RAND CORPORATION

Research Report

QUENTIN E. HODGSON, CHARLES A. GOLDMAN, JIM MIGNANO, KARISHMA R. MEHTA

Educating for Evolving Operational Domains

Cyber and Information Education in the Department of Defense and the Role of the College of Information and Cyberspace

For more information on this publication, visit **www.rand.org/t/RRA1548-1**.

Published by the RAND Corporation, Santa Monica, Calif.

Cover: DOD photo by Mass Communication Specialist 1st Class Daniel Hinton. Data: matejmo/ Getty Images/iStockphoto.

Cover design by Rick Penn-Kraus.

About this Report

In the Fiscal Year 2021 National Defense Authorization Act, Congress directed the U.S. Department of Defense (DoD) to submit a report that explained plans to close the College of Information and Cyberspace (CIC) at the National Defense University and the department's needs for cyberspace and information education. The department submitted a report in April 2021 addressing the plans for CIC and concluding that more work was needed to address the broader question of the department's educational needs. The Office of the Secretary of Defense, Cyber Policy, tasked the National Defense Research Institute at RAND to conduct a broader study on these educational needs and the role that CIC should play in meeting them in the future. This report examines how DoD educational institutions are approaching education in cyberspace and the information environment and the potential demand for this education at the Joint Professional Military Education Phase II and graduate levels. The report then evaluates CIC's missions and options for adapting its governance to meet current and future educational needs.

The research reported here was completed in September 2022 and underwent security review with the sponsor and the Defense Office of Prepublication and Security Review before public release.

RAND National Security Research Division

This research was sponsored by the Office of the Secretary of Defense, Cyber Policy, and conducted within the Forces and Resources Policy Center of the RAND National Security Research Division (NSRD), which operates the National Defense Research Institute (NDRI), a federally funded research and development center sponsored by the Office of the Secretary of Defense, the Joint Staff, the Unified Combatant Commands, the Navy, the Marine Corps, the defense agencies, and the defense intelligence enterprise.

For more information on the RAND Forces and Resources Policy Center, see www.rand.org/nsrd/frp or contact the director (contact information is provided on the webpage).

Acknowledgments

We thank the faculty and staff at each of the Department of Defense schools of higher education who were generous with their time and provided data. We are particularly grateful to Dr. Cassandra Lewis, Chancellor of the College of Information and Cyberspace, for her enthusiastic support and engagement, and to Dr. Bryon Greenwald, Deputy Provost of the National Defense University, for his assistance. We thank Mieke Eoyang, Deputy Assistant Secretary of Defense for Cyber Policy, for her engagement and support, and Scott Lewis,

Dr. Gary Schaub, and Dr. Eric Russi. Dr. Paul Mayberry and Daniel Ginsberg provided valuable feedback on our analysis throughout the project and we thank Thomas F. Atkin for his careful review and critique of the draft report. Barbara Bicksler thoroughly reviewed the report and her edits and recommendations significantly improved its readability and cohesiveness. Any errors remain the authors'.

Summary

In April 2021, the U.S. Department of Defense (DoD) submitted a report to Congress in response to a National Defense Authorization Act for Fiscal Year 2021 requirement that assessed the requirements for educating military and civilian leaders in the information environment and the cyberspace domain. The motivation for this request was concern in Congress about DoD's plans to close the College of Information and Cyberspace (CIC), part of the National Defense University (NDU). The report concluded that CIC should remain at NDU but also suggested that further research should be done to ensure that CIC's capability and capacity are in line with both near-term and longer-term needs for education in the information environment and cyberspace domain.[1]

At the request of the Office of the Secretary of Defense, this RAND Corporation report responds to that call for additional research. The findings agree that CIC plays an important role in providing information and cyberspace education in the DoD educational ecosystem but goes beyond that to recommend that CIC should expand its role as a center of excellence in these areas, given continued and likely growing requirements for this expertise.

Approach

Because this report focuses on the future role of CIC in the DoD educational ecosystem, it addresses education primarily at the Joint Professional Military Education Phase II, typically provided to officers in the grades of O-5 (lieutenant colonel/commander) and O-6 (colonel/captain) and equivalent graduate education levels. The research team employed a mixed-methods approach that focused on the 13 institutions with the most relevant course or degree programs—reviewing websites and detailed information about each institution's cyber and information offerings through open-source literature and semistructured discussions with college faculty and staff. This work was supplemented with additional data on faculty, student, and curriculum offerings; review of relevant literature; and additional interviews focused on workforce needs for education in cyberspace and information.

Findings

Our assessment of the degree and certificate programs offered by the educational institutions included in this research effort indicated an array of educational options for generalists and specialists—communities that have different responsibilities but also must be able to collaborate

[1] DoD, *Matters Concerning the College of Information and Cyberspace and Limitation of Funding for National Defense University,* report to Congress submitted Pursuant to Section 1741 of the FY 2021 NDAA, April 9, 2021a.

and communicate effectively. Specialist degree programs tend to focus on strategy, management, and/or technical curricula. Among these programs, CIC's focus is distinct from other institutions within the DoD educational ecosystem in that it is the only institution that provides multiple degrees and graduate certificates that span strategy and management specializations, as well as continuing education in cyberspace and information. Moreover, the CIC degree programs benefit from synergies with the college's certificate offerings—often leading alumni who begin certificate programs to complete additional credentials or degree programs.

Furthermore, interviews with stakeholders suggest that programs like CIC's have high utility—that warfighters in general need more education in joint planning, joint cyberspace operations, nonkinetic warfare, and whole-of-government cooperation. Leaders and operators alike need a better understanding of cyberspace capabilities and how to better communicate about them. But current cyberspace and information curriculum needs to adapt more quickly to the evolving operational needs—something institutions said they needed more assistance with. Similarly, many of the organizations we talked to desire more engagement with educational institutions to support the organizations' missions through continuing education. Yet it is often up to the individual to pursue professional development opportunities—with little institutional motivation or coordination.

Although future demand for cyber and information educational opportunities is difficult to project, our estimates suggest that the capacity of the current system—with supply measured in the annual number of academic year graduates—may not cover all of DoD's needs for either the military or civilian workforce. Our conclusion is that DoD needs at least its current capacity to educate cyber and information professionals and should likely look for opportunities to grow, particularly in the strategy and management focus areas that CIC specializes in. Moreover, DoD institutions also serve some of the needs of other federal agencies and international military partners, which adds to this demand.

This landscape suggests that there is a role for CIC not only in maintaining its distinct educational offerings but also in playing other leadership roles in the DoD educational ecosystem—an overarching finding that motivates our recommendations.

Recommendations

DoD recognizes the importance of educating specialists and generalists in cyberspace and the information environment. Its educational institutions are working to meet the need, although there is greater potential demand than the current throughput can address. CIC plays an important role in meeting this need and has capacity to expand its offerings. The following recommendations will better position CIC to realize its full potential in the DoD educational ecosystem.

- **Maintain CIC's dual mission educating joint warfighters and the cyber workforce.** CIC provides strategic and management focus on cyberspace and information not

provided by other DoD education—knowledge for which there will be an enduring need for warfighters and other civilian personnel. This distinctive focus could well be lost if CIC's role is eliminated or reduced, and eliminating one area of focus would also eliminate synergies between the different CIC programs.

- **Advertise CIC's programs more effectively across the department and beyond.** CIC is not well known across DoD. CIC, NDU, and military and civilian education policymakers should work with all DoD components, as well as other U.S. government agencies, to make more people aware of CIC and its programs. In this context, CIC should not only continue to offer at least the current number of spaces in its programs—which will maintain faculty with needed expertise—but also posture itself to expand to meet demand in the future.
- **Strengthen governance arrangements for the cyberspace workforce education mission.** This mission has suffered over the years as financial and governance support has shifted, and CIC has faced repeated plans to downsize or eliminate it. We recommend that DoD identify one or more governance partners to take on responsibility for development of the cyberspace workforce, to complement the Joint Staff's focus on the joint warfighting community; provide and update guidance on roles and responsibilities; and align associated funding streams.
- **Position CIC as a resource on cyberspace education and research across DoD.** We recommend that CIC reinvigorate and increase its role as a center of excellence for cyberspace curriculum development and solicit inputs from DoD components to shape a research agenda that can contribute directly to their missions.
- **Improve cross-departmental accounting for cyberspace and information environment work roles and functions.** The need for cyberspace and information professionals—both military and civilian—will likely grow in the next decade as the nation faces a rapidly changing technological landscape. DoD cannot keep up with these challenges if it cannot adequately account for the personnel it has in these work roles and job functions and use this accounting as a basis to project future demand.

Concluding Thoughts

CIC's role can be reinforced and sustained through implementation of these recommendations. By doing so, the department can demonstrate its commitment to ensuring a workforce that is prepared to think critically about cyberspace and the information environment, and how DoD, with its partners in other departments and agencies and abroad, can achieve national security objectives through integration of capabilities.

Contents

Tables

Chapter 1. Introduction

In an April 2020 letter to then–Secretary of Defense Mark Esper, members of Congress expressed concern about plans at the National Defense University (NDU) to close the College of Information and Cyberspace (CIC), one of five schools at NDU and the only joint school focused exclusively on cyberspace education.[1] Congress subsequently included a provision in the Fiscal Year (FY) 2021 National Defense Authorization Act (NDAA) that prohibited any action to close or reorganize CIC until the Secretary of Defense submitted a report that assessed the requirements for educating military and civilian leaders in the information environment and the cyberspace domain and that reviewed the options and plans for CIC.[2]

The U.S. Department of Defense (DoD) submitted a report in response to the NDAA provision in April 2021 that concluded that CIC should remain at NDU but that further study was required to "ensure capability and capacity is aligned and balanced within the portfolio of NDU programs" and to examine the longer-term needs for education in the information environment and cyberspace domain.[3] The Office of the Secretary of Defense, Cyber Policy, tasked RAND's National Defense Research Institute with undertaking that study. This report examines the current approach to providing cyberspace and information education across DoD institutions of higher education, postulates the likely potential demand for this type of education, and addresses options for how CIC can help meet that demand.

Before looking more closely at these issues, we provide a brief overview of why cyberspace and information education are needed now, given the growing importance of these domains to national security and future warfare. We also describe education policy in the department briefly for readers wanting a grounding in how DoD defines and guides the provision of education to its military and civilian personnel. We then lay out our research objectives and approach.

Cyberspace and Information Are Increasingly Important Aspects of National Security and Warfare

Cyberspace was declared an operational domain alongside the traditional domains of air, land, and sea in the 2004 National Military Strategy, which was subsequently supported by the

[1] M. Michael Rounds, Joe Manchin III, James R. Langevin, and Elise Stefanik, "Letter to the Honorable Mark T. Esper and the Honorable David L. Norquist," April 24, 2020.

[2] Section 1741, "Matters Concerning the College of Information and Cyberspace and Limitation of Funding for National Defense University," in Pub. L. 116-283, William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, January 1, 2021. The full legislative requirement is included in Appendix A.

[3] DoD, *Matters Concerning the College of Information and Cyberspace and Limitation of Funding for National Defense University,* report to Congress submitted Pursuant to Section 1741 of the FY 2021 NDAA, April 9, 2021a.

creation of U.S. Cyber Command (USCYBERCOM) in 2009 and the Cyber Mission Force in 2012.[4] DoD has issued three cyberspace strategies in the last dozen years (2011, 2015, 2018) with another one currently in development. In addition, then–Secretary of Defense Ashton Carter issued the defense Strategy for Operations in the Information Environment in 2016, followed by the Joint Chiefs of Staff declaring information the seventh joint function and issuing the Joint Concept for Operating in the Information Environment in 2018.[5]

The joint concept recognizes the vast growth in information that is generated and shared globally and notes that these new dynamics change behavior among actors of all types, from major powers to weak states and populations. For the U.S. military, then, understanding and leveraging information to "shape perceptions, attitudes, and other elements that drive desired behavior and the course of events" is central to achieving strategic objectives.[6] This means that war, as "the continuation of policy by other means" is also more than just the imposition of will through force but an attempt to shape and influence decisionmaking and perception.[7]

Although cyberspace and the information environment are not new to the department, the role they play in warfare and shaping the strategic environment has come more to the fore in recent years. Increasing connectivity, both digitally and in terms of interconnectedness of populations, means that the role that cyberspace and the information environment play in our everyday lives and in international relations is growing.[8] The narrative of the battlefield is shaped by thousands of "sensors," from individuals uploading videos captured on smartphones to video feeds captured by unmanned aerial systems.[9] For example, in Russia's war against Ukraine, the Russian government has attempted to portray the conflict as "a special military operation" to root out fascists in the Ukrainian government and restore Ukraine to the Russian

---

[4] USCYBERCOM, "Our History," webpage, undated. DoD defines *cyberspace* as "a global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" (Joint Publication 3-12 *Cyberspace Operations*, June 8, 2018, p. GL-4).

[5] DoD, *Department of Defense Strategy for Operations in the Information Environment*, June 2016; Joint Chiefs of Staff, *Joint Concept for Operating in the Information Environment (JCOIE)*, July 25, 2018. DoD defines the *information environment* as the "aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information" (*DoD Dictionary of Military and Associated Terms*, November 2021b). Joint Chiefs of Staff, 2018, expands on this definition to state that the information environment

> is comprised of and aggregates numerous social, cultural, cognitive, technical, and physical attributes that act upon and impact knowledge, understanding, beliefs, world views, and, ultimately, actions of an individual, group, system, community, or organization. The IE [information environment] also includes technical systems and their use of data. The IE directly affects and transcends all [operational environments]. (Joint Chiefs of Staff, 2018, p. 42)

[6] Joint Chiefs of Staff, 2018, p. viii.

[7] Carl von Clausewitz, *On War*, ed. and trans. by Michael Howard and Peter Paret, Princeton University Press, 1976, p. 87.

[8] United Nations Conference on Trade and Development, *Digital Economy Report 2021,* United Nations Publications, 2021.

[9] "Database of 235 Videos Exposes the Horrors of War in Ukraine," *Washington Post*, May 9, 2022.

sphere while closing off the Russian people from outside news to reinforce the perception of the West against Russia.[10] Each side in the conflict has employed cyber operations to send messages (such as playing the Ukrainian national anthem on Russian radio) and disrupt digital communications. Microsoft noted in late April 2022 that Russian nation state and affiliated cyber actors had launched more than 237 cyber operations against Ukraine.[11] Ukraine has mobilized its own "IT [information technology] Army" to defend itself against Russian cyber operations.[12]

The 2018 Defense Cyber Strategy, like previous strategies, emphasizes the need to sustain a ready cyber workforce. This includes providing for its continuing professional development and career progression.[13] Cyber skills are often seen as highly technical and as requiring emphasis at all levels of education.[14] But for DoD, cyberspace operations are not simply about bits and bytes, command line command prompts, or hash functions.[15] A cyber-savvy workforce has to understand the way cyber capabilities contribute to achieving strategic and operational objectives and be able to communicate to other, nontechnical communities, such as planners, programmers, budgeteers, and senior leaders. At the same time, nontechnical managers and leaders need a grounding in cyberspace and information policy, doctrine, and strategy to be able to ask the right questions and make decisions about how to integrate capabilities to achieve objectives.

These strategies and concepts belie a much longer history of evolution in DoD's thinking about the role and contribution of cyberspace operations and operations in the information environment (OIE) to achieving strategic and operational objectives across the spectrum of conflict.[16] But the developments of the past decade and more indicate DoD's desire to improve its capabilities in both areas. Simultaneously, DoD's educational institutions have sought to support these developments by adding or expanding their focus on cyberspace and information.

---

[10] For more on the role of narrative in the Ukraine conflict, see Alyssa Demus and Christopher Paul, "Don't Sleep on Russian Information-War Capabilities," DefenseOne, April 5, 2022. On Russia's isolation from the global internet, see David Ingram, "Russia Is Nearly Isolated Online. What Does That Mean for the Internet's Future?" NBC News, March 15, 2022.

[11] Microsoft Digital Security Unit, *Special Report: Ukraine—An Overview of Russia's Cyberattack Activity in Ukraine,* April 27, 2022.

[12] Matt Burgess, "Ukraine's Volunteer 'IT Army' Is Hacking in Uncharted Territory," *Wired*, February 27, 2022.

[13] The full strategy is not publicly available, but there is an unclassified summary. DoD, *Summary Department of Defense Cyber Strategy*, 2018a, p. 5.

[14] U.S. Cyberspace Solarium Commission, *United States of America Cyberspace Solarium Commission*, final report, March 2020, p. 45.

[15] *Command line command prompts* are execution commands that automate tasks and allow the user to interact directly with a computer's operating system. See Microsoft, "Windows Commands," Microsoft Ignite website, January 4, 2022. *Hash functions* are mathematical functions that convert a large input value of any length into a more compressed fixed length string value. See Computer Security Resource Center, "Hash Function," webpage, undated.

[16] For example, the department promulgated its Information Operations Roadmap in 2003. See DoD, *Information Operations Roadmap*, Washington, D.C., October 30, 2003; Washington Headquarters Services, "Reading Room List, Other," webpage, undated.

Education in DoD

DoD has policies and systems that govern the education of officers, enlisted, and civilian personnel. In this report, we focus mostly on education relevant to officers and civilians.

The education of U.S. military officers starts before commissioning and extends throughout an officer's career. Both officers and enlisted members participate in various forms of professional military education (PME). For officers, this education addresses both joint and service-specific needs. Officer education prior to commissioning occurs through service academies and Reserve Officers' Training Corps programs at other colleges and universities. After commissioning, the Joint Professional Military Education (JPME) system is organized into three phases. Service command and staff schools and a joint option at NDU offer programs in JPME Phase I (JPME-I), typically to officers in the grade of O-4 (major/lieutenant commander). Service war colleges and multiple joint colleges at NDU offer programs in JPME Phase II (JPME-II), typically to officers in the grades of O-5 and O-6. NDU also offers the CAPSTONE course to general and flag officers. JPME, in general, provides the education needed to develop service officers to be proficient in joint matters.[17]

JPME is required for officer career progression following the framework laid out in the Goldwater-Nichols Department of Defense Reorganization Act of 1986, referred to as Goldwater-Nichols.[18] In particular, JPME-II completion is required to be designated joint officer–qualified, which is a requirement for promotion to general or flag officer rank (O-7).[19]

Aside from DoD's education options, military and civilian personnel can access education at civilian institutions through fellowship programs, continuing education, and enrolling as full or part-time students.

More specifically in the domains relevant to this report, the education of the cyber workforce (officers, enlisted, and civilians) is governed by DoD Directive (DoDD) 8140.01, *Cyberspace Workforce Management*.[20] This directive establishes roles and responsibilities for developing requirements, qualification standards, and certification for roles in the workforce.

CIC's Role and History

CIC was founded in 1964 as the DoD Computer Institute and has been renamed and reorganized multiple times since then. In 1982, CIC became part of NDU and became the

---

[17] As defined in U.S. Code, Title 10, Armed Forces (10 U.S.C.), Section 668, Definitions. This material is adapted from Paul W. Mayberry, Charles A. Goldman, Kimberly Jackson, Eric Hastings, Hannah Acheson-Field, and Anthony Lawrence, *Making the Grade: Integration of Joint Professional Military Education and Talent Management in Developing Joint Officers*, RAND Corporation, RR-A473-1, 2021, drawing on Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 1800.01F, *Officer Professional Military Education Policy*, May 15, 2020.

[18] Pub. L. 99-433, Goldwater-Nichols Department of Defense Reorganization Act of 1986, October 1, 1986.

[19] Mayberry et al., 2021; CJCSI 1800.01F, 2020.

[20] DoDD 8140.01, *Cyberspace Workforce Management*, October 5, 2020.

Information Resources Management College (IRMC) in 1988. IRMC also came to be known as the "iCollege" for a period; most recently, it was renamed CIC in 2016.[21] Its name and role as one of the constituent colleges at NDU are enshrined in law as well.[22] The DoD Computer Institute originally came under the oversight and responsibility of the Under Secretary of Defense Comptroller (USD[C]) but was transitioned to the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD[C3I]) in 1997 with the passage of legislation mandating each government agency have a designated senior official in charge of IT matters.[23]

Prior to 2012, the DoD Chief Information Officer (CIO) (the title ASD[C3I] transitioned to) provided funding to the college to support its programs for educating IT, information resource management, and cybersecurity professionals. In a previous review of IRMC in 2012, the college was ranked lowest in priority because it lacked a JPME program at the time, leading to considerations for closing the college.[24] The DoD CIO sponsored a study to examine the future role of the college in 2012. In September 2012, the DoD CIO and the Director for Joint Force Development (DJ-7) agreed to fund the college at $9 million through the NDU budget (representing a reduction of approximately 35 percent from its FY 2012 funding, including NDU institutional support and reimbursable funding).[25]

Today, CIC operates at the JPME-II level in the JPME system and also offers non-JPME degrees and certificates. Specifically, CIC offers two graduate degrees at the master's level (one in residence that confers JPME-II for U.S. military officers and one hybrid or distance learning degree that does not confer JPME credit). It also offers graduate certificate programs.

CIC's enrollment has varied over time. In FY 2011, 120 personnel were enrolled in the master's program and more than a 1,000 were enrolled in certificate programs. The JPME-II in-residence master's program grew from 14 students in FY 2016 (its first year) to 49 students in FY 2022, and nonresident master's enrollment remained relatively steady at more than 300 from FY 2013 to FY 2019 before falling below 200 in FY 2021, when the school stopped new enrollments because of the announced plans to close the school. The planned closure is also reflected in the drop in certificate program enrollment from more than 1,100 in FY 2018 to fewer than 160 in FY 2021. Since the plans to close the school were shelved, enrollment has slowly started to recover, as the data in Table 1.1 indicate.

---

[21] CIC, "Fact Sheet," May 2022.

[22] 10 U.S.C., Section 2165, National Defense University: Component Institutions.

[23] Alfred E. Brenner, J. Katherine Burton, and Paul K. Ketrick, *Future Options for the National Defense University (NDU) iCollege*, NS D-4438, Institute for Defense Analyses, May 2012, p. 5.

[24] Brenner, Burton, and Ketrick, 2012, p. ES-1.

[25] Teresa M. Takai, "National Defense University (NDU) iCollege Restructuring," memorandum for Director, Joint Force Development (DJ7), September 21, 2012, Not available to the general public. FY 2012 funding figures are from Brenner, Burton, and Ketrick, 2012, p. 6.

Table 1.1. CIC Student Enrollment by Program, FYs 2011–2022

FY	JPME-II Master's	Hybrid Master's	Certificate Programs
2011	N/A	120	1,003
2012	N/A	260	777
2013	N/A	326	975
2014	N/A	370	607
2015	N/A	336	990
2016	14	340	1,254
2017	16	328	1,195
2018	16	365	1,126
2019	17	323	290
2020	31	220	179
2021	41	177	158
2022	49	157	292

SOURCE: Data provided by CIC. FY 2022 enrollment numbers are revised from original data provided in October 2021.
NOTE: Hybrid master's and certificate programs are typically part-time programs; therefore, enrolled students may be counted in multiple years.

CIC is not the only institution in DoD that addresses cyberspace and information in its curriculum. As we discuss throughout this report, institutions across the spectrum of PME have all taken steps to address cyberspace and the information environment in their curricula, to varying degrees.

Research Objectives

Given the importance DoD has placed on these topics and continued congressional interest and support for education and training in cyberspace and information, this is a fitting time to examine how and to what extent the department is institutionalizing cyberspace and information as core topics for educating its leaders and managers to achieve national security objectives. This report seeks to address the following questions:

1. What is the potential demand for cyberspace and information education in DoD?
2. How is this demand being addressed currently across DoD educational institutions?
3. What is CIC's optimum role as part of the DoD educational ecosystem, and what other ways can CIC support DoD components?
4. What is the appropriate governance mechanism to support CIC executing its mission successfully?

This report addresses education but not training. Education is fundamentally about the acquisition of knowledge and learning modes of thinking critically to analyze problems and apply that knowledge. Training confers skills to carry out specific tasks and functions. Some institutions can provide both education and training. The distinctions between education and

training are also not always clearly delineated. Some educational institutions in DoD, for example, have educational programs and also teach short courses in specific skills or topics that would be considered training.

Our focus in this report is motivated by the congressional reporting requirement and developing recommendations for the future role of CIC in the DoD educational ecosystem. Therefore, we address education primarily at the JPME-II and equivalent graduate education levels. We do not address the needs of enlisted education, JPME-I, or undergraduate education, although we believe these are also important topics, given the roles filled by enlisted personnel, junior officers, and civil servants. As one interviewee noted to us, "if you're starting [education on cyber and information] at the JPME-II level, you're starting too late." We agree. Our focus on JPME-II and equivalent graduate education is for practical reasons due to the scope of the report requirements and available resources. A broader examination of the educational requirements in cyberspace and information topics is also needed.[26]

Research Approach

We employed mixed methods (i.e., interviews, data collection and analysis, and document analysis) to answer the research questions. Thirteen educational institutions administered by DoD components and accredited to award JPME-II credit or otherwise providing equivalent-level specialized education constitute what we call the DoD educational ecosystem in cyberspace and information (as we will discuss in Chapter 2).[27]

We reviewed each institution's website for an overview of its curriculum, student body, and activities related to cyberspace and information. In parallel, we reviewed previous related RAND Corporation reports and DoD guidance documents while consulting with the project sponsor and NDU administrators to scope further data collection. We then gathered detailed information about each institution's cyber and information offerings through open-source literature and semistructured discussions with college faculty and staff and requested additional documentation and data on faculty and student composition and curriculum content. Appendix B summarizes the results of this investigation. This information provides qualitative insights into how DoD's educational ecosystem functions in practice and, because each institution differs in many respects, enables meaningful comparisons of the quantitative data we gathered.

We gathered quantitative data to estimate demand for—and supply of—senior level strategic cyber and information education. The project sponsor distributed a request for information (RFI)

---

[26] Indeed, the FY 2022 National Defense Authorization Act includes a provision (Section 1506, Matters Concerning Cyber Personnel Requirements) that calls for this more comprehensive examination. See Pub. L. 117-81, National Defense Authorization Act for Fiscal Year 2022, December 27, 2021.

[27] Unless otherwise noted, the phrase *cyberspace and information* refers to either or both (i.e., cyberspace and/or information) throughout this report. Civilian institutions that offer graduate cyber and information programs are not included because they differ substantially from DoD institutions, generally focusing less on DoD and federal policy and requiring different tuition arrangements (i.e., DoD personnel must secure their own funding for tuition).

to DoD components ("customers"), requesting data on potential demand (see Chapter 3).[28] We also arranged semistructured discussions with 15 people at seven DoD organizations to obtain a deeper understanding of their specific workforce needs in cyber and information. To collect supply data, we requested from each educational institution counts of students and faculty in relevant programs. To validate the supply data provided, we leveraged information collected through a concurrent RAND project and engaged in follow up conversations with staff at the educational institutions.

To facilitate analysis, we classified the 13 institutions according to three general approaches to cyber and information education (see Chapter 2), as well as the types of educational programs offered. Classifying institutions in this manner illuminated CIC's specific niche in DoD's educational ecosystem. Additionally, because CIC's certificate programs emerged as a unique offering in the ecosystem, we carried out a series of semistructured discussions with CIC certificate program alumni to understand why students chose CIC, what their educational experience was, and how they have applied that education in their subsequent careers.

Based on the information gathered and subsequently analyzed, we developed a set of options for CIC's future role in the DoD educational ecosystem. We assessed the pros and cons of each option, devoting special attention to feasibility, from which we derived recommendations for DoD to meet needs for educating strategic leaders in cyber and information.

Organization of This Report

This remainder of this report contains the findings and recommendations from our research. Chapter 2 reviews the current approach that defense educational institutions are taking to address cyberspace and information in their respective curricula and activities. Chapter 3 compares the potential demand for education at this level to the capacity of DoD educational institutions to meet that demand. Chapter 4 then addresses options for the roles CIC should play, including in the classroom, but also as a center of educational and research excellence to support other DoD educational institutions and components. Chapter 5 offers recommendations and concluding thoughts. Appendix A provides the NDAA language that guided this research. Appendix B offers detailed profiles of the cyberspace and information activities conducted in the DoD educational institutions included in this research to supplement the analysis in the main body.

[28] We did not have the means to collect similar, reliable data from other U.S. government agencies.

Chapter 2. How the DoD Educates Leaders and Managers in Cyber and Information

The DoD educational ecosystem at the JPME-II and equivalent graduate level comprises the 13 educational institutions included in this report. Table 2.1 summarizes the rationale for their inclusion. The research included all senior-level service schools with accredited JPME-II programs. Additionally, while not accredited to offer JPME-II credit, the Air Force Institute of Technology (AFIT), Air Force Cyber College (AFCC), Naval Postgraduate School (NPS), and National Intelligence University (NIU) are included because they offer relevant specialized

Table 2.1. Educational Institutions Included in This Report

Institution	Reason for Inclusion
National Defense University (NDU)	
National War College	JPME-II accreditation
Eisenhower School for National Security and Resource Strategy	JPME-II accreditation
CIC	JPME-II accreditation
College of International Security Affairs (CISA)	JPME-II accreditation
Joint Forces Staff College (JFSC)	JPME-II accreditation
Air University	
AFIT	Relevant graduate degree programs
AFCC[a]	Relevant graduate degree program (proposed)
Air War College	JPME-II accreditation
Army War College (USAWC)	JPME-II accreditation
Marine Corps University (MCU)	JPME-II accreditation
NPS	Relevant graduate degree programs
Naval War College	JPME-II accreditation
NIU	Relevant graduate degree programs

[a] As of the 2022–2023 academic year (AY), the Air Force Cyber College ceased its graduate degree and certificate programs.

graduate degrees and have large DoD student populations.[1] Appendix B provides a detailed profile of each school.

In this chapter, to characterize the DoD educational ecosystem, we identify the major sources of educational requirements and governance mechanisms applicable to each institution. We then describe and categorize the approaches to—and types of—cyberspace and information education each institution provides. We end the chapter with some customer perspectives on the education offerings, challenges facing the educational institutions, and opportunities for CIC.

Requirements and Governance for DoD Educational Institutions

Sources of Education Requirements

As explained in Chapter 1, JPME-II is the second of three progressive phases of JPME instruction. Federal law defines *JPME* as "the rigorous and thorough instruction and examination of officers of the armed forces in an environment designed to promote a theoretical and practical in-depth understanding of joint matters and, specifically, of the subject matter covered."[2] According to statute, JPME subject matter must include the following:

> (1) National Military Strategy.
> (2) Joint planning at all levels of war.
> (3) Joint doctrine.
> (4) Joint command and control.
> (5) Joint force and joint requirements development.
> (6) Operational contract support.[3]

At the JPME-II level, subject matter must also include the following:

> (1) National security strategy.
> (2) Theater strategy and campaigning.
> (3) Joint planning processes and systems.
> (4) Joint, interagency, and multinational capabilities and the integration of those capabilities.[4]

The Chairman of the Joint Chiefs of Staff (CJCS) establishes objectives, policies, and related responsibilities for JPME accredited programs through the Officer Professional Military Education Policy (OPMEP).[5] The OPMEP is wide ranging. For example, it identifies general "Desired Leader Attributes" that JPME programs must help develop in students and sets specific student-body mix and student-to-faculty ratio requirements. The CJCS also directs institutions to

---

[1] The NIU formerly came under the direction of the Defense Intelligence Agency but transitioned to the Director of National Intelligence in 2021. See National Intelligence University, "NIU History," webpage, undated-b.

[2] 10 U.S.C., Section 2151, Definitions.

[3] 10 U.S.C., Section 2151, Definitions.

[4] 10 U.S.C., Section 2155, Joint Professional Military Education Phase II Program of Instruction.

[5] CJCSI 1800.01F, 2020.

incorporate "special areas of emphasis" that are regularly refreshed to ensure JPME curriculum is current.[6] The 2020 OPMEP revision also mandates that JPME programs "adopt an outcomes-based military education" (OBME) approach.[7] OBME orients education toward developing the knowledge, skills, and attributes that the services and commands demand for operational assignments. The Office of the Under Secretary of Defense for Personnel and Readiness (USD[P&R]) issues guidance for implementing OBME.[8]

The JPME ecosystem derives additional education requirements and guidance from DoD strategy and joint doctrine. Key strategy documents include the National Defense Strategy, National Security Strategy, National Military Strategy, and Capstone Concept for Joint Operations.[9] The OPMEP emphasizes joint doctrine, including Joint Publication 1 and the 1-0, 2-0, 3-0, 4-0, 5-0, and 6-0 series (covering personnel, intelligence, operations, logistics, planning, and communications, respectively).[10]

Cyberspace workforce education is governed by DoDD 8140.01 *Cyberspace Workforce Management*.[11] This directive mandates the use of the Defense Cyberspace Workforce Framework (DCWF) as the construct for identifying, tracking, and reporting on cyberspace work roles in the department. DoDD 8140.01 uses the "total force" construct, meaning that it is intended to apply across military, civilian, and contractor personnel. Depending on the type of cyberspace role, the requirements are developed and overseen by different Office of the Secretary of Defense (OSD) components. For example, the Under Secretary of Defense for Intelligence and Security establishes the requirements for "intelligence, counterintelligence, security, law enforcement, sensitive activities, and other related positions and personnel" (including those related to cyberspace), while the Under Secretary of Defense for Acquisition and Sustainment oversees the requirements for acquisition professionals (including those related to cyberspace).[12]

More generally, civilian career management and education are governed by separate DoD issuances, particularly DoDI 1430.02, *Civilian Career Management*, and DoDI 1430.16,

---

[6] Joseph F. Dunford, Jr., "Special Areas of Emphasis for Joint Professional Military Education in Academic Years 2020 and 2021," memorandum for Chiefs of the Military Services, President, National Defense University, CM-0108-19, May 6, 2019.

[7] CJCSI 1800.01F, 2020, p.2.

[8] Department of Defense Instruction (DoDI) 1322.35, Vol. 1, *Military Education: Program Management and Administration*, April 26, 2022.

[9] DoD, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge*, 2018b; White House, *National Security Strategy of the United States of America*, December 2017; Joint Staff, *Description of the National Military Strategy 2018*, 2018; Joint Staff, *Capstone Concept for Joint Operations: Joint Force 2020*, September 10, 2012.

[10] CJCSI 1800.01F, 2020, p. A-4. The individual series are available online via the Joint Chiefs of Staff website.

[11] DoDD 8140.01, 2020.

[12] DoDD 8140.01, 2020, pp. 5–6.

Growing Civilian Leaders.[13] DoDI 1430.02 does not speak directly to education but, more broadly, speaks to career development, of which education is a part. DoDI 1430.16 does state that civilians will be provided appropriate learning opportunities, including education to prepare for leadership roles.

For the information environment, the most current DoD issuance at the time of writing (August 2022) is DoDD 3600.01, *Information Operations*.[14] It places responsibility for developing policies on the training and education of service and joint information operations (IO) forces with the Under Secretary of Defense for Policy (USD[P]) and USD(P&R). DoDD 3600.01, like 8140.01, also notes that the "total force" construct is desired.[15] The FY 2018 National Defense Authorization Act mandated the designation of a senior official to "establish processes and procedures to integrate strategic information operations and cyber-enabled information operations across the elements of DoD responsible for such operations . . . ."[16] Congress further directed that the designated official conduct a review of the 2016 DoD Strategy for Operations in the Information Environment and to make recommendations on creating training and education programs to facilitate implementation of the strategy.[17] In our discussions with the DoD educational institutions, each indicated that it also analyzes strategic guidance, such as the 2018 Defense Cyber Strategy and the Strategy for Operations in the Information Environment to ensure their curricula are current and course content covers relevant topics.[18]

Governance of Educational Institutions

The Military Education Coordination Council (MECC) helps coordinate the implementation of the OPMEP among JPME accredited institutions.[19] According to the OPMEP, "The purpose of the MECC is to address key educational issues of interest to the joint education community, promote cooperation and collaboration amongst the MECC member institutions, and coordinate joint education initiatives."[20] Representatives from JPME-accredited institutions serve on the MECC in advisory roles to the MECC chair, the DJ-7. The DJ-7, in turn, reports to the CJCS.

---

[13] DoDI 1430.02, *Civilian Career Management,* April 6, 2006; DoDI 1430.16, *Growing Civilian Leaders*, August 23, 2022.

[14] DoDD 3600.01, *Information Operations,* May 2, 2013, change 1, May 4, 2017.

[15] DoDD 3600.01, 2017.

[16] Section 1637, "Integration of Strategic Information Operations and Cyber-Enabled Information Operations," in Pub. L. 115-91, National Defense Authorization Act for Fiscal Year 2018, December 12, 2017

[17] Pub. L. 115-91, 2017, Section 1637; DoD, 2016.

[18] DoD, 2018a; DoD, 2016.

[19] CJCSI 1800.01F, 2020, pp. A-13–A-14.

[20] CJCSI 1800.01F, 2020, p. A-13.

Several reporting relationships are at play in our sample of 13 educational institutions. The president of NDU oversees NDU's constituent colleges, and reports to the Secretary of Defense.[21] The CJCS advises and assists the Secretary of Defense on matters pertaining to NDU and all JPME-accredited programs.[22] The commander of Air University oversees AFIT and the Air War College (of which AFCC is part) and reports to the Secretary of the Air Force.[23] The USAWC president reports to the Secretary of the Army.[24] The presidents of MCU, NPS, and the Naval War College each report to the Secretary of the Navy.[25] The NIU president reports to the Director of National Intelligence.[26] In addition to these direct lines of authority, the governance of each institution is complicated by varying degrees of participation by internal (e.g., advisory boards, faculty committees) and external (e.g., combatant commands, military services) stakeholders.

DoDD 8140.01, *Cyberspace Workforce Management*, establishes the DCWF and designates related cyberspace workforce management responsibilities to DoD components.[27] For example, the directive assigns the DoD CIO the responsibility to "[establish], in coordination with the CJCS, academic programs at NDU to educate leaders in IT, information resources management, and cybersecurity requirements and capabilities"[28] and assigns the OSD and DoD component heads the responsibility to "[t]rain students on the cyberspace domain and cyberspace operations considerations in professional military education."[29] To supervise the implementation of DoDD 8140.01 and associated issuances,[30] the directive also establishes an executive level Cyberspace Workforce Management Board. Its charter establishes the board as a decisionmaking body responsible for managing the cyberspace workforce's "health, welfare, and maturity" through, among other things, determining departmentwide workforce standards and requirements

[21] 10 U.S.C., Section 2163, Degree Granting Authority for National Defense University.

[22] 10 U.S.C., Section 2152, Joint Professional Military Education: General Requirements.

[23] 10 U.S.C., Section 9414, Degree Granting Authority for United States Air Force Institute of Technology; 10 U.S.C., Section 9417, Degree Granting Authority for Air University.

[24] 10 U.S.C., Section 7421, Degree Granting Authority for United States Army War College.

[25] 10 U.S.C., Section 8592, Degree Granting Authority for Marine Corps University; 10 U.S.C., Section 8548, Degree Granting Authority for United States Naval Postgraduate School; 10 U.S.C., Section 8591, Degree Granting Authority for Naval War College.

[26] 50 U.S.C., Section 3227a, Degree-Granting Authority.

[27] The DCWF catalogs and organizes cyber roles and responsibilities across the department into categories, specialty areas, and work roles; knowledge, skills, abilities, and tasks (KSATs); and workforce elements (i.e., IT, cybersecurity, cyberspace effects, intelligence, cyberspace enablers). DoD intends to use DCWF to inform talent management in meeting its cyber workforce needs.

[28] DoDD 8140.01, 2020, p. 4.

[29] DoDD 8140.01, 2020, p. 8.

[30] Associated issuances include DoDI 8140.02, *Identification, Tracking, and Reporting of Cyberspace Workforce Requirements*, December 21, 2021, and an expected DoD 8140 manual to replace DoD 8570.01-M, *Information Assurance Workforce Improvement Program*, December 19, 2005, change 4, November 10, 2015.

and "providing advice and recommendations to DoD leadership on cyber workforce development and enhancement."[31] The board includes representatives from several DoD components and is chaired by the DoD CIO, USD(P&R), and the Principal Cyber Advisor.[32]

For IO, DoDD 3600.01 directs each military department to provide education. CJCS is to ensure that joint education is "consistent . . . with joint IO policy, strategy, and doctrine" and must evaluate joint education to see that it is meeting combatant commands' requirements.[33] In September 2017, the Secretary of Defense noted the elevation of information to a joint function and directed USD(P) and the CJCS, as co-chairs of the Strategy for Operations in the Information Environment Executive Steering Group, to coordinate implementing necessary changes, including in education.[34] (A new Strategic Information Oversight Board has now replaced the Executive Steering Group.) The Joint Staff subsequently issued *Operations in the Information Environment Curriculum Development Guide* to expand on the OPMEP guidance and specify "OIE enabling learning objectives" for each level of JPME.[35]

Cyberspace and Information Education, Research, and Engagement

With an understanding of how cyber and information education is provided in DoD, we turn to an examination of the activities of the DoD educational institutions listed in Table 2.1 as they relate to cyber and information topics. Specifically, we review these institutions' offerings in graduate degrees and certificates, continuing education, research, and engagement.

The educational institutions we examined generally approach education in cyberspace and information in one of three ways:

- granting degrees in cyber and information (specialized major degree field programs)
- offering areas of concentration in cyber and information
- integrating cyber and information topics into the general curriculum.

Table 2.2 aligns the institutions with the approaches to cyber and information education that they provide.

---

[31] DoD, *DoD Cyber Workforce Management Board Charter*, January 13, 2017.

[32] John Sherman, "Statement by John Sherman Acting Chief Information Officer for Department of Defense Before the Senate Armed Services Committee Subcommittee on Personnel on Cyber Workforce," April 21, 2021.

[33] DoDD 3600.01, 2017.

[34] Joint Staff J3, *Operations in the Information Environment Curriculum Development Guide*, October 2019, p. ii.

[35] Joint Staff J3, 2019.

Table 2.2. DoD Educational Institutions' Approaches to Cyberspace and Information Education

Approach	Institution
Degree granted in cyber and/or Information	• AFIT • CIC (NDU) • NPS
Area of concentration offered in cyber and/or information	• AFCC[a] • USAWC • Eisenhower School (NDU) • NIU
General curriculum integrates topics in cyber and/or information	• Air War College • CISA (NDU)[b] • JFSC (NDU)[b,c] • MCU • National War College (NDU)[b] • Naval War College

[a] AFCC developed a master's curriculum in cyber strategy but had not secured funding to sustain the program and ceased its graduate programs as of AY 2022–2023.
[b] While the institution does not offer a degree specialization or area of concentration in cyber and/or information, students may enroll in NDU's two-course elective Cyber Studies Concentration (known as Cyber Security Leadership Concentration before AY 2021–2022). CIC offers six courses, and National War College offers one course in the concentration (NDU, *2021–2022 Electives Program Catalog*, 2021, p. 4). We do not classify this as an area concentration because it is below the three-course threshold that we use.
[c] JFSC's Joint Command, Control, and Information Operations School (JC2IOS) offers continuing education focusing on cyber and information topics. JFSC's main curriculum does not provide JPME-II credit, but JFSC's Joint Advanced Warfighting School does confer senior service school/JPME-II credit. With the exception of one Joint Advanced Warfighting School elective, neither provides cyberspace or information content.

A school that offers *a specialized degree* has graduate level coursework leading to either a master's or doctorate in a relevant field, such as software engineering, IO, or cyber systems and operations. CIC offers a Master of Science in Government Information Leadership (through a full-time, in-residence program that grants JPME-II credit for U.S. military officers and a part-time, hybrid program that does not grant JPME-II credit).[36] It also offers graduate certificates in cyber disciplines, such as Chief Data Officer and CIO. The AFIT and NPS have broad course offerings but largely focus on technical degrees. CIC offerings are aimed toward leaders and managers and are less technically focused than AFIT or NPS degrees, but nonetheless require some technical understanding of cyberspace principles and architecture.

Schools that offer cyberspace or information as an *area of concentration* typically require students to take at least three elective courses in cyber or information to qualify as an area of

[36] "The MS Degree program is currently titled Government Information Leadership (GIL), but is in the process of being renamed to Strategic Information and Cyberspace Studies" (CIC, *Academic Catalog AY 2021–2022*, NDU, 2021a, p. 9).

concentration within their degree program.[37] For example, USAWC grants a Master of Strategic Studies with an optional concentration in "Strategic Cyberspace Studies." In addition to core coursework, the cyber concentration requires completion of a cyber strategy related research project and three cyberspace electives. As another example, the Eisenhower School offers several "industry studies" with substantial content in cyberspace and information.

Finally, such schools as the Air War College and MCU have *integrated cyber and information topics into the general curriculum* for all students. These schools do not offer specialized degrees or areas of concentration in cyber and information (see note b in Table 2.2 for an explanation of special circumstances unique to NDU schools).

Educating Generalists and Specialists in Cyberspace and Information

In addition to overall approaches to cyberspace and information education, the educational institutions focus on different professional orientations within the graduate degrees they offer. We identified two primary professional orientations: specialist and generalist. Professionals who specialize in strategy, management, or technical applications and implications of cyberspace and information need education consistent with their specializations while also enabling them to understand the broader context that cyberspace and information feed into. In our analysis, we consider specific specialist orientations along these lines: strategy, management, and technical. Generalists must be able to integrate capabilities—including cyberspace and information—across domains to achieve objectives. Moreover, both specialists and generalists must be able to communicate effectively with each other.

Table 2.3 compares the educational institutions according to their degree programs' orientation and notes whether they are JPME-II accredited. Cell shading indicates each institution's focus, organized by column (darker shading indicates the institution offers a relevant degree specialization, whereas lighter shading indicates the institution offers an area of concentration). For ease of comparison, orange shading distinguishes CIC in the table. As the table shows, CIC is the only DoD institution offering a degree specialization in the areas of strategy and management.

[37] We use the term "concentration" informally to distinguish institutions that offer an in-depth, dedicated course of study in cyber and information from institutions that offer specific degrees in cyber and information. In most cases, our use of the term is equivalent to the "area of concentration" schools formally designate.

Table 2.3. Variations in Cyber and Information Graduate Degrees Offered by DoD Educational Institutions

Institution	Generalist Orientation	Specialist Orientations			JPME-II
		Strategy	Management	Technical	
NDU					
National War College	■				Yes
Eisenhower School	■	▒	▒		Yes
CIC		■	■		Yes
CISA	■				Yes
JFSC[a]					Yes
Air University					
AFIT			■	■	No
AFCC[b]					No
Air War College	■				Yes
USAWC	■	▒			Yes
MCU	■				Yes
NPS			■	■	No
Naval War College	■				Yes
NIU	■	▒			No

NOTE: Dark shading indicates degree specialization; light shading indicates areas of concentration. Dark orange shading is also for specialization and is used only to highlight CIC for ease of comparison.

[a] JFSC's graduate degree programs do not contain substantial cyber and information content (see note c to Table 2.2 and Appendix B).

[b] AFCC developed a master's curriculum in cyber strategy, which specialized in strategy and management. The college subsequently ceased operations in 2022.

Additionally, many institutions offer graduate certificates or continuing education on cyberspace or information. Table 2.4 compares the types of graduate certificates offered by the schools examined and indicates whether they offer cyberspace or information continuing education (including short courses). Again, CIC appears to occupy a distinctive niche in the DoD educational ecosystem. It provides multiple graduate certificates that span strategy and management specializations, as well as continuing education in cyberspace and information. Some other institutions do offer programs that address these areas, typically in a less-intensive or less-comprehensive fashion. For example, as the table notes, AFCC began a pilot program in January 2022 to offer a certificate with strategy and management content, although AFCC has subsequently stopped offering graduate education.

Table 2.4. Variations in Cyber and Information Graduate Certificates and Continuing Education Offered by DoD Educational Institutions

Institution	Graduate Certificate Specialist Orientations			Continuing Education
	Strategy	Management	Technical	
NDU				
National War College				
Eisenhower School				
CIC				
CISA				
JFSC				
Air University				
AFIT				
AFCC				
Air War College				
USAWC				
MCU				
NPS				
Naval War College				
NIU				

NOTES: Orange shading is used only to highlight CIC for ease of comparison. AFCC launched the Cyber Leadership Certificate as a pilot in January 2022 (shown in light shading).

Research and Engagement

All the institutions, except for JFSC, report that their faculties engage in research and publishing on cyberspace and information topics. At most of the schools, research plays a supporting role to instruction but is important for helping faculty maintain currency in their fields and for engaging with the wider DoD enterprise. Research also tends to be driven by individual faculty expertise and interests rather than reflecting an institution-wide research agenda. By comparison, research is more institutionalized and plays a more central role at AFIT and NPS (e.g., through doctoral programs, dedicated research grants). The schools also report participating in various types of engagement and professional service (e.g., informing DoD policy, hosting or providing guest speakers, convening conferences).

Customer Views and Challenges

Operational and Customer Views on Cyberspace and Information Education

To understand the cyberspace and information education needs of warfighters, we asked leaders from several combatant commands and the military services to participate in semistructured discussions with our project team. Not all the commands and services elected to participate, but we were able to interview representatives at headquarters elements and in operational commands, providing us perspectives that covered the strategic to the operational—the communities we determined most likely to benefit from staff educated on cyberspace and information at the DoD institutions we examined and potentially to benefit from other forms of service and engagement, such as operationally relevant research. Because we did not have the opportunity to speak with all the operational commands and the services, our findings are necessarily provisional and may not reflect the views of others we did not interview. That said, we did identify common themes across the 15 interviewees and seven organizations.

Most of the common themes that emerged involved demands on curriculum. Many participants argued that warfighters in general need more education in joint planning, joint cyberspace operations, nonkinetic warfare, and whole-of-government cooperation. They also conveyed that leaders specifically need greater understanding of cyberspace capabilities and a balance of strategic and technical education, while operators need the ability to communicate effectively with leaders. Several claimed that "overclassification" hinders learning, especially in cyberspace education, echoing faculty's desire for more unclassified (or lower classification) case studies. Several interviewees also argued that cyberspace and information curricula need to adapt quickly, with updates involving regular dialogue between educational institutions and operators, because operational circumstances are constantly evolving.

Similarly, many of the organizations desire more engagement with educational institutions to support the organizations' missions through continuing education. The commands and services we talked with supplement JPME with mission-related professional development (e.g., guest speakers, self-study, on-the-job training). However, such professional development opportunities appear to lack institutionalization and coordination, leaving their effectiveness up to individual initiative. This approach to professional development may also contribute to a lack of awareness of available professional development opportunities. For example, we observed that there is a perceived lack of senior-level guest speakers on the information environment. Organization representatives also expressed a desire for more service-initiated or -sponsored research conducted at DoD educational institutions.

Views of CIC's Graduate Certificate Programs

To understand CIC's unique graduate certificate programs in greater detail, we conducted semistructured discussions with 18 alumni of four CIC certificate programs.[38] We analyzed observations collected through discussions along seven themes: paths to CIC, program quality, learning objectives, CIC's fit in providing the certificates, what CIC certificates signal, work after CIC, and additional remarks.

We provided an unpublished project report to our sponsor and CIC to document our findings from these discussions so that CIC could use these findings in program evaluation and improvement. Here, we summarize the main points.

The CIC alumni we spoke with found, in general, that CIC certificate programs are relevant to their work, of high quality, and well-positioned within CIC and at NDU.[39] To the degree that commentary was not positive, it reflected a desire to expand CIC's certificate program offerings and capacity.

It is evident that CIC's degree programs benefit from synergies with the college's certificate offerings. Many of the certificate classes are cross listed with, or derived from, degree program courses. Offering coursework in this manner increases efficiency, in economic terms, by decreasing the average cost of per-student production. In addition, certificate programs appear to facilitate recruitment into the CIC degree programs.

Several alumni who started at CIC indicated that they came to CIC intending only to complete a certificate and ended up earning additional CIC credentials or completing the master's program. In addition to the original program certificate, four graduated from CIC with a master's degree and two earned an additional certificate. Those who earned master's degrees often explained the appeal and ease of applying certificate courses to meet degree requirements. DoD component staff and CIC graduates we contacted over the course of this research reported that they valued this education.

Challenges Educational Institutions Face in Delivering Cyberspace and Information Education

During discussions we held with faculty and staff at each of the 13 educational institutions, we observed several common challenges related to delivering cyberspace and information education. Each institution develops its own curricula and materials, which comes with drawbacks. Some schools lack sufficient faculty expertise to develop and refresh their own

---

[38] The four certificate programs are the Chief Financial Officer (CFO), CIO, Cyber Leadership, and Cyber Security programs. We did not interview graduates of the Chief Data Officer or the IT Program Management certificate programs because the former is too new to have a sufficient number of graduates with posteducation experience and because CIC is considering eliminating the latter.

[39] We specifically asked alumni of the CFO certificate program their view on whether CIC was an appropriate home for the CFO Academy, or if there was another institution that would be better. Those expressing an opinion on this thought CIC was appropriate, with one interviewee commenting that "finance lives in the cyber domain."

curricula and materials, leading to suboptimal and dated content. College faculty frequently expressed a need for unclassified case studies or at least at a lower classification than Top Secret, neither of which they were able (or incentivized) to curate or procure on their own.

Two observations are unique to DoD institutions other than CIC. First, cyberspace and information educational content risks being crowded out by other demands on course time because of shifting priorities and limited resources. To paraphrase what we heard on multiple occasions, "if you add something to the curriculum, you have to take out something else." Second, some staff appear to have an incomplete picture of cyberspace and information education offerings in other parts of the DoD educational ecosystem (i.e., expressing surprise when we informed them of specific courses of study or resources).

Opportunities for CIC

As the previous section explains, while DoD educational institutions are interested in expanding their cyber and information content, they face challenges in doing so. CIC could assist the whole ecosystem by functioning as a cyberspace (and perhaps information) "center of excellence." As such, it could develop curriculum materials, such as case studies that could be used across the institutions. CIC previously facilitated curriculum development conferences through the Cyber PME Consortium, but coronavirus 2019 restrictions led CIC to cancel the meetings after the first event in 2019.[40] CIC has reinstated this event and could expand it to play a convening and information-sharing role, enabling institutions to see a fuller picture of which institutions are pursuing which topics in these domains and to coordinate their activities for greater efficiency and effectiveness. In the domains of research and engagement, CIC can similarly serve DoD with outreach and knowledge discovery that are relevant to DoD's cyberspace and information missions.

The discussion of supply and demand in the next chapter highlights potential needs for information and cyber education that CIC could support beyond expanding its own educational offerings.

[40] CIC, "Cyber PME Colloquium," website, undated-c.

Chapter 3. Comparing Demand and Supply for Cyber and Information Education

In this chapter we address the potential demand for cyberspace and information education and compare that with the current throughput of the DoD educational institutions.

Determining Potential Demand for Cyberspace and Information Education

In contrast to training requirements for cyberspace and information roles, what education is needed for specialists in these domains is less well defined, particularly at the JPME-II and equivalent graduate levels.[1] Because our focus is on the role of CIC and how it can meet the educational needs of the department, we determined that our examination of demand should focus on the ranks and roles that would most likely benefit from the CIC curriculum or other specialized education at other educational institutions.

The cyberspace workforce has defined work roles in the DCWF, intended to apply across the spectrum of DoD personnel. The DCWF was developed to standardize and categorize cyber workforce roles to streamline identification, tracking, and reporting.[2] The DCWF groups cyber work roles into five overarching bins: cyber IT, cybersecurity, cyber effects, intelligence (cyber), and cyber enablers. There are a total of 54 cyber work roles in the DCWF.[3] These roles sometimes align with military operational specialties and Air Force specialty codes, but not always. There is not yet an equivalent of the DCWF for other information functions.

For the information environment, we reviewed current joint doctrine and previous RAND work on the information environment to identify relevant roles.[4] We identified 17 DCWF work roles and 16 information environment job functions that we assessed would be most likely to benefit from this type of education. We also gave an option for the respondents to add additional roles they deemed relevant. We requested data on the roles listed in the box on p. 23.

---

[1] Military specialties, such as a Cyber Operations Officer or Psychological Operations Specialist, will have required training progression and the Defense Cyber Workforce Framework defines training requirements for many of the work roles.

[2] Greg Belding, "Introduction to the DOD Cyber Workforce Framework (DCWF)," webpage, Infosec, October 26, 2020.

[3] DoD, "DoD Cyber Workforce Framework," website, undated.

[4] At the time we developed the RFI, the prevailing joint doctrine was Joint Publication 3-13, *Information Operations*, change 1, November 20, 2014. Joint Publication 3-04, *Operations in the Information Environment,* was being developed but had not yet been published as of this writing. For a relevant RAND report, see Michael Schwille, Anthony Atler, Jonathan Welch, Christopher Paul, Richard C. Baffa, *Intelligence Support for Operations in the Information Environment: Dividing Roles and Responsibilities Between Intelligence and Information Professionals,* RAND Corporation, RR-3161-EUCOM, 2020.

Defense Cyberspace Workforce and Information Environment Roles and Job Functions Included in the Request for Information

DCWF Work Role (Work Role Identifier)	Information Environment Job Function or Role
All-Source Collection Manager (DCWF #311)	IO planners
All-Source Collection Requirements Manager (DCWF #312)	IO Intelligence planners
Cyber Intelligence Planner (DCWF #331)	IO legal advisors
Cyber Operations Planner (DCWF #332)	IO program manager
Partner Integration Planner (DCWF #333)	All-source collection requirements manager (if not already captured in cyberspace above)
Authorizing Official/Designating Representative (DCWF #611)	IO assessments leads
Cyber Instructional Curriculum Developer (DCWF #711)	Civil-military operations (CMO) planners
Cyber Instructor (DCWF #712)	Public affairs representatives
Cyber Legal Advisor (DCWF #731)	Operational security (OPSEC) officers
Cyber Workforce Developer and Manager (DCWF #751)	Operational security (OPSEC) planners
Cyber Policy and Strategy Planner (DCWF #752)	Counterintelligence officers
Program Manager (DCWF #801)	Military deception (MILDEC) officers
IT Project Manager (DCWF #802)	Cyber and electronic warfare officers
Product Support Manager (DCWF #803)	Electronic warfare specialists
IT Investment/Portfolio Manager (DCWF #804)	Psychological operations (PSYOP) officers
IT Program Auditor (DCWF #805)	Technical effects officers
Executive Cyber Leadership (DCWF #901)	

We then worked with the sponsor to develop an RFI based on these work roles and functions. This RFI's assessment had two goals. First, we aimed to understand what the potential needs for cyberspace and information education for senior and midlevel leaders and managers are across the department.[5] Second, we wanted to examine the purpose of the types of education to prepare personnel to lead organizations; develop and implement policy, strategy, and plans; manage cyberspace and information programs; and execute cyberspace and information missions in support of the National Defense Strategy. Two populations benefit from DoD cyberspace and information environment education and training. The first population is personnel—military or civilian—who have defined work roles in cyberspace or the information environment. The second population is personnel who do not have specific cyberspace or information environment work roles but would benefit from cyberspace and information education. Examples of the latter are personnel who are in line to lead planning efforts at operational and strategic commands and program managers and acquisition professionals. Our RFI was developed to capture the anticipated requirements for personnel, focusing on the field grade officers and the civilian

[5] We did not have a reliable method for requesting similar data from other U.S. government departments and agencies.

equivalents of General Schedule (GS)-13 to GS-15, with identified cyber work roles and non-cyberspace work roles for FY 2022 to FY 2027. The RFI was sent out to the military services, a subset of the defense agencies that we identified as likely to require cyberspace and information professionals (such as the National Security Agency and Defense Information Systems Agency, but also the Pentagon Force Protection Agency and Defense Media Activity), OSD components, and the combatant commands requesting numerical data on the work roles and job functions we identified and included an open-ended question on needs for education for the broader workforce on these topics.

There is some potential for double-counting (particularly for all-source collection requirements managers and the cyber and electronic warfare officers), and we asked the respondents to provide unique counts of each role. In subsequent conversations with the services, in particular, we clarified that military occupational specialties or Air Force specialty codes could be provided as separate counts rather than attempting to align them to DCWF work roles that would be misleading or fit poorly into the work roles.

The RFI yielded inconsistent and incomplete responses. For the numerical data responses, we received incomplete data where the responding component may have only provided data for certain FYs or did not provide data for cyberspace work roles or information job functions. This resulted partially from the fact that components often have a single point of entry for cyberspace work roles (e.g., service principal cyber advisors) but not for the various information environment functions. In some cases, respondents only provided military or civilian personnel counts, but not both. We also received additional data from one respondent that went into more detail. Furthermore, we are unaware of the method each respondent used to gather the number of billets per FY and the methodology used to project needs in future FYs.[6] The open-ended responses gave varying degrees of specificity, and not all respondents provided a response to that query. With this in mind, we sought to follow up with each respondent, including those who did not respond, to fill in the gaps in the data or to clarify their responses. We were not able to have discussions with all the respondents, and the information gathered was inconsistent.

Table 3.1 summarizes the number of filled field grade officers (O-4 to O-6) and civilians in cyberspace and information work roles that we identified through the RFI that would benefit from cyberspace and information education.[7]

[6] We did ask the respondents to identify whether outyear projections were validated requirements or estimates.

[7] For consistency, we also treat Navy O-4s (lieutenant commanders) as a field grade position, although the Navy does not consider them field grade as the other services classify O-4s.

Table 3.1. Estimates of DoD Cyber and Information Personnel Inventory, Fiscal Year 2022

	Cyber		Information	
DoD Component	**Military**	**Civilian**	**Military**	**Civilian**
Army	1,738[a]	13	No data received	29
Air Force	990	2,491	No data received	No data received
Navy	345	16,764	484	211
Space Force	244	0	0	0
Marine Corps	360	482	152	No data received
OSD, Joint Staff, and field agencies and activities[b]	97	523	67	170
Combatant commands[b]	13	74	46	24
Totals	3,787	20,347	749	434

NOTE: Inventory is for filled billets, as opposed to authorized billets.

[a] Includes Army Military Occupational Specialties 17A, 17B, 17D, 25A, 35D, and 35G.

[b] Incomplete data.

As we just noted, the data we received were inconsistent and incomplete. For information personnel, several services were not able to supply any estimates of inventory for military personnel, civilian personnel, or both. As a result, we expect that the numbers we did receive represent an undercount of the total personnel in this domain.

For the cyber personnel inventory, we especially highlight large differences among the Navy, Air Force, and Army in civilian personnel. Although we acknowledge that the services will take different approaches to the balance of military and civilian personnel filling these roles, the striking disparity among these civilian personnel inventories raises concerns about the validity of the data. We will address these concerns later in this chapter with a sensitivity analysis.

In terms of components outside the services, only some OSD components, field agencies, and field activities provided responses. For the combatant commands, we received a direct response from one command while three others reported through the Joint Staff, leaving us without data on the remaining commands. These omissions also contribute to undercounting personnel inventory in both the cyber and information domains.

Determining DoD Educational Institutions' Current Production of Graduates in Cyberspace and Information Specialized Degrees and Certificates

The 13 institutions in the DoD educational ecosystem provide some form of senior-level cyberspace and information education. Only a subset of these institutions currently provides the type of specialized education under examination. As Chapter 2 describes, six institutions integrate cyber and information within their general curricula and do not have specialized

degrees or areas of concentration in cyberspace or information. We did not include these six institutions when estimating the supply of cyber and information education because they do not directly meet cyber or information workforce personnel requirements, although they clearly play an important role in exposing generalists to cyberspace and information concepts. Furthermore, recall from Chapter 1 that this report focuses on education, not training. We did not include the provision of short courses or similar forms of professional development as components of supply. Consequently, graduate degree and certificate programs with a major or area of concentration in cyberspace and information represent the supply of DoD cyber and information education. To estimate this supply in a manner comparable with demand, we obtained the number of students each institution graduated in AY 2020–2021.[8]

Table 3.2 summarizes the student graduation data provided by educational institutions in our research. It presents our overall estimate of DoD cyber and information education graduate supply and facilitates comparisons between different types of education offered.[9] The table rows list institutions organized by the three program orientations discussed in Chapter 2: (1) strategy and management, (2) management and technical competence, and (3) cyber and information as an area of concentration. Table columns distinguish a major from an area of concentration, as well as degree from certificate. Unless otherwise noted, cell values indicate the number of students conferred degrees or certificates in AY 2020–2021.

Using our analysis of detailed data provided by each educational institution, we estimate that, of the 981 annual graduates shown in Table 3.2, about 600 represent DoD military personnel; about 300 represent DoD civilian personnel; and the remaining approximately 80 represent a combination of other U.S. government civilians, international military, and industry. This breakdown is further discussed in the next section. We note that these data do not represent the full production capacity at these institutions; some indicated in our interviews that they could expand capacity if called to do so.

[8] Other ways to operationalize supply include considering institutional resources (e.g., funding, staffing, facilities) or services (e.g., classes, degree and certificate programs). We used institutional capacity, approximated here by student throughput, as tractable and more directly comparable with demand estimates provided in the preceding section. Furthermore, in most cases, student throughput can also convey information about resources, such as current staffing levels, because student-to-faculty ratios in JPME programs are relatively stable.

[9] The following section in this report elaborates comparisons between institutions.

Table 3.2. Estimates of DoD Cyber and Information Education Supply, Academic Year 2020–2021 Graduates

		Cyber and Information Major			Cyber and Information Area of Concentration	
Area	**Institution**	**Master's**	**Doctorate**	**Certificate**	**Master's**	**Total**
Cyber and Information strategy and management	CIC	117	N/A	80	0	197
	Subtotal	117	N/A	80	0	197
Cyber and Information management and technical	AFIT[a]	157	4	19	0	180
	NPS	276	6	188	0	470
	Subtotal	433	10	207	0	650
Cyber and Information areas of concentration	AFCC	0	N/A	14[b]	0	14
	USAWC	0	N/A	0	22	22
	Eisenhower	0	N/A	0	63	63
	NIU	0	N/A	10	25	35
	Subtotal	0	N/A	24	110	134
	Grand total	550	10	311	110	981

SOURCE: RAND analysis, based on data provided by each educational institution.

NOTES: If individual graduates of an institution earn multiple credentials, they are counted only once under the most advanced credential. Not all institutions grant doctoral degrees, indicated by "N/A."

[a] Due to complexities of mapping the many AFIT degree programs that provide access to cyber and information courses, we counted AFIT graduates who completed three or more courses in cyber and information.

[b] Degree and certificate counts are based on AY 2021–2022 enrollment because conferral counts were not provided. Because the program has one cohort per year, the student counts are likely similar to conferrals.

Comparison of Demand and Supply

To place these figures in perspective, we present approximate comparisons of our estimates of demand and supply. To do so, we need to estimate the annual demand for graduations based on the personnel inventory we obtained from the services and other DoD components.

Discussions with the services indicate that they typically plan that about 20 percent of field grade officers will complete graduate education each year. Table 3.1 shows that the services and other components estimate they have about 4,500 field grade military officers in cyber and information specialties. Using the 20 percent rate of annual completion, this population generates a demand of about 900 graduations per year. As we explained previously, current throughput of cyber and information specializations in the DoD education system is about 600 military personnel, so the current system is producing about 67 percent of the estimated throughput needed.

While the services did not specifically estimate a similar ratio for civilian personnel, they indicated that civilians are anticipated to work more years between educational experiences than field grade military officers and that some civilians start their careers with graduate education

already completed (while this is rare for military officers). To generate a rough estimate, we assumed that about 10 percent of civilians will complete graduate education each year. Because Table 3.1 shows about 21,000 DoD civilian cyber and information civilian professionals, this generates a demand of about 2,100 graduations per year. The current estimated throughput of DoD civilians is 300, so the current DoD system is producing about 14 percent of the estimated throughput needed.

As explained earlier, our data have omissions and inconsistencies. Because of partial responses, the data are not likely to capture all personnel inventory, and the actual coverage of needs may be lower than we estimate earlier. There may also be effects in the other direction. The large Navy civilian cyber personnel inventory seems inconsistent with the other services and accounts for about 80 percent of all the civilian inventory. The Army value is quite low compared with the other services. As a sensitivity analysis, we considered the results of using the Air Force civilian cyber personnel inventory as an estimate to replace both the high Navy and low Army values. This substitution reduces the civilian professionals to about 9,000, generating and estimated annual demand of 900. The current estimated throughput of DoD civilians, 300, would thus represent 33 percent of the throughput needed. Even with this sensitivity analysis scenario, there is still a significant unmet need for DoD civilians. Because the sensitivity analysis concerns only civilians, our estimates for military personnel are unaffected.

DoD institutions also serve the needs of other federal agencies and international military partners. While we do not have estimates of the potential demands from these sources, we think it is reasonable that some fraction of DoD's capacity will continue to serve these needs.

DoD institutions need not satisfy all potential demands. Aside from the DoD educational institutions, military officers and, especially, civilians also complete graduate education at civilian institutions. Because civilians have multiple options to complete graduate education, the low (14–33 percent) DoD coverage of estimated civilian requirements may not prevent civilians from acquiring the knowledge and skills they need, but these individuals are likely obtaining the knowledge and skills from sources with much less relevance to federal and DoD policy and planning concepts that may help them perform in DoD.

Military officers are likely to complete PME required for future promotions (e.g., JPME-II). Because the current DoD system covers only 62 percent of the estimated military demand, many military officers in cyber and information roles are likely getting more general PME without the cyber and information content that might help them perform their duties.

Aside from these broad comparisons, Table 3.2 shows that the topical focus of the current DoD system may not cover all DoD's needs. In particular, AFIT and NPS account for 66 percent of graduates in cyber and information programs, focusing on technical education. NIU accounts for an additional 4 percent of students, focusing on intelligence topics. Thus, among these three specialized institutions, about 70 percent of the throughput is in technical or intelligence areas rather than broader strategic management of cyber and information that DoD also requires.

CIC does focus on strategy and management of cyberspace, is one of only two DoD institutions with that focus, and is more mature and established than AFCC. CIC accounts for 20 percent of graduates, which appears to be a modest proportion, given the importance of these skills in DoD, as shown by the priority that DoD customers place on such skills reported in Chapter 2. Our data analysis and interviews indicate that the services see value in a cyber-information-focused JPME-II program, such as the one CIC offers, but they have not signaled a need to increase the number of officers they send to CIC. The graduate certificate programs' enrollment is currently about one-third of its prior peak, and the hybrid master's enrollment has also fallen from its peak, indicating that CIC can expand these programs in the coming years with little difficulty. Such expansion could help DoD meet more of its needs to educate cyber workforce professionals.

Although all these calculations are necessarily approximate, the clear message is that DoD needs at least its current capacity to educate cyber and information professionals and should likely look for opportunities to grow, particularly in the strategy and management focus areas that CIC specializes in (especially if the services indicate greater demand in the future) because these focuses are not well represented in other DoD educational institutions. Also note that other U.S. government departments and agencies have personnel who attend DoD schools. We do not have data to indicate future demand or requirements from these agencies; however, because these demands have persisted over time, we anticipate that they are likely to continue.

Chapter 4. Evaluating Options for the College of Information and Cyberspace

Our analysis in Chapters 2 and 3 identified the role that CIC plays in educating cyber and information professionals in DoD. CIC's focus on DoD and federal strategic management in these domains gives it a distinctive remit within DoD, and our analysis of demand and supply indicates that CIC is needed within the DoD ecosystem.

CIC can play several roles in that ecosystem. In this chapter, we focus on options to align CIC's core educational missions with governance and funding. As we observed in Chapter 2, schools can also make important contributions through research, engagement, and service to other educational institutions, DoD components, other federal agencies, and the public. In Chapter 5, we will address ways CIC can strengthen its approach to these roles and support the entire DoD ecosystem.

CIC's Missions, Governance, and Funding

CIC serves two audiences in education. First, joint warfighters attend the in-residence master's program and earn JPME-II credit to prepare for senior uniformed leadership roles, including as future general and flag officers. Second, DoD and other federal cyber and information workforce professionals (and a small number of industry professionals and international partner officers) attend the hybrid master's and graduate certificate programs that prepare them for various uniformed and civilian roles in these domains. CIC also offers continuing education to serve this workforce.

There is tension between serving these two populations at CIC. CIC's governance and resourcing clearly enable the program for joint warfighters. CIC performs this core mission under the Joint Staff's resource sponsorship and with direction from CJCS (through DJ-7) to the president of NDU. In 2018, CJCS certified CIC to provide JPME-II education after a pilot program that began in August 2015. The CJCS fully accredited CIC in 2019 through 2025.[1] Importantly, CIC initially established the JPME program from existing resources it received for the cyber workforce education. It did not receive dedicated funding for the JPME program.[2] The DoD CIO funded CIC's cyber workforce education programs until 2012, at which time the Joint

[1] Director for Joint Forces Development, "Process for Accreditation of Joint Education (PAJE)," memorandum for Chancellor (Acting), College of Information and Cyberspace, May 1, 2019. The initial pilot program allowed for JPME credit through a National Security and Cyberspace Studies concentration within the existing master's program.

[2] Discussions with NDU and CIC leadership, August 1, 2022.

Staff assumed responsibility for funding the school based on an agreement between the DoD CIO and DJ-7.[3]

The DoD CIO, the USD(C)/CFO, and USD(P) have historically relied on CIC for workforce education. A series of agreements between NDU and each of these three stakeholders has complicated CIC's governance and funding. For example, CIC currently operates the CFO Academy, monitored by the USD(C)/CFO and resourced by NDU and a variety of DoD components.[4] The academy was originally launched in 2008 with funding provided by the USD(C)/CFO.[5] The academy's placement in CIC at that time was predicated on the determination that CIOs and CFOs needed to collaborate to transition federal departments and agencies to using IT more effectively and efficiently and that CIC's existing curriculum created benefits for both communities.[6] The DoD CIO oversees CIC's CIO certificate program, which was originally established in 1997.[7]

While the DoD CIO no longer sponsors the CIO program, DoDD 8140.01 assigns the DoD CIO the responsibility to "[establish], in coordination with the CJCS, academic programs at the National Defense University to educate leaders in IT, information resources management, and cybersecurity requirements and capabilities."[8] This mandate means that the DoD CIO works with the Joint Staff and NDU to ensure that courses are relevant to cyberspace workforce needs, but as a practical matter, NDU will be most responsive to the needs of its funding sponsor, the Joint Staff. DoDD 8140.01 does not assign a corresponding responsibility to the CJCS, although the chairman does have a general responsibility for education that facilitates joint force development.

Shared governance and resourcing are not unique to CIC among NDU schools. For example, the Office of the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict sponsors CISA's Regional Defense Fellowship Program,[9] and Defense Acquisition University partners with the Eisenhower School in offering Eisenhower's Senior Acquisition Course.[10]

---

[3] Takai, 2012.

[4] DoDI 1025.10, *Chief Financial Officer (CFO) Academy*, June 22, 2018.

[5] Under Secretary of Defense (Comptroller)/Chief Financial Officer and the National Defense University, Memorandum of Agreement, March 13, 2008.

[6] Brenner, Burton, and Ketrick, 2012, p. 12.

[7] Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, "DoD Chief Information Officer (CIO) Certificate Program," memorandum, February 28, 1997.

[8] DoDD 8140.01, 2020, p. 4.

[9] Memorandum of Agreement Between the Office of the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict (OASD[SO/LIC&IC]) and the National Defense University, December 20, 2010.

[10] Eisenhower School for National Security and Resource Strategy, "Senior Acquisition Course," webpage, undated.

Reflecting CIC's history and sponsoring stakeholder interests, the college's primary focus has been on cyberspace and IT management, while its focus on other information-related capabilities has varied over time.[11] The college piloted a JPME-II program in Information Warfare and Strategy in 1991, then offered an IO elective concentration to National War College and Eisenhower (then the Industrial College of the Armed Forces) students starting in 1992. The concentration ceased in 2012, shortly after the primary faculty member leading it retired.[12] While CIC's vision statement expresses a goal of being "the premier national security educational institution focused on the information environment,"[13] and the college has some faculty with relevant expertise, most CIC faculty in recent years have focused on cyberspace.[14] The college is reinvigorating the information aspects of its curriculum to integrate it more fully, and has recently hired additional faculty with expertise in IO/OIE. For AY 2022–2023, each master's student will take classes titled Foundations of the Information Environment, Information Warfare Strategy, and Strategic Competition in the Information Environment.[15] At the same time, other NDU schools also address aspects of the information environment. For example, the JC2IOS at JFSC offers short courses in IO and MILDEC, and CISA emphasizes information concepts in its curriculum on irregular warfare.

Lessons from Civilian Master's Programs

A RAND NDRI project on DoD PME conducted in parallel with this research developed case studies of five civilian master's programs aimed at professional students, with the goal of learning lessons that could be applied to PME programs. From these case studies, the team learned that these civilian programs have a clearly identified market that drives educational offerings. Whether promoting a program aimed at local governance issues, expertise in supply chain management, or cybersecurity, many civilian institutions have identified specific populations of interest and tailored coursework and experiential learning to meet the needs of a desired market.

The cases also revealed how civilian institutions regard their own value proposition. In these programs, the skills taught directly align with the abilities both students and future employers

---

[11] For example, in CIC's 2019 self-study report for PAJE recertification, it states a weakness:

> Reflecting its initial charter, the curriculum is currently weighted toward the strategic use of the cyberspace domain and an insufficient weighting of strategic information warfare. Going forward, a larger portion of the curriculum will need to be allocated toward teaching information warfare concepts and the use of cyber capabilities to conduct strategic information operations. (CIC, *Self Study Report for PAJE Accreditation*, 2019, p. 47)

[12] Email correspondence with College of Information and Cyberspace leadership, August 8, 2022.

[13] CIC, "CIC Overview," webpage, undated-a.

[14] CIC previously offered an Information Operations Certificate and an Information Operations concentration within its Master of Science program (Brenner, Burton, and Ketrick, 2012, p. 12).

[15] Email correspondence with CIC leadership, August 8, 2022.

seek and are updated to meet the desired qualifications of the professional market. By maintaining sharp focus on developing specific skill sets and marketing them to carefully identified individuals, civilian programs simultaneously keep a competitive edge in the marketplace and ensure their continued value regarding the future professional success of graduates.

While PME programs operate in a different context, military educational programs would benefit from both this kind of highly specific market identification and the tailoring of educational programs to meet the current (and likely future) needs of the services. Market forces compel civilian institutions to find a competitive edge in a way that a military educational system may not, yet DoD still stands to benefit from careful thought about which individuals best fit educational programs and how the programs could more effectively meet the professional needs of the force. Potential innovations could include more-intensive consideration when matching officers with enrollment in existing programs, greater focus on the connection between educational programming and professional needs, and even the potential for greater uptake of individuals from industry in the defense education enterprise to expand the pool of individuals capable of meeting DoD needs in the private sector.[16]

CIC faces similar challenges in many respects. It operates in an ecosystem with multiple providers, many of which offer or are developing offerings in cyberspace and information. To thrive in this environment, CIC needs to distinguish its offerings, market them to identified groups of potential students, and continue to align its offerings with the needs of DoD employers.

Options for CIC Mission and Governance

Taken together, this discussion highlights the importance of aligning mission, governance, and resources to position CIC for success in the future. As mentioned earlier, we considered options related to CIC's primary missions to educate leaders and managers in cyberspace and information in this analysis. Focusing on the two missions CIC is responsible for—JPME-II and cyber workforce education—we considered four options for aligning CIC's core education function and its governance:

1. continue both missions with the current governance arrangements focused on JPME-II
2. continue both missions and adopt dedicated funding and governance for cyber workforce education
3. continue both missions and add governance (but not funding) for cyber workforce education
4. focus CIC exclusively on JPME-II and cease cyberspace workforce education.

[16] Several of these ideas are also developed in Mayberry et al., 2021.

Table 4.1 summarizes our assessment of the implications of these four options. Option 1 is a continuation of the status quo. Its benefit is that governance remains straightforward and focused on a single line related to JPME-II. But it does nothing to resolve the tension with CIC's broader workforce mission and leaves those programs vulnerable to future cuts.

Options 2 and 3 add a governance arrangement for the cyber workforce mission either with funding (Option 2) or without (Option 3). Both options may increase CIC's responsiveness to the cyber workforce mission but also complicate the governance of CIC by adding additional stakeholders to the governance structure who may express different priorities and requirements for CIC. Option 2 may make this mission more sustainable because it will be tied to a dedicated source of funding, but that source of funding will need to be identified. Dedicated sources of funding to support each of the two mission areas means that each stakeholder has a vested interest in the college's success and makes it harder in future to either focus on just one mission or to de-emphasize a mission, as long as the funding is sustained.

Table 4.1. Comparison of CIC Mission and Governance Options

Options	Resource Implications	Benefits to DoD	Risks
1. Status quo	Neutral	• Straightforward governance structures and funding line	• Non-JPME programs vulnerable to future cuts
2. Add governance and funding for cyber workforce	Dedicated funding for cyber workforce education	• Cyber workforce education delivery more sustainable • Responsive to cyber workforce needs	• More complex governance structure and funding lines
3. Add governance for cyber workforce (no funding)	Neutral	• May increase responsiveness to cyber workforce needs	• More complex governance structure • Lack of funding can still decrease emphasis on cyber workforce programs
4. Focus exclusively on JPME	Potentially free resources at NDU	• Clarifies CIC governance and funding • Resources could be used for cyber workforce education elsewhere or other missions	• Unclear there is a better source for cyber workforce programs • Reduce curriculum breadth for JPME-II program • Decreased educational opportunities for cyber and information workforce • Could signal deprioritizing cyber education to Congress and other audiences

Option 4 is the most radical. It removes the cyber workforce mission and focuses CIC entirely on joint warfighter education, likely shrinking CIC significantly. While this option aligns governance and mission, it does so by removing the valuable cyber workforce mission. Such a change would free resources at NDU but would likely require DoD to invest the resources

elsewhere. That may not be a cost-effective approach because of the high faculty-to-student ratios DoD educational institutions are required to maintain for JPME-designated programs. We did not identify an obvious candidate to take over these missions aside from CIC.

Because our analysis indicates that DoD benefits from both of CIC's missions, Option 4 is the least preferred. While Option 1 preserves both missions, it does not address the deficiencies in governance (i.e., that there is no advocate for the cyberspace workforce with a voice and a stake in funding needed programs), which have, in the past, led to calls for closing or downsizing the college. Therefore, Options 2 and 3 offer the best prospects for meeting anticipated DoD needs. These options both require one or more proponents of the cyber workforce in the governance structure, which can complicate governance. New governance stakeholders will bring different perspectives and priorities that are needed but can cause additional friction because these stakeholders have to work together to agree a path forward. Two organizations have roles in DoD that may make them suitable governance partners. DoD CIO is lead in OSD for cyber workforce management and previously occupied such a position in the governance and funding of CIC.[17] USCYBERCOM's missions give it an interest in the development of joint warfighters *and* the cyber workforce, which may enable it to serve such a role with CIC. That said, one could argue that, as a combatant command, it would still prioritize the needs of joint warfighters over the cyber workforce needs because much of the "operate and defend the DoD Information Network" mission is delegated to the Joint Force Headquarters DoD Information Network at the Defense Information Systems Agency.[18]

In general, governance is strengthened when accompanied by resources, so providing a funding line for the workforce mission should reinforce the substantive role that one of these proponents could play in governance of CIC's workforce mission. Although we did not conduct a cost analysis to determine what an appropriate level of funding should be, CIC's historical funding profile indicates that it would likely not exceed more than a few million dollars.

[17] Also note that the principal cyber advisor also engages on cyberspace training and education issues but has a much smaller staff than either DoD CIO or USCYBERCOM and does not have funding it can dedicate to supporting CIC.

[18] Defense Information Systems Agency, "Director," website, undated.

Chapter 5. Recommendations and Conclusion

DoD recognizes the importance of educating specialists and generalists in cyberspace and the information environment. Its educational institutions are working to meet the need, although potential demand is greater than the current throughput can address. The schools do have room to grow and could accommodate more students, and it appears that there is scope for improving the development and delivery of course content, operationally relevant research, and subject-matter expertise. The projections of demand for this education are murkier for a variety of reasons, including continued challenges with identifying and tracking personnel in relevant positions and specialties and with competing budgetary pressures that can tamp down demand.[1]

Recommendations

Maintain CIC's Dual Mission Educating Joint Warfighters and the Cyberspace Workforce

We found that DoD has an enduring need for warfighters and other cyberspace personnel with sophisticated understanding of how to develop and employ cyberspace capabilities in furtherance of national security and defense objectives. Eliminating or reducing CIC's role in providing that education does not automatically mean that other DoD institutions or civilian counterparts are positioned to pick up the slack. Other DoD education institutions do not provide the same expansive strategic and management focus on cyberspace and information that CIC does; civilian institutions lack the defense and federal context that senior leaders and managers require to effectively navigate government in pursuit of national security objectives. There are synergies between the different CIC programs that would be lost if one or more of them was eliminated.

Advertise CIC's Programs More Effectively Across the Department and Beyond

CIC is not as well known across the department as it should be, even in its targeted communities, which means that its value and offerings are known mostly through word of mouth. One senior leader at a cyberspace component command for example admitted that he was not familiar with CIC's curriculum or programs. Some of this lack of awareness may also be due to the multiple name changes over the past ten years, which means that CIC's brand does not have the market penetration and name recognition it needs. CIC, NDU, and military and civilian

[1] One combatant command acknowledged that it would likely need more cyberspace and information personnel in the future, but its projection across the Future Years Defense Program was flat because of expectations that authorized headquarters endstrength would remain constant or potentially decrease.

education policymakers should work with the services in particular but also with all DoD components to make more people aware of CIC and its programs.

As the curriculum and value of CIC's offerings become more broadly known across the department, demand for spaces for students may increase. CIC has indicated it has the capacity to expand its JPME-II classes and could also increase non-JPME-II enrollment if demand increases. Until the demand manifests, CIC should continue to offer at least the current number of spaces in its programs but posture itself to expand to meet demand in the future. It should also be noted that maintaining the dual focus of the school ensures that CIC can sustain an adequate faculty depth to accommodate future increases in demand.

Strengthen Governance Arrangements for the Cyberspace Workforce Education Mission

CIC's mission to support the education of the cyberspace workforce has suffered over the years as financial and governance support has shifted and faced repeated plans to downsize or eliminate it. We assess that this lack of support is a direct consequence of the shift in governance in 2012 and concomitant removal of financial support to the college from the DoD CIO, who has a vested interest in supporting the development of the cyberspace workforce.[2] We therefore recommend that DoD identify one or more governance partners to take on this responsibility, to complement the Joint Staff's focus on the joint warfighting community, and promulgate a DoD Instruction to lay out the governance roles and responsibilities. We also recommend revising DoDD 8140.01 to clarify the CJCS role in coordinating with DoD CIO on establishing cyberspace academic programs at NDU that address the total force needs of the department.

More importantly, we assess that aligning funding streams with cyber workforce education governance would strengthen and sustain that part of CIC's mission with more durability than a governance role without funding could possibly achieve.

Position CIC as a Resource on Cyberspace Education and Research Across DoD

Cyberspace is an increasingly important operational domain in which the United States competes with adversaries, cooperates with allies and partners, and benefits from its contribution to continued economic dynamism and vitality. How cyberspace capabilities will evolve is difficult to forecast with any certainty beyond the next few years. Increasing networking, smart everything from buildings to cities, artificial intelligence, machine learning, quantum computing, and so forth will continue to evolve and will shape national security decisions into the future. We heard from many DoD educational institution representatives that they feel they are on their own when it comes to developing course content. We also heard from DoD components that there is a

[2] We could not identify the specific reason for the shift in funding, although Brenner, Burton, and Ketrick, 2012, indicates that the DoD CIO at the time was sufficiently concerned about potential elimination of the college to commission a study of the matter.

need for operationally relevant research and expertise. CIC is well placed to serve both these needs. We therefore recommend that CIC reinvigorate and increase its role as a "center of excellence" for cyberspace curriculum development, including collecting and crafting case studies at appropriate classification levels for schools across the DoD educational ecosystem. We also recommend that CIC solicit inputs from DoD components to shape a research agenda that can contribute directly to their missions.

Improve Cross-Departmental Accounting for Cyberspace and Information Environment Work Roles and Functions

Despite many years of effort, DoD components continue to struggle to identify current and future workforce needs against common frameworks like the DCWF. The need for cyberspace and information professionals—both military and civilian—will likely grow in the next decade as the nation faces a rapidly changing technological landscape. DoD cannot keep up with these challenges if it cannot adequately account for the personnel it has in these work roles and job functions and use this accounting as a basis to project future demand.

Concluding Thoughts

CIC is an important component of the DoD educational ecosystem that brings value in terms of the education, research, engagement, and service it provides, but its role can be reinforced and sustained through implementation of these recommendations. By doing so, the department can demonstrate its commitment to ensuring a workforce that is prepared to think critically about cyberspace and the information environment and about how DoD, with its partners in other departments and agencies and abroad, can achieve national security objectives through integration of capabilities.

Appendix A. Legislative Requirement from Public Law 116-283, 2021

SEC. 1741. MATTERS CONCERNING THE COLLEGE OF INFORMATION AND CYBERSPACE AND LIMITATION OF FUNDING FOR NATIONAL DEFENSE UNIVERSITY.

(a) PROHIBITIONS.—The Secretary of Defense may not—

(1) eliminate, divest, downsize, reorganize, or seek to reduce the number of students educated at the College of Information and Cyberspace of the National Defense University, or

(2) obligate or expend more than 60 percent of the funds authorized to be appropriated by this Act for fiscal year 2021 for the National Defense University, until 60 days after the date on which the congressional defense committees receive the report required by subsection (d).

(b) ASSESSMENT.—The Chairman of the Joint Chiefs of Staff, in consultation with the Under Secretary of Defense for Policy, the Under Secretary of Defense for Personnel and Readiness, the Principal Cyber Advisor, the Principal Information Operations Advisor of the Department of Defense, the Chief Information Officer of the Department, the Chief Financial Officer of the Department, and the Commander of United States Cyber Command, shall assess requirements for joint professional military education and civilian leader education in the information environment and cyberspace domain to support the Department and other national security institutions of the Federal Government.

(c) FURTHER ASSESSMENT, DETERMINATION, AND REVIEW.—The Under Secretary of Defense for Policy, in consultation with the Under Secretary of Defense for Personnel and Readiness, the Principal Cyber Advisor, the Principal Information Operations Advisor of the Department of Defense, the Chief Information Officer of the Department, the Chief Financial Officer of the Department, the Chairman of the Joint Chiefs of Staff, and the Commander of United States Cyber Command, shall—

(1) determine whether the importance, challenges, and complexity of the modern information environment and cyberspace domain warrant—

(A) a college at the National Defense University, a college independent of the National Defense University whose leadership is responsible to the Office of the Secretary of Defense, or an independent public or private university; and

(B) the provision of resources, services, and capacity at levels that are the same as, or decreased or enhanced in comparison to, those resources, services, and capacity in place at the College of Information and Cyberspace on January 1, 2019;

(2) review the plan proposed by the National Defense University for eliminating the College of Information and Cyberspace and reducing and restructuring the information and

cyberspace faculty, course offerings, joint professional military education and degree and certificate programs, and other services provided by the College and the effects of such changes on the military and civilian personnel requirements of the cyber workforce;

(3) assess the changes made to the College of Information and Cyberspace since January 1, 2019, and the actions necessary to reverse those changes, including relocating the College and its associated budget, faculty, staff, students, and facilities outside the National Defense University; and

(4) determine Department of Defense's overall personnel requirement for cyber and information educated military and civilian personnel.

(d) REPORT REQUIRED.—Not later than March 1, 2021, the Secretary shall present to the Committee on Armed Services of the House of Representatives and the Committee on Armed Services of the Senate a briefing, and not later than May 1, 2021, the Secretary shall submit to such committees a report, on—

(1) the findings of the Secretary with respect to the assessments, determinations, and reviews conducted under subsections (b) and (c); and

(2) such recommendations as the Secretary may have for higher education needs in the information environment and cyberspace domain.

Appendix B. Department of Defense Educational Institutions and Their Approach to Cyberspace and Information

This appendix contains an overview of each DoD educational institution that provides education at the JPME-II and equivalent graduate level. Unless otherwise noted, data on faculty and students are for AY 2021–2022 and were provided to us by the academic institutions. We provided a draft of each overview to the respective educational institution for review and comment. Where appropriate, we incorporated technical comments provided by each educational institution.

National Defense University

NDU consists of five colleges, one research institute (consisting of three small research centers), and one wargaming center. Four independent research centers also reside on the NDU campus. For our purposes, we focus on the five colleges:

- National War College
- Eisenhower School
- CIC
- CISA
- JFSC/JC2IOS.

NDU is a USCYBERCOM Academic Engagement Network Partner Institution.[1]

With limited exceptions, students admitted to a full-time degree program in any of NDU's five colleges are eligible to enroll in electives offered by another NDU college.[2] Some elective concentrations are restricted to specific colleges, and classified coursework is not available to foreign students or those who do not have the requisite security clearance. Limits may apply to the number of elective credits a student may take outside their college. For example, students eligible to enroll in CIC courses may take up to 9 credits of CIC coursework "without declaring an intent to complete a particular CIC program" ("non–program seeking status").[3]

[1] The Academic Engagement Network is designed to foster collaboration and communication between USCYBERCOM and academic institutions along four lines of effort: future cyber workforce, applied cyber research, applied analytics, and strategic issues.

[2] National Defense University Regulation 5.75, "National Defense University Electives Program," June 1, 2014, p. 8.

[3] CIC, 2021a, p. 15.

National War College

Educational Focus

The National War College is primarily oriented toward national security strategy in joint, interagency, and multinational contexts. National War College prepares students for high-level strategic leadership positions in the military and civilian agencies, focusing on the interplay between the instruments of national power and their application to achieve national security objectives.

Approach to Cyber and Information Education

Integrated into the general curriculum.

Degree Program(s) with Cyber and Information Areas of Concentration (and Enrollment)

- Master of Science in National Security Strategy, with optional Cyber Studies Concentration in AY 2021–2022 (10 students in AY 2020–2021)

The National War College master's program is offered only in residence and grants JPME-II credit for U.S. military officers.

Graduate Certificate Programs in Cyber and Information Areas (and Enrollment)

None.

Continuing Education or Short Courses in Cyber and Information Areas

None.

Other Functions Related to Cyber or Information

Faculty members with expertise in cyberspace and information write for general interest and academic publications. Faculty members also engage as guest lecturers at other institutions and DoD components.

Details of Approach to Cyber and Information Education

The National War College has integrated cyber and information topics across its curriculum to educate the entire student body in these topics. One of the seminars in the college's required National Security Strategy Practicum is a year-long cyber seminar that focuses on developing cyber strategies. Other seminars in the practicum are encouraged to include cyber as a focus area.

The core courses include 42.5 course hours covering cyber and information topics. In addition to the core courses, students take electives and conduct field studies. The year culminates in a capstone exercise. Students may choose to create an area of concentration in cyberspace, which requires taking at least two cyber electives. One cyber elective course is taught at the National War College, while the other eligible electives are taught at CIC.

The college conducts instruction in the Cyber Practicum and cyber electives at both the unclassified and classified levels.

Faculty with Domain Expertise

Four faculty members (three civilian, one military) in AY 2021–2022.

Overall Student Body

The student body consists of representatives from the Army, Navy, Air Force, Marine Corps, Space Force, Coast Guard, DoD civilians, civilians from other U.S. government departments and agencies, and 35 international fellows. The National War College conferred a total of 208 JPME-II MS degrees in AY 2020–2021.

Eisenhower School for National Security and Resource Strategy

Educational Focus

The Eisenhower School focuses on the relationship between industry and national security. Eisenhower prepares select military and civilian leaders for strategic leadership in "evaluating, marshaling, and managing resources" to execute national security strategy.[4]

Approach to Cyber and Information Education

Offers an opportunity for students to focus on cyber and information through an industry studies program (described later).

Degree Program(s) with Cyber and Information Areas of Concentration (and Enrollment)

- Master of Science in National Resource Strategy is a ten-month, 32-credit course of instruction where students complete an industry study during their second semester. The cyber and information industry concentrations and number of students in AY 2021–2022 were
  - command, control, communications, computers, intelligence, surveillance, and reconnaissance (17 students)
  - electronics (16 students)
  - networking and communication technology (17 students)
  - robotics and autonomous systems (17 students)
  - software engineering and artificial intelligence (17 students).

This program grants JPME-II credit for U.S. military officers.

[4] Eisenhower School for National Security and Resource Strategy, "Forging a New Generation of Strategic Leaders," webpage, undated.

Graduate Certificate Programs in Cyber and Information Areas (and Enrollment)

None.

Continuing Education or Short Courses in Cyber and Information Areas

None.

Other Functions Related to Cyber or Information

Eisenhower encourages its staff and faculty to attend conferences and pursue research opportunities.

Details of Approach to Cyber and Information Education

The Master of Science in National Resource Strategy program allows students, if they choose, to study cyber or information through the school's industry study courses, which occur in the second semester. An industry study focuses on a sector of the economy and is organized as a series of seminars, discussions, and site visits. The study gives students access to different organizations that contribute to the sector to give an executive-level view of the sector so that students can analyze the sectors and present a report at the end of the semester. In the first semester, the Strategic Leader Foundations course includes a cyber-focused scenario. In both semesters, Eisenhower also invites speakers from other institutions to lecture to the student body on cyber and information topics.

The college conducts instruction at the unclassified and classified levels.

Faculty with Domain Expertise

Eight faculty members (four civilian, four military) in AY 2021–2022.

Overall Student Body

The student body consists of representatives from the Army, Navy, Air Force, Marine Corps, Space Force, Coast Guard, DoD civilians, civilians from other U.S. government departments and agencies, private-sector fellows, and 40 international fellows. Eisenhower conferred a total of 282 JPME-II MS degrees in AY 2020–2021.

College of Information and Cyberspace

Educational Focus

NDU's CIC is primarily oriented toward national security strategy in the cyberspace domain and information as an "instrument of national power."[5] CIC prepares students for strategic

[5] CJCSI 1800.01F, 2020, p. A-B-9.

leadership and advisory positions that emphasize "the military, government, and private sector dimensions of information/cyberspace as a critical component of national security strategy."[6]

Approach to Cyber and Information Education

Exclusively offers graduate degree and certificate specializations in cyber and information.

Degree Program(s) with Cyber and Information Areas of Concentration (and Enrollment)

- Master of Science in Government Information Leadership (multiple concentrations, most offered in alignment with graduate certificate programs listed in the next subsection)[7]
  - 206 students enrolled in AY 2021–2022, including 49 JPME-II students enrolled in the National Security and Cyberspace Studies concentration (218 in AY 2020–2021, including 41 JPME-II students enrolled in the National Security and Cyberspace Studies concentration)

The master's program comes in two modalities: a full-time, in-residence program that grants JPME-II credit for U.S. military officers and a part-time, hybrid (online and in-residence) program that does not grant JPME-II credit.

Graduate Certificate Programs in Cyber and Information Areas (and Enrollment)

The college offers six graduate certificates: Chief Data Officer, Chief Financial Officer, Chief Information Security Officer, Cyber Leadership, Cyber Security, and IT Program Management. Total certificate program enrollment was 292 in AY 2021–2022.

Continuing Education or Short Courses in Cyber and Information Areas

CIC offers a 14-week CIO Leadership Development Program and plans to begin a 14-week Cyber Leadership Development Program in AY 2022–2023.

Other Functions Related to Cyber or Information

Faculty members write for general interest and academic publications. Faculty members also engage as guest lecturers at other institutions, DoD components, forums, and conferences. CIC also

- hosts an annual Cyber Beacon conference that "brings together experts and leaders from across the national security community, private sector, and academia to discuss the most pressing issues concerning cyberspace, information, and national security"[8]
- cohosts the annual USCYBERCOM academic symposium
- hosts an occasional chancellor's speaker series open to CIC students, faculty, and staff

---

[6] CIC, "JPME Master Degree," webpage, undated-d.

[7] "The MS Degree program is currently titled Government Information Leadership (GIL), but is in the process of being renamed to Strategic Information and Cyberspace Studies" (CIC, 2021a, p. 9).

[8] CIC, "Cyber Beacon 2021," webpage, undated-b.

- supported the congressionally mandated Cyberspace Solarium Commission by "hosting events, providing policy development input, and networking with other experts"[9]
- coordinates the University Consortium for Cybersecurity, which serves as a two-way communication channel between the Secretary of Defense and consortium members on DoD's cybersecurity strategic plans, requirements, and research, as well as academic institutions' relevant needs, expertise, and opportunities to collaborate (pursuant to Section 1659 of the NDAA for FY 2020)[10]
- leads the Cyber Professional Military Education Colloquium, which convenes PME leaders biannually to consider opportunities and challenges in cyber PME
- participates in and convenes working groups on the Joint Concept for Operating in the Information Environment in support of the Joint Warfighting Concept
- participates in the Joint Staff J-7 Analytic Research Program (The program is designed to develop repeatable processes and yield analytical products that advance strategic and operational ideas for the Joint Force Development and Design enterprise.)
- engages in capacity building with international allies and partners
- provides venues for hosting external cyber and information education events
- "maintains Memoranda of Agreement and partnerships for faculty research and information sharing with key national security and educational institutions"[11]
- participates in regular events, such as the Massachusetts Institute of Technology's Military Cyber Stability Roundtable and the Atlantic Council's Cyber 9/12 Strategy Challenge.

As of March 2022, the college had completed Phase 1 of the recertification process for designation by the National Security Agency as a Center of Academic Excellence.

Details of Approach to Cyber and Information Education

CIC's programs are designed to directly support the objectives of strategic guidance and stakeholders' requirements. The college's master's program focuses on cyber and information education in strategic and joint contexts. In addition to requirements established through the OPMEP and the Chairman's Special Areas of Emphasis, the curriculum is primarily informed by the needs of the DoD CIO; other stakeholders, such as USCYBERCOM and Congress; and DoDD 8140.01, *Cyberspace Workforce Management*.

The Master of Science JPME-II curriculum has nine core courses: Strategic Leader Foundational Course; Strategic Thinking and Communication; International Challenges in Cyberspace; Foundations of the Information Environment; Strategic Competition in the Information Environment; National Security Strategy; Cyberlaw; Information, Warfare and

[9] CIC, "US Cyberspace Solarium Commission," webpage, undated-e.

[10] Pub. L. 116-92, National Defense Authorization Act for Fiscal Year 2020, December 20, 2019.

[11] CIC, "Memorandum for Joint Staff J-7: College of Information and Cyberspace 2021 Academic Programs," National Defense University, January 2, 2021b, p. 2.

Military Strategy; and Warfighting and Disruptive Technologies.[12] In addition to the 30-credit core, JPME-II students take three electives (six credits total) that can be selected from CIC's elective offerings and from electives offered by other NDU colleges.

The college conducts instruction at the unclassified and classified levels.

Faculty with Domain Expertise

Thirty full-time faculty members (22 civilian, eight military), three part-time expert consultants, and eight faculty vacancies as of May 11, 2022.

Overall Student Body

The AY 2021–2022 student body consisted of representatives from the Army, Navy, Air Force, Marine Corps, Coast Guard, DoD civilians, civilians from other U.S. government departments and agencies, 20 international fellows, and two private-sector civilians. CIC conferred a total of 117 degrees and 80 certificates in AY 2020–2021 (including JPME-II Master's and non-JPME-II master's degrees). Total student enrollment was 376 in AY 2020–2021 (including JPME-II master's, non-JPME-II master's, and certificate programs), reflecting decreased enrollment stemming from prior plans to close the college. Enrollment for AY 2021–2022 was 498 students.

College of International Security Affairs

Educational Focus

CISA focuses on educating and developing partner capacity in combating terrorism and irregular warfare. CISA's primary focus is the Regional Defense Fellowship Program—administered and financially supported by the Office of the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict and Interdependent Capabilities—which educates international students in geopolitical environments, ideological movements, challenges to national and international security, understanding terrorism, and strategy development and design thinking of coalition building.[13]

Approach to Cyber and Information Education

CISA integrates cyber and information into its general curriculum. CISA has a ten-month Master of Arts in Strategic Security Studies with three phases and two programs. The Regional Defense Fellowship Program at Ft. McNair focuses on irregular warfare in its global and local contexts and the Joint Special Operations Master of Arts Program at Ft. Bragg that offers a

[12] The curriculum of the part-time, online version of the master's program is closely aligned and meets the same learning outcomes as the resident, JPME-II program. However, students do not earn JPME-II credit.

[13] Memorandum of Agreement Between the Office of the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict (OASD[SO/LIC&IC]) and the National Defense University, December 20, 2010.

strategic-level perspective on the global threat environment, also focusing on irregular warfare. The Regional Defense Fellowship Program at Ft. McNair grants JPME-II credit for U.S. military officers.

Degree Program(s) with Cyber and Information Areas of Concentration (and Enrollment)

None.

Graduate Certificate Programs in Cyber and Information Areas (and Enrollment)

None.

Continuing Education or Short Courses in Cyber and Information Areas

CISA faculty travel to educate partner countries on irregular warfare approximately three times per year, accompanied by a CIC professor and/or including information subject matter in about one-half of the visits. CISA participates in an annual NDU international alumni event, alongside CIC.

Other Functions Related to Cyber or Information

CISA faculty provide input into DoD policy on irregular warfare. Faculty members write and publish for DoD, general interest, and academic publications.

Details of Approach to Cyber and Information Education

CISA emphasizes the information environment rather than the cyber domain. This is done through the seminars and contextualized through the frame of irregular warfare. Information concepts are presented to students as case studies and simulations and gaming exercise.

The college presently conducts instruction at the unclassified level but is working with NDU to expand into classified instruction for U.S. military and interagency students per future guidance.

Faculty with Domain Expertise

Five faculty members in AY 2021–2022.

Overall Student Body

CISA has a combination of officers, enlisted, and civilian students from across the Army, Navy, Marine Corps, Air Force, Coast Guard, interagency, and partnered militaries (35 international students in AY 2020–2021). CISA conferred a total of 337 degrees and certificates in AY 2020–2021 (including 55 JPME-II master's degrees, 54 non-JPME-II master's degrees, and 228 certificates).

Joint Forces Staff College/Joint Command, Control, and Information Operations Center

Educational Focus

JFSC is primarily oriented toward joint, multinational, and interagency operations as they concern the national security, defense, and military strategies. Within JFSC, the JC2IOS focuses on cyber and information education.

Approach to Cyber and Information Education

JFSC offers cyber and information education through JC2IOS, which provides short courses (one to two weeks) designed to train and educate practitioners in the application of cyber and information in support of joint force requirements.

Degree Program(s) with Cyber and Information Areas of Concentration and Enrollment

None.

Graduate certificate programs and enrollment

None.

Continuing Education or Short Courses Available

- The Joint Command, Control, Communications, Computers and Intelligence/Cyber Staff and Operations Course is a three-week, in-residence or mobile training team (MTT) course designed to provide a broad overview of service command, control, communications, computers, and intelligence and cyber capabilities and trains students from varied functional backgrounds to operate in joint operational–level billets. Emphasis is balanced between the operational constructs associated with the command and control process and the management and operation of current joint command, control, communications, computers, and intelligence and cyber systems.
- The Joint Information Operations Orientation Course is a four-week, online course designed to provide the foundations on which to develop practical IO skills and the ability to integrate and synchronize information-related capabilities within an IO cell in support of an operational-level joint planning group.
- The Joint Information Operations Planner's Course is a four-week, in-residence and distance-learning, MTT course designed to train students to "plan, integrate, and synchronize IO into joint operational-level plans and orders."[14] The course is taught at the Top Secret/Sensitive Compartmentalized Information (TS/SCI) level and focuses on IO orientation, information environment, IO planning, OPSEC planning, MILDEC planning, and information-related capabilities synchronization. Students must attend the Joint Information Operations Orientation Course as a prerequisite.

[14] JFSC, "Joint Information Operations Planners' Course (JIOPC)," webpage, February 4, 2021a.

- The Joint Military Deception Training Course is a two-week, in-residence or MTT course designed to train students to "plan, integrate, and synchronize MILDEC into joint operational-level plans and orders."[15]
- The Defense Operations Security Planners Course is a one-week, in-residence or MTT course designed to train students to effectively use the OPSEC process to "plan, integrate, conduct, and assess Joint OPSEC at the joint/operational level, across the range of military operations, in accordance with applicable doctrine, policy, and authorities."[16]

In AY 2021–2022, a total of 544 students attended JC2IOS classes. JC2IOS courses do not grant JPME-II credit but do provide joint certification for MILDEC and IO practitioners.

Other Functions Related to Cyber or Information

None.

Details of Approach to Cyber and Information Education

As just detailed, JC2IOS provides short courses and certificate programs to students. The train the trainer methodology is utilized when providing short courses to supported commands. Students write papers and conduct practical exercises based on information-related case studies and scenarios to reinforce course learning objectives.

The college conducts instruction at the unclassified and classified levels.

Faculty with Domain Expertise

As of April 28, 2022, JC2IOS had eight faculty members (two civilian, six military).

Overall Student Body

JC2IOS has a combination of officers, enlisted, and civilian students from across the Army, Navy, Marine Corps, Air Force, Space Force, interagency, and partner militaries. The host college, JFSC, conferred a total of 987 degrees and certificates in AY 2020–2021 (including 43 JPME-II MS degrees and 944 JPME-II certificates).

Air University

Air University provides education across the officer, enlisted, and civilian workforce and includes components dedicated to research, doctrine, and training in addition to education. There are three educational institutions relevant to the focus of this report: the AFIT at Wright-Patterson Air Force Base and the Air War College and AFCC at Maxwell Air Force Base.

[15] JFSC, "Joint MILDEC Training Course (JMTC)," webpage, March 31, 2021b.

[16] JFSC, "Defense Operations Security Planners Course (DOPC)," webpage, July 20, 2022.

Air Force Institute of Technology

Educational Focus

AFIT focuses on preparing students to develop innovative solutions for the deterrence and warfighting missions of the Air Force and Space Force. AFIT has four schools. The Graduate School of Engineering and Management offers certificates, master's degrees and doctorates. The Civil Engineer School, School of Strategic Force Studies, and the School of Systems and Logistics provide continuing education for cyber and information education.

Approach to Cyber and Information Education

AFIT offers specialized degrees in cyber and information.

Degree Program(s) with Cyber and Information Areas of Concentration and Enrollment

The Graduate School of Engineering and Management offers master's degrees and doctorates in six departments. Cyber and information courses are available to all students in the graduate school. The following lists the departments and the numbers of programs they offer:

- Aeronautics and Astronautics (four)
- Electrical and Computer Engineering (four, including a master's in Cyber Operations)
- Engineering Physics (six)
- Mathematics and Statistics (one)
- Operational Sciences (six)
- Systems Engineering and Management (seven).

In AY 2020–2021, 180 AFIT degree or certificate graduates took at least three cyber or information courses, which we consider as representing a specialized degree or certificate in these fields because the base engineering and management content of all these programs is also relevant to cyber and information domains. AFIT does not provide JPME-II credit.

Graduate Certificate Programs and Enrollment

The Graduate School of Engineering and Management offers certificates in five departments. The following lists the departments and the numbers of programs they offer:

- Aeronautics and Astronautics (two)
- Electrical and Computer Engineering (three)
- Engineering Physics (two)
- Operational Sciences (seven)
- Systems Engineering and Management (two).

Continuing Education or Short Courses Available

The Civil Engineer School, School of Strategic Force Studies, and School of Systems and Logistics each provide continuing education opportunities in cyberspace. The Civil Engineer School has integrated cyberspace subject-matter experts into ten courses, including those focused

on installation cybersecurity, and provides hands-on technical training. The School of Strategic Force Studies offers courses tailored to cyberspace and information warfare career field education requirements that educate students in the application of offensive and defensive cyberspace operations and information network operations. The School of Systems and Logistics offers courses in cyber and intelligence, primarily for the acquisition, sustainment, and logistics communities, including joint and industry partners. These courses focus on air and space systems.

Other Functions Related to Cyber or Information

AFIT has a research center and a center of excellence dedicated to cyber. The Center for Cyberspace Research is a research center that has focus areas in human factors of cyber weapons, cyber in multidomain operations, advanced networking and security, the radio frequency and physical layer, reverse engineering and cyber defense, and cyber physical and embedded systems.[17] The Air Force's Cyberspace Technical Center of Excellence (CyTCoE) focuses on offensive and defensive cyber operations, cybersecurity, and resiliency in weapon systems.[18]

AFIT holds the National Security Agency Center of Academic Excellence designation in Cyber Defense Research and is designated the Air Force CyTCoE by the Chief of Staff of the Air Force and the Secretary of the Air Force.[19]

Details of Approach to Cyber and Information Education

Master's degree and doctorate programs span a range of technical fields, many of which are related to cyber and information topics. Graduate students in every program have access to cyber and information courses. A maximum of 12 quarter hours earned through certificate courses may be transferred toward a degree.

The college conducts instruction at the unclassified and classified levels.

Faculty with Domain Expertise

As of May 6, 2022, a total of 39 faculty members had domain expertise in cyber and information. Of the 39, 15 are DoD military officers, 22 are DoD civilians, and two are

---

[17] AFIT, "Center for Cyberspace Research (CCR)," webpage, undated.

[18] AFIT, "Air Force Cyberspace Technical Center of Excellence," webpage, undated.

[19] The Air Force CyTCoE is designed to address the technical workforce development requirements driven by the continuously evolving cybersecurity challenges and rapid technological change, as highlighted in the National Defense Strategy. Air Force CyTCoE resources are allocated to facilitate and support cyber education and research efforts throughout all four AFIT schools and to provide a central point for external partnership requirements. In addition to the creation and sustainment of a dedicated research network, called the Cyber Defense Network, the Air Force CyTCoE maintains a robust software development capability focusing on agile and DevSecOps methodologies through its Innovative Solutions Team and the Rapid Development Team, which tailors unique cyber education curriculum for external partners lacking cyber expertise.

contractors. Additionally, the remaining continuing education schools have 18 instructors with cyber domain expertise.

Overall Student Body

For AY 2020–2021, AFIT conferred 562 graduate degrees or certificates. In addition, AFIT enrolled about 22,000 students in short courses and continuing education.

Air Force Cyber College

NOTE: After completion of the research for this report, AFCC ceased its graduate programs, starting with AY 2022–2023. We elected to keep the information on the college in the report for completeness.

Educational Focus

AFCC focuses on preparing airmen to be strategists in offensive and defensive cyberspace operations and information warfare. AFCC helps meet the challenges of creating and sustaining strategic thinkers in the cyber and information workforce and increased awareness in the total workforce, arming airmen to counter the adversary use of cyber and information for strategic competition.

Approach to Cyber and Information Education

AFCC offers specific classes in cyber and information warfare.

Degree Program(s) with Cyber and Information Areas of Concentration and Enrollment

None.

AFCC has developed a master's curriculum in cyber strategy, which focuses on the topics of leadership, strategy, influence and partnerships, operations, emerging technologies, law, and policy in the cyber and information realms. As of July 2022, the master's program was unfunded and had been put on hold indefinitely.

Graduate Certificate Programs and Enrollment

AFCC offers a graduate Cyber Leadership Certificate sponsored by the National Security Agency's National Cryptologic School. The certificate program, launched in January 2022, requires three 14-week online courses and is the first of three certificates in the proposed Cyber Strategy Master of Arts curriculum.

Continuing Education or Short Courses Available

AFCC offers continuing education through three courses: Functional Mission Analysis—Cyber (virtually, primarily for members of Mission Defense Teams), Senior Executive Cyber Threats, Operations, Risk & Strategy (SECTORS), and Cyber for Aviation.

The Senior Executive Cyber Threats, Operations, Risk & Strategy and Cyber for Aviation courses can be delivered by the AFCC Mobile Education Team on a limited basis, to educate U.S. airmen of all backgrounds on cyber operations and how to employ and integrate cyber into joint all-domain operations.

Other Functions Related to Cyber or Information

Faculty members with expertise in cyberspace and information warfare conduct research and write for general interest and academic publications. AFCC conducts several functions related to cyber or information. Cyber LITE is a strategic competition course cosponsored with the Air Force Culture and Language Center. AFCC hosts a biweekly Virtual Cyber Seminar in which presentations from public and private sector experts on cyber and information warfare topics are made to a wide audience. AFCC publishes a cyber case study series, designed to provide educators with materials for teaching various cyber topics (e.g., policy, law, strategy).

AFCC is a USCYBERCOM Academic Engagement Network Partner Institution.

Details of Approach to Cyber and Information Education

Seven AFCC graduate courses are available as electives to Air War College and Air Command and Staff College students, although course availability will be limited beginning with AY 2022–2023 and a 70 percent drawdown of the AFCC faculty.

The college conducts instruction at the unclassified and classified levels.

Faculty with Domain Expertise

There were 14 faculty members (11 civilian, three military) as of May 12, 2022. Beginning July 1, 2022, the AFCC drawdown is projected to reduce these numbers to four faculty members (three civilian, one military).

Overall Student Body

During AY 2021–2022, a total of 39 students were enrolled in the graduate electives; 14 students in the Leadership Certificate; and 2,169 students in continuing education courses.

Air War College

Educational Focus

Air War College is primarily oriented toward military strategy in the air, space, and cyberspace domains. Air War College prepares students for strategic leadership positions in military and civilian agencies at the joint, interagency, and international levels.

Approach to Cyber and Information Education

Air War College integrates cyber and information into the general curriculum. The Master of Strategic Studies is a 35-credit course with the option for a grand strategy concentration or a joint warrior seminar. This program grants JPME-II credit for U.S. military officers.

Degree Program(s) with Cyber and Information Areas of Concentration and Enrollment

None.

Graduate Certificate Programs and Enrollment

None.

Continuing Education or Short Courses Available

None.

Other Functions Related to Cyber or Information

Air War College has a Cyber Research Task Force, which is run in conjunction with Air Staff and Command College and taught by AFCC. Beginning in AY 2023, the Air War College plans to separate its Research Task Force from ACSC and focus on the broader realm of information warfare.

Air War College is a USCYBERCOM Academic Engagement Network Partner Institution through its subordinate unit, the AFCC.

Details of Approach to Cyber and Information Education

For specific cyber courses, students can take cyber electives at AFCC, though the offerings are expected to be significantly reduced due to the AFCC drawdown.

The college conducts instruction at the unclassified and classified levels.

Faculty with Domain Expertise

Air University has a Cyber Chair position that works for the Air War College and provides cyber and information expertise and serves as the Air War College's liaison to other subject matter experts.

Overall Student Body

The AY 2021–2022 student body consisted of representatives from the Army, Navy, Air Force, Marine Corps, Space Force, Coast Guard, DoD civilians, civilians from other U.S. government departments and agencies, and 47 international fellows. Air War College conferred a total of 211 degrees and certificates in AY 2020–2021 (including 183 JPME-II or non-JPME-II master's degrees and 28 graduate certificates).

Army War College

Educational Focus

USAWC is primarily oriented toward the role of ground forces in national security. USAWC prepares students for strategic leadership in the development and application of land power through education "in the theory and practice of strategy, operations, national security, and resource management" and the principles of command.[20]

Broad Approach to Cyber and Information Education

These are integrated into the general curriculum; USAWC offers a degree program area of concentration.

Degree Program(s) with Cyber and Information Areas of Concentration (and Enrollment)

- Master of Strategic Studies, with a concentration in Strategic Cyberspace Studies
  - 13 students enrolled in AY 2021–2022

The master's program comes in two modalities: a full-time, in-residence program that grants JPME-II credit for U.S. military officers and a part-time, hybrid (online and in-residence) program with JPME-I and limited JPME-II options.

Graduate Certificate Programs in Cyber and Information Areas (and Enrollment)

None.

Continuing Education or Short Courses in Cyber and Information Areas

The college's U.S. Army Heritage and Education Center presents lectures on cyber war for students, faculty, and guests.

Other Functions Related to Cyber or Information

Faculty members write for general interest and academic publications and for standalone publications, such as the *Strategic Cyberspace Operations Guide*.[21] Faculty members also engage as guest lecturers at other institutions, DoD components, forums, and conferences. The USAWC Center for Strategic Leadership's Strategic Landpower and Futures Group conducts symposia "concerned with the application of strategic Cyberspace to national defense and military operations."[22]

USAWC is a USCYBERCOM Academic Engagement Network Partner Institution.

---

[20] USAWC, "Military Education Level 1 Programs," webpage, undated-a.

[21] USAWC, *Strategic Cyberspace Operations Guide*, August 1, 2021.

[22] USAWC, "Mission Command and Cyber Division (MCCD)," webpage, undated-b.

Details of Approach to Cyber and Information Education

In addition to the core coursework, students pursuing the Strategic Cyberspace Studies area of concentration must complete a cyber-related strategy research project and three of the following cyberspace electives:

- Cyberspace Issues: Fundamentals and Strategy (unclassified)
- Cyberspace Effects in Multi-Domain Operations (classified)
- National Cyberspace Issues (classified)
- Cybersecurity Law and Policy (unclassified).

Students may also participate in cyber-focused fellowships at Carnegie Mellon University, University of Pittsburgh, and the National Security Agency.

The college conducts instruction at the unclassified and classified levels.

Faculty with Domain Expertise

There were nine full-time faculty members (five civilian, four military) and three part-time faculty members (two civilian, one military) as of May 3, 2022.

Overall Student Body

The AY 2021–2022 student body consisted of representatives from the Army, Navy, Air Force, Marine Corps, Space Force, Coast Guard, DoD civilians, civilians from other U.S. government departments and agencies, and 80 international fellows. USAWC conferred a total of 1,269 degrees and certificates in AY 2020–2021 (including 751 JPME-II or non-JPME-II master's degrees and 518 graduate certificates).

Marine Corps University

Educational Focus

MCU is primarily oriented toward littoral military strategy and operations. Within MCU, the Marine Corps War College (MCWAR) develops senior military and civilian leaders who "complement competence in national defense matters with an understanding of the political, economic, social, and informational environments, which influence the formulation of national strategy."[23] The School of Advanced Warfighting (SAW) focuses on operational art, "[w]hat military organizations do to win campaigns," and operational planning, "[h]ow military organizations prepare for war."[24]

[23] MCU, *AY 2020–2021 Catalog*, 2020a, p. 7.

[24] MCU, "USMC School of Advanced Warfighting, Academic Year 2019–2020," briefing, 2020b, p. 3.

Approach to Cyber and Information Education

Integrated into the general curriculum. MCWAR grants the Master of Strategic Studies degree, and awards JPME-II credit to U.S. military officers. SAW grants the Master of Operational Studies but does not award JPME-II credit.

Degree Program(s) with Cyber and Information Areas of Concentration (and Enrollment)

None.

Graduate Certificate Programs in Cyber and Information Areas (and Enrollment)

None.

Continuing Education or Short Courses in Cyber and Information Areas

Marine Corps University offers continuing education and short courses on campus, online, and through MTTs. Some of these courses include cyber and information topics in civil-military operations, cyberspace operations, and IO and last from five hours to 60 days.

Other Functions Related to Cyber or Information

Faculty members with expertise in cyberspace and information write for general interest and academic publications. Faculty members also engage as guest lecturers at other institutions and DoD components. SAW Professor Benjamin Jensen was a lead author of the Cyberspace Solarium Commission report.[25]

Details of Approach to Cyber and Information Education

Cyber and information education is incorporated in MCWAR's core curriculum and wargames and in the SAW curriculum through exercises, operational decision games, and seminars.[26] MCWAR students visit combatant commands, including USCYBERCOM.

MCWAR and SAW conduct instruction at the unclassified level.

Faculty with Domain Expertise

There were four faculty members as of May 2, 2022.

Overall Student Body

The AY 2020–2021 MCWAR student body totaled 32 students, consisting of representatives from the Army, Navy, Air Force, Marine Corps, Coast Guard, DoD civilians, civilians from other U.S. government departments and agencies, and four international officers. The AY 2020–2021 SAW student body totaled 26 students, consisting of representatives from the Army, Navy,

[25] U.S. Cyberspace Solarium Commission, 2020.

[26] Discussion with Marine Corps University faculty, November 19, 2021.

Air Force, Marine Corps, Coast Guard, and three international officers. MCWAR and SAW conferred a combined total of 57 JPME-II master's degrees in AY 2020–2021.

Naval Postgraduate School

Educational Focus

NPS is primarily oriented toward national defense in the maritime domain, focusing on technological leadership and applied research. NPS degree programs are technical, with instruction on subject matter, methods and technical skills, critical thinking, communication skills, and defense relevance.[27]

Approach to Cyber and Information Education

NPS offers degree and certificate specializations in cyber and information education.

Degree Program(s) with Cyber and Information Areas of Concentration (and Enrollment)

NPS offers a number of degree programs with cyber and information specializations, and awarded degrees to 282 students in AY 2020–2021.

The school awarded 282 master's degrees in the following areas (with numbers):

- Applied Cyber Operations (4 students in AY 2020–2021)
- Combat Systems Technology (1)
- Cyber Systems and Operations (6)
- Defense Analysis (Information Operations) (2)
- Information Operations (0)
- Information Strategy and Political Warfare (10)
- Information Technology Management (13)
- Information Warfare Systems Engineering (11)
- Network Operations and Technology (18)
- Software Engineering (0)
- Space Systems Operations (19)
- Systems Engineering (99)
- Systems Engineering Analysis (1)
- Systems Engineering Management (73)
- Systems Technology (Command, Control, and Communications) (3)
- Master of Systems Analysis (22).

[27] NPS, "Institutional Learning Objectives," webpage, undated.

The school also awarded six doctorates in AY 2020–2021 to students who had also received master's degrees:

- Information Sciences (5)
- Systems Engineering (1).

NPS does not grant JPME-II credit.

Graduate Certificate Programs in Cyber and Information Areas (and Enrollment)

NPS offers 18 graduate certificate programs in cyber and information: Chief Information Officer (CIO) Management; Combat Systems Science and Engineering; Cyber Security Adversarial Techniques; Cyber Security Defense; Cyber Security Fundamentals; Cyber Systems; Cyber Warfare; Electronic Warfare Engineer; Information Systems Security Engineering; Mathematics of Secure Communication; Signal Processing; Space Control Tactics & Operations; Space Nuclear Command, Control & Communications; Space Systems; Space Systems Design; Space Systems Fundamentals; Systems Analysis; and Systems Engineering. NPS awarded certificates to 188 students in AY 2020–2021.

Continuing Education or Short Courses in Cyber and Information Areas

NPS offers short courses, ranging in duration from one day to two months, to mid- and senior-grade professionals. Short courses are not for academic credit, but some award continuing education units. During FY 2020 and FY 2021, NPS delivered 21 cyber and information short courses to 2,424 professionals.

Other Functions Related to Cyber or Information

Faculty members write for general interest and academic publications. Faculty members engage as guest lecturers at other institutions, DoD components, forums, and conferences. Faculty are also available to create short courses to meet on-demand Navy and DoD needs. NPS also

- supports faculty and student research through classified studies and interdisciplinary research through its Cybersecurity Operations Center
- promotes and reimburses research through its Cyber Academic Group
- convenes researchers and students, organizes occasional events, and publishes commentary through the DoD Information Strategy Research Center
- hosts competitions and experiments at its Cyber Battle Lab.

NPS holds the following National Security Agency designations:

- National Center of Academic Excellence in Cyber Defense Education
- National Center of Academic Excellence in Cyber Defense Research
- National Center of Academic Excellence in Cyber Operations.

NPS is a USCYBERCOM Academic Engagement Network Partner Institution.

Details of Approach to Cyber and Information Education

Curricula vary by degree and typically include completion of a degree-specific sequence of core courses, a set of electives chosen by the student, and a thesis or capstone project.[28] All NPS master's degrees require completion of at least 32 graduate-level quarter credits. Master's degree programs in cyber and information education last from 15 to 24 months.

NPS conducts instruction at the unclassified and classified levels.

Faculty with Domain Expertise

As of May 11, 2022, there were 70 full-time (62 civilian, eight military) and seven part-time civilian faculty members.

Overall Student Body

The AY 2021–2022 student body consists of representatives from the Army, Navy, Air Force, Marine Corps, Coast Guard, DoD civilians, civilians from other U.S. government departments and agencies, international fellows, and private sector civilians. NPS conferred a total of 2,733 degrees and certificates in AY 2020–2021 (including doctorates, non-JPME-II master's, and graduate certificates).

Naval War College

Educational Focus

The Naval War College is primarily oriented toward military strategy in the maritime domain. Within the Naval War College, the College of Naval Warfare's National Security and Strategic Studies program prepares students for strategic leadership positions and "emphasizes the theory and practice of operational art in terms of maritime and joint forces."[29]

Approach to Cyber and Information Education

Integrated into the general curriculum, with several electives focused on cyber and information. The Naval War College's College of Naval Warfare grants the Master of Arts in National Security and Strategic Studies and awards JPME-II credit to U.S. military officers. The Naval Command College offers an equivalent course of study to senior international officers.

Degree Program(s) with Cyber and Information Areas of Concentration (and Enrollment)

None.

---

[28] NPS, "Degree-Specific Requirements," webpage, November 23, 2021.

[29] U.S. Naval War College, "College of Naval Warfare Core Curriculum," website, undated-a.

Graduate Certificate Programs in Cyber and Information Areas (and Enrollment)

None.

Continuing Education or Short Courses in Cyber and Information Areas

The Naval War College's College of Maritime Operational Warfare offers intermediate- and senior-level PME short courses, all of which include cyber and/or information content.

Other Functions Related to Cyber or Information

Faculty members with expertise in cyberspace and information write for general interest and academic publications. Faculty members also engage as guest lecturers at other institutions and DoD components. The Cyber and Innovation Policy Institute is the Naval War College's "hub for cyber operations and strategy research . . . to help senior leaders advance cybersecurity and innovation policy."[30] The institute's activities include research, gaming, teaching, and outreach.

The Naval War College is a USCYBERCOM Academic Engagement Network Partner Institution.

Details of Approach to Cyber and Information Education

Three College of Naval Warfare core courses—Joint Military Operations, Strategy and Policy, and National Security Decision Making—dedicate course sessions to cyber and/or information education. The Naval War College offers several electives focused on cyber and/or information, including Strategic Communications & Information Operations; Military Deception; Cyber Seas; the Law of Air, Space, and Cyber Operations; and Cyber Security.

Core Naval War College courses are taught at the unclassified level, but certain operational-level electives, wargaming, research, and education are conducted at the classified level.

Faculty with Domain Expertise

As of April 28, 2022, there were 14 current faculty members (12 civilian, one military, one contractor).

Overall Student Body

The student body consists of representatives from the Army, Navy, Air Force, Marine Corps, Space Force, Coast Guard, DoD civilians, civilians from other U.S. government departments and agencies, and 49 international officers. The College of Naval Warfare and Naval Command College conferred a total of 206 degrees and certificates in AY 2020–2021 (including JPME-II master's and equivalent degrees for international officers).

[30] U.S. Naval War College, "Cyber & Innovation Policy Institute," webpage, undated-b.

National Intelligence University

Educational Focus

NIU focuses on providing an education in strategic intelligence topics to TS/SCI cleared U.S. government professionals. NIU is the sole accredited, degree-granting institution in the intelligence community. NIU focuses on developing strategic leaders with the "analytical skills and competencies of intelligence analysis."[31]

Approach to Cyber and Information Education

Cyber and information education is integrated into the general curriculum. NIU offers a degree program area of concentration and graduate certificates in cyber and information education.

Degree Program(s) with Cyber and Information Areas of Concentration (and Enrollment)

- Master of Science and Technology Intelligence, with a concentration in Cyber Intelligence (23 students enrolled in AY 2022–2023) or a concentration in Information and Influence Intelligence (nine students enrolled in AY 2022–2023).[32]

NIU does not grant JPME-II credit.

Graduate Certificate Programs in Cyber and Information Areas (and Enrollment)

NIU offers a graduate Certificate in Intelligence Studies (CIS) that has two cyber and information-related focuses (called *topics* in NIU): Eight students were admitted to the AY 2021–2022 Cyber Intelligence CIS topic, and two students were admitted to the AY 2021–2022 Information and Influence Intelligence CIS topic.

Continuing Education or Short Courses in Cyber and Information Areas

Although NIU offers continuing education at its main campus, five regional academic centers, and a network of secure video teleconferencing sites, continuing education in cyber and information is currently offered only at the main campus. Continuing education students must hold an active security clearance and be able to attend at one of the listed sites.

Other Functions Related to Cyber or Information

Faculty members with expertise in cyberspace and information conduct applied research with U.S. government entities, write for general interest and academic publications, and write classified research. NIU also engages with other institutions (e.g., National Academy of

[31] National Intelligence University, "About NIU," webpage, undated-a.

[32] AY 2021–2022 enrollment numbers were not reported by concentration. The concentration numbers represent approximately 25 to 50 percent of the total enrollment in courses specific to each concentration.

Sciences, Office of the Director of National Intelligence, College of William and Mary) through conferences and speaking engagement.

Details of Approach to Cyber and Information Education

NIU uses a problem-based learning model and integrates aspects of cyber and information into its curriculum to educate the entire student body in these topics. In addition to core coursework in strategic intelligence, the optional Master of Science and Technology Intelligence areas of concentration in Cyber Intelligence or Information and Influence Intelligence require completing four courses (12 credits) in the desired concentration and conducting a capstone exercise or concentration-related thesis. Students are not required to take a concentration. Students enrolled in the Master of Science of Strategic Intelligence program can also take information and cyber courses.

Other degree concentrations and certificates (e.g., counterintelligence, China) require some in-depth study of cyber and information topics through the specific lens of the concentration.

NIU conducts a substantial degree of teaching and research at the classified level,[33] and all students must hold an active TS/SCI clearance. As a result, NIU students can conduct study on cyber and information relatively uninhibited by classification concerns.

Faculty with Domain Expertise

There were eight full-time faculty members as of June 16, 2022, with two information faculty positions advertised for hire.

Overall Student Body

The AY 2021–2022 student body consists of representatives from the Army, Navy, Air Force, Marine Corps, Coast Guard, DoD civilians, and civilians from other U.S. government departments and agencies, such as the Federal Bureau of Investigation, Department of Homeland Security, and Department of Commerce. NIU only admits U.S. citizens that are members of the U.S. armed forces or federal government employees. Total graduate student enrollment was 768 in AY 2021–2022 (including master's degree and certificate programs). In contrast with the DoD institutions we reviewed, NIU also offers some undergraduate programs and enrolls enlisted military members.

[33] National Intelligence University, *Catalog for Academic Year 2021–22*, 2021, p. 10.

Abbreviations

AFCC	Air Force Cyber College
AFIT	Air Force Institute of Technology
ASD(C3I)	Assistant Secretary of Defense for Command, Control, Communications, and Intelligence
AY	academic year
CFO	chief financial officer
CIC	College of Information and Cyberspace
CIO	chief information officer
CIS	Certificate in Intelligence Studies
CISA	College of International Security Affairs
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CyTCoE	Cyberspace Technical Center of Excellence
DCWF	Defense Cyberspace Workforce Framework
DJ-7	Director for Joint Force Development
DoD	U.S. Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
FY	fiscal year
GS	General Schedule
IO	information operations
IRMC	Information Resources Management College
IT	information technology
JC2IOS	Joint Command, Control, and Information Operations School
JFSC	Joint Forces Staff College
JPME	Joint Professional Military Education

JPME-I	Joint Professional Military Education Phase I
JPME-II	Joint Professional Military Education Phase II
MCU	Marine Corps University
MCWAR	Marine Corps War College
MECC	Military Education Coordination Council
MILDEC	military deception
MTT	mobile training team
NDAA	National Defense Authorization Act
NDU	National Defense University
NIU	National Intelligence University
NPS	Naval Postgraduate School
OBME	outcomes-based military education
OIE	operations in the information environment
OPMEP	Officer Professional Military Education Policy
OASD(SO/LIC)	Office of the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict
OSD	Office of the Secretary of Defense
PME	professional military education
RFI	request for information
SAW	School of Advanced Warfighting
TS/SCI	Top Secret/Sensitive Compartmentalized Information
USAWC	U.S. Army War College
U.S.C.	U.S. Code
USCYBERCOM	U.S. Cyber Command
USD(C)	Under Secretary of Defense Comptroller
USD(P)	Under Secretary of Defense for Policy
USD(P&R)	Under Secretary of Defense for Personnel and Readiness

References

10 U.S.C.—*See* U.S. Code, Title 10.

50 U.S.C.—*See* U.S. Code, Title 50.

AFIT—*See* Air Force Institute of Technology.

Air Force Institute of Technology, "Center for Cyberspace Research (CCR)," webpage, undated. AGSs of March 25, 2022: https://www.afit.edu/CCR/

Air Force Institute of Technology, "Air Force Cyberspace Technical Center of Excellence," webpage, undated. As of March 25, 2022: https://www.afit.edu/CYBER/

Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, "Department of Defense Chief Information Officer (CIO) Certificate Program," memorandum, February 28, 1997.

Belding, Greg, "Introduction to the DOD Cyber Workforce Framework (DCWF)," webpage, Infosec, October 26, 2020. As of July 10, 2022: https://resources.infosecinstitute.com/topic/introduction-to-the-dod-cyber-workforce-framework-dcwf/

Brenner, Alfred E., J. Katherine Burton, and Paul K. Ketrick, *Future Options for the National Defense University (NDU) iCollege*, NS D-4438, Institute for Defense Analyses, May 2012.

Burgess, Matt, "Ukraine's Volunteer 'IT Army' Is Hacking in Uncharted Territory," *Wired*, February 27, 2022.

Chairman of the Joint Chiefs of Staff Instruction 1800.01F, *Officer Professional Military Education Policy*, May 15, 2020.

CIC—*See* College of Information and Cyberspace.

CJCSI—*See* Chairman of the Joint Chiefs of Staff Instruction.

College of Information and Cyberspace, "CIC Overview," webpage, undated-a. As of June 17, 2022: https://cic.ndu.edu/About/Mission-Vision/

College of Information and Cyberspace, "Cyber Beacon 2021: The Impacts of a Global Pandemic," webpage, undated-b. As of February 14, 2022: https://cic.ndu.edu/Events/Cyber-Beacon/Cyber-Beacon-2021/

College of Information and Cyberspace, "Cyber PME Colloquium," webpage, undated-c. As of June 30, 2022:
https://cic.ndu.edu/Events/Cyber-PME-Colloquium/

College of Information and Cyberspace, "JPME Master Degree," webpage, undated-d. As of June 9, 2022:
https://cic.ndu.edu/Academics/JPME-Master-Degree/

College of Information and Cyberspace, "US Cyberspace Solarium Commission," webpage, undated-e. As of February 14, 2022:
https://cic.ndu.edu/Events/Solarium-Commission/

College of Information and Cyberspace, *Self Study Report for PAJE Accreditation*," 2019.

College of Information and Cyberspace, *Academic Catalog AY 2021–2022*, National Defense University, 2021a.

College of Information and Cyberspace, "Memorandum for Joint Staff J-7: College of Information and Cyberspace 2021 Academic Programs," National Defense University, January 2, 2021b.

College of Information and Cyberspace, "Fact Sheet," May 2022. As of October 20, 2022:
https://cic.ndu.edu/About/Fact-Sheet/

Computer Security Resource Center, "Hash Function," webpage, undated. As of July 9, 2022:
https://csrc.nist.gov/glossary/term/hash_function

Defense Information Systems Agency, "Director," website, undated.

Demus, Alyssa, and Christopher Paul, "Don't Sleep on Russian Information-War Capabilities," DefenseOne, April 5, 2022.

Department of Defense 8570.01-M, *Information Assurance Workforce Improvement Program*, December 19, 2005, change 4, November 10, 2015.

Department of Defense Directive 3600.01, *Information Operations*, May 2, 2013, change 1, May 4, 2017.

Department of Defense Directive 8140.01, *Cyberspace Workforce Management*, October 5, 2020.

Department of Defense Instruction 1025.10, *Chief Financial Officer (CFO) Academy*, June 22, 2018.

Department of Defense Instruction 1322.35, Vol. 1, *Military Education: Program Management and Administration*, April 26, 2022.

Department of Defense Instruction 1430.02, *Civilian Career Management,* April 6, 2006.

Department of Defense Instruction 1430.16, *Growing Civilian Leaders*, August 23, 2022.

Department of Defense Instruction 8140.02, *Identification, Tracking, and Reporting of Cyberspace Workforce Requirements,* December 21, 2021.

Director for Joint Forces Development, "Process for Accreditation of Joint Education (PAJE)," memorandum for Chancellor (Acting), College of Information and Cyberspace, May 1, 2019.

DoD—*See* U.S. Department of Defense.

DoDD—*See* Department of Defense Directive.

DoDI—*See* Department of Defense Instruction.

Dunford, Joseph F., Jr., "Special Areas of Emphasis for Joint Professional Military Education in Academic Years 2020 and 2021," memorandum for Chiefs of the Military Services, President, National Defense University, CM-0108-19, May 6, 2019.

Eisenhower School for National Security and Resource Strategy, "Forging a New Generation of Strategic Leaders," webpage, undated. As of May 31, 2022: https://es.ndu.edu/About/Mission

Eisenhower School for National Security and Resource Strategy, "Senior Acquisition Course," webpage, undated. As of June 20, 2022: https://es.ndu.edu/Programs-and-Departments/Senior-Acquisition-Concentration/

Ingram, David, "Russia Is Nearly Isolated Online. What Does That Mean for the Internet's Future?" NBC News, March 15, 2022.

JFSC—*See* Joint Forces Staff College.

Joint Chiefs of Staff, *Joint Concept for Operating in the Information Environment (JCOIE)*, Washington, D.C., July 25, 2018.

Joint Forces Staff College, "Joint Information Operations Planners' Course (JIOPC)," webpage, February 4, 2021a. As of August 26, 2022: https://jfsc.ndu.edu/Academics/Joint-C2-Information-Operations-School-JC2IOS/Information-Operations-Division/JIOPC/

Joint Forces Staff College, "Joint MILDEC Training Course (JMTC)," webpage, March 31, 2021b. As of August 26, 2022: https://jfsc.ndu.edu/Academics/Joint-C2-Information-Operations-School-JC2IOS/Information-Operations-Division/JMTC/

Joint Forces Staff College, "Defense Operations Security Planners Course (DOPC)," webpage, July 20, 2022. As of August 26, 2022: https://jfsc.ndu.edu/Academics/Joint-C2-Information-Operations-School-JC2IOS/Information-Operations-Division/DOPC/

Joint Staff, *Capstone Concept for Joint Operations: Joint Force 2020*, September 10, 2012.

Joint Staff, *Description of the National Military Strategy 2018*, 2018.

Joint Staff J3, *Operations in the Information Environment Curriculum Development Guide*, October 2019.

Joint Publication 3-12, *Cyberspace Operations*, June 8, 2018.

Joint Publication 3-13, *Information Operations*, November 27, 2012, change 1, November 20, 2014.

Marine Corps University, *AY 2020–2021 Catalog*, 2020a. As of February 23, 2022: https://www.usmcu.edu/Portals/218/Registar/AY20-21-MCU-Catalog.pdf

Marine Corps University, "USMC School of Advanced Warfighting, Academic Year 2019–2020," briefing, 2020b. As of February 24, 2022: https://www.usmcu.edu/Portals/218/SAW%20Inbrief-9%20Jul%2019%20(1).pdf

Mayberry, Paul W., Charles A. Goldman, Kimberly Jackson, Eric Hastings, Hannah Acheson-Field, and Anthony Lawrence, *Making the Grade: Integration of Joint Professional Military Education and Talent Management in Developing Joint Officers*, RAND Corporation, RR-A473-1, 2021. As of September 23, 2022: https://www.rand.org/pubs/research_reports/RRA473-1.html

MCU—*See* Marine Corps University.

Memorandum of Agreement Between the Office of the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict (OASD(SO/LIC&IC)) and the National Defense University, December 20, 2010.

Microsoft, "Windows Commands," Microsoft Ignite website, January 4, 2022. As of September 23, 2022: https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/windows-commands

Microsoft Digital Security Unit, S*pecial Report: Ukraine—An Overview of Russia's Cyberattack Activity in Ukraine*, April 27, 2022.

National Defense University Regulation 5.75, "National Defense University Electives Program," June 1, 2014. As of October 3, 2022: https://www.ndu.edu/Portals/59/Documents/AA_Documents/AA%205.75.pdf

National Defense University, *2021–2022 Electives Program Catalog*, 2021.

National Intelligence University, "About NIU," webpage, undated-a. As of February 28, 2022: https://ni-u.edu/wp/about-niu/

National Intelligence University, "NIU History," webpage, undated-b. As of June 21, 2022: https://ni-u.edu/wp/about-niu/niu-history/

National Intelligence University, *Catalog for Academic Year 2021–22*, 2021.

Naval Postgraduate School, "Institutional Learning Objectives," webpage, undated. As of February 14, 2022: https://nps.smartcatalogiq.com/en/Current/Academic-Catalog/General-Academic-Information/Institutional-Learning-Objectives

Naval Postgraduate School, "Degree-Specific Requirements," webpage, November 23, 2021. As of September 23, 2022: https://nps.smartcatalogiq.com/Current/Academic-Catalog/General-Academic-Information/Degree-Specific-Requirements

NDU—*See* National Defense University.

NPS—*See* Naval Postgraduate School.

Public Law 99-433, Goldwater-Nichols Department of Defense Reorganization Act of 1986, October 1, 1986.

Public Law 115-91, National Defense Authorization Act for Fiscal Year 2018, December 12, 2017.

Public Law 116-92, National Defense Authorization Act for Fiscal Year 2020, December 20, 2019.

Public Law 116-283, William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, January 1, 2021.

Public Law 117-81, National Defense Authorization Act for Fiscal Year 2022, December 27, 2021.

Rounds, M. Michael, Joe Manchin III, James R. Langevin, and Elise Stefanik, "Letter to the Honorable Mark T. Esper and the Honorable David L. Norquist," April 24, 2020.

Schwille, Michael, Anthony Atler, Jonathan Welch, Christopher Paul, and Richard C. Baffa, *Intelligence Support for Operations in the Information Environment: Dividing Roles and Responsibilities Between Intelligence and Information Professionals*, RAND Corporation, RR-3161-EUCOM, 2020. As of June 23, 2022: https://www.rand.org/pubs/research_reports/RR3161.html

Sherman, John, "Statement by John Sherman Acting Chief Information Officer for Department of Defense Before the Senate Armed Services Committee Subcommittee on Personnel on Cyber Workforce," April 21, 2021. As of June 16, 2022: https://www.armed-services.senate.gov/hearings

Takai, Teresa M., "National Defense University (NDU) iCollege Restructuring," memorandum for Director, Joint Force Development (DJ7), September 21, 2012, Not available to the general public.

Under Secretary of Defense (Comptroller)/Chief Financial Officer and the National Defense University, Memorandum of Agreement, March 13, 2008.

United Nations Conference on Trade and Development, *Digital Economy Report 2021*, United Nations Publications, 2021. As of June 21, 2022: https://unctad.org/webflyer/digital-economy-report-2021

U.S. Army War College, "Military Education Level 1 Programs," webpage, undated-a. As of March 8, 2022: https://www.armywarcollege.edu/programs/mel_1.cfm

U.S. Army War College, "Mission Command and Cyber Division (MCCD)," webpage, undated-b. As of February 23, 2022: https://csl.armywarcollege.edu/SLET/mccd/default.aspx

U.S. Army War College, *Strategic Cyberspace Operations Guide*, August 1, 2021.

USAWC—*See* U.S. Army War College.

U.S. Code, Title 10, Armed Forces, Subtitle A, General Military Law, Part II, Personnel, Chapter 38, Joint Officer Management, Section 668, Definitions.

U.S. Code, Title 10, Armed Forces, Subtitle A, General Military Law, Part III, Training and Education, Chapter 107, Professional Military Education, Section 2151, Definitions.

U.S. Code, Title 10, Armed Forces, Subtitle A, General Military Law, Part III, Training and Education, Chapter 107, Professional Military Education, Section 2152, Joint Professional Military Education: General Requirements.

U.S. Code, Title 10, Armed Forces, Subtitle A, General Military Law, Part III, Training and Education, Chapter 107, Professional Military Education, Section 2155, Joint Professional Military Education Phase II Program of Instruction.

U.S. Code, Title 10, Armed Forces, Subtitle A, General Military Law, Part III, Training and Education, Chapter 108, Department of Defense Schools, Section 2163, Degree Granting Authority for National Defense University.

U.S. Code, Title 10, Armed Forces, Subtitle A, General Military Law, Part III, Training and Education, Chapter 108, Section 2165, National Defense University: Component Institutions.

U.S. Code, Title 10, Armed Forces, Subtitle B, Army, Part III, Training, Chapter 751, Training Generally, Section 7421, Degree Granting Authority for United States Army War College.

U.S. Code, Title 10, Armed Forces, Subtitle C, Navy and Marine Corps, Part III, Education and Training, Chapter 855, United States Naval Postgraduate School, Section 8548, Degree Granting Authority for United States Naval Postgraduate School.

U.S. Code, Title 10, Armed Forces, Subtitle C, Navy and Marine Corps, Part III, Education and Training, Chapter 859, Professional Military Education Schools, Section 8591, Degree Granting Authority for Naval War College.

U.S. Code, Title 10, Armed Forces, Subtitle C, Navy and Marine Corps, Part III, Education and Training, Chapter 859, Professional Military Education Schools, Section 8592, Degree Granting Authority for Marine Corps University.

U.S. Code, Title 10, Armed Forces, Subtitle D, Air Force and Space Force, Part III, Training, Chapter 951, Training Generally, Section 9414, Degree Granting Authority for United States Air Force Institute of Technology.

U.S. Code, Title 10, Armed Forces, Subtitle D, Air Force and Space Force, Part III, Training, Chapter 951, Training Generally, Section 9417, Degree Granting Authority for Air University.

U.S. Code, Title 50, War and National Defense, Chapter 44, National Security, Subchapter VIII, Education in Support of National Intelligence, Part D, National Intelligence University, Section 3227a, Degree-Granting Authority.

USCYBERCOM—*See* U.S. Cyber Command.

U.S. Cyber Command, "Our History," webpage, undated. As of March 2, 2022: https://www.cybercom.mil/About/History/

U.S. Cyberspace Solarium Commission, *United States of America Cyberspace Solarium Commission*, final report, March 2020.

U.S. Department of Defense, "DoD Cyber Workforce Framework," website, undated. As of June 28, 2022: https://public.cyber.mil/cw/dcwf/

U.S. Department of Defense, *Information Operations Roadmap*, Washington, D.C., October 30, 2003. As of July 9, 2022: https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Other/Information_Operations_Roadmap_30_October_2003.pdf

U.S. Department of Defense, *Department of Defense Strategy for Operations in the Information Environment*, June 2016.

U.S. Department of Defense, *DoD Cyber Workforce Management Board Charter*, January 13, 2017.

U.S. Department of Defense, *Summary Department of Defense Cyber Strategy*, 2018a.

U.S. Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge*, 2018b.

U.S. Department of Defense, *Matters Concerning the College of Information and Cyberspace and Limitation of Funding for National Defense University*, report to Congress submitted Pursuant to Section 1741 of the FY2021 NDAA, April 9, 2021a.

U.S. Department of Defense, *DoD Dictionary of Military and Associated Terms*, November 2021b. As of September 26, 2022: https://irp.fas.org/doddir/dod/dictionary.pdf

U.S. Naval War College, "College of Naval Warfare Core Curriculum," webpage, undated-a.

U.S. Naval War College, "Cyber & Innovation Policy Institute," webpage, undated-b.

von Clausewitz, Carl, *On War*, ed. and trans. by Michael Howard and Peter Paret, Princeton University Press, 1976.

Washington Headquarters Services, "Reading Room List, Other," webpage, undated. As of July 9, 2022: https://www.esd.whs.mil/FOIA/Reading-Room/Reading-Room-List_2/Other/

Washington Post Staff, "Database of 235 Videos Exposes the Horrors of War in Ukraine," The *Washington Post*, May 9, 2022. As of June 14, 2022: https://www.washingtonpost.com/world/interactive/2022/ukraine-russia-war-videos-verified/

White House, *National Security Strategy of the United States of America*, December 2017.

NATIONAL DEFENSE RESEARCH INSTITUTE

The Fiscal Year 2021 National Defense Authorization Act directed the Department of Defense (DoD) to provide a report on plans for closing the College of Information and Cyberspace (CIC) at the National Defense University and addressing the broader needs in the department for the types of education the college provided. DoD provided a response in April 2021 that outlined the original options considered for the college but deferred questions regarding the role for CIC and the department's needs for cyberspace and information education for a follow-on study that RAND's National Defense Research Institute conducted.

This report examines how DoD educational institutions operating at the graduate level, including CIC, are currently addressing cyberspace and information education in their curricula, the potential demand across the department for this education, and how CIC can contribute to fulfilling this demand, as well as what role it should play more broadly in supporting other DoD educational institutions and DoD components.

www.rand.org

RR-A1548-1