains*, 28.

[34] Carl J. Horn, "College of Information and Cyberspace Update," National Defense University, August 7, 2019, 6.

[35] Hodgson et al., *Educating for Evolving Operational Domains*, 37.

[36] NDAA FY22, 492.

[37] Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1989), 220.

[38] Marc Bloch, *Strange Defeat: A Statement of Evidence Written in 1940* (New York: Norton, 1999), 125.