

JOINT PROFESSIONAL MILITARY EDUCATION INSTITUTIONS IN AN AGE OF CYBER THREAT

Francesca Spidalieri

August 7, 2013

The United States military—already the world’s largest military spender—plans to expand its offensive and defensive capabilities in cyberspace and increase its budget for cyber operations to an estimated \$4.7 billion, according to the FY2014 defense budget proposal. In January, the Pentagon announced a major expansion of its Cyber Command and the development of new cyber weapons and a revised set of “rules of engagement” for cyber conflicts, which will help field commanders determine how and when to deploy cyber capabilities.¹ A top-secret presidential policy directive issued last October but only recently leaked to the media confirmed the government’s plans to step up America’s offensive capabilities relating to cyber-attacks, including identifying potential overseas targets.² Together, these expansions reflect the understanding that any future conflict and crisis will contain a cyber component, particularly when one considers that “no modern military enters the battlespace without at least some reliance on computers and computer networks.”³ James Clapper, Director of National Intelligence, decried cyber threats as the top threat to national security in his Worldwide Threat Assessment prepared for Congress. “Threats are more diverse, interconnected, and viral than at any time in history,” the report stated, adding that “destruction can be invisible, latent, and progressive.”⁴ General Keith Alexander, U.S. Cyber Command chief and director of the National Security Agency, reiterated to Congress during another recent hearing that cyber threats are growing dramatically and that “when you look at the strategic landscape from our perspective, it’s getting worse.”⁵

The growing scope and sophistication of cyber threats and the development of cyber tools as technical weapons have also been accompanied by another realization: that there are far too few people—whether civilian or military—equipped with knowledge sufficient to protect the information infrastructure, improve resiliency, and leverage information technology for strategic advantage. In 2009, President Barack Obama identified cyber threats as “one of the most serious economic and national security challenges we face as a nation.” In addition to recognizing the threat, President Obama also recognized our shortcomings: “it’s also clear that we’re not as prepared as we should be as a government or country.”⁶ Admiral James Stavridis, the recently retired Supreme Allied Commander of NATO, echoed that sentiment by noting that, in cyber-conflicts, “the greatest mismatch between the level of threat to our

Francesca Spidalieri is a fellow at the Pell Center for International Relations and Public Policy at Salve Regina University. This study follows the report “One Leader at a Time: The Failure to Educate Future Leaders for an Age of Persistent Cyber Threat,” which detailed the failing of America’s most prestigious graduate programs to prepare the nation’s next generation of leaders to stand the test of modern cybersecurity. That report can be accessed at: <http://pellcenter.salvereginablogs.com/files/2013/04/One-Leader-at-a-Time-FINAL.pdf>



country (high) and our level of preparation (low) is evident.”⁷ Lieutenant General Michael Flynn, Director of the U.S. Defense Intelligence Agency, in discussing the “invisible war” that is currently being waged in cyberspace, also emphasized the preparation gap: “for every person working in military cybersecurity today, we could use 28 more.”⁸

The U.S. Navy, for example, which relies heavily on computer networks and satellites for its weapons systems and command and control, desperately needs cybersecurity experts for a panoply of activities. They must not only protect computer systems ashore, each warship’s self-contained network, and the intranet shared with the Marine Corps, but they must also coordinate ships, planes, and personnel.⁹ Similarly, security of satellites is paramount as they underpin nearly all U.S. military functions with communications, target, and weather data, along with warning of missile launches.¹⁰

Cyber espionage and cyber sabotage can not only speed up enemies’ development of their own defense technologies but can also impose severe consequences for U.S. forces engaged in combat, as enemies can knock out communications, corrupt data, and cause computer-based weapons to malfunction.¹¹ A well-executed cyber-attack could shut down or disrupt military command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) systems, and jeopardize the execution of entire military missions. The consequences for the U.S. military, and national security, could be devastating.

While cybersecurity should not be viewed solely or primarily as a military problem, the U.S. military relies extensively on cyberspace and its information and networks for its missions, and military networks are increasingly the target of cyber-attacks, exfiltration, and espionage. Moreover, the military would be called upon to respond, probably kinetically, in the case of a major cyber-attack that produces death, damage, destruction or high-level disruption similar to the results that a traditional military attack would cause. Finally, cyberspace is now considered a new battlefield, one that you cannot see and where a “silent war” is already underway between countries that have been ramping up their cyber-arsenals for at least the past decade.¹² The important question is not whether the U.S. can develop advanced cyber capabilities, but whether our military—and our leaders in general—are equipped with knowledge sufficient to tackle the cyber threat. The way to meet that challenge rests in establishing a competitive and security advantage on the modern battlefield.

The Role of Education in Preparing for an Age of Cyber Threats

No “silver bullet” solution exists for cyber threats to military or government networks. No single technology, government policy, law, treaty, or program can stop all cyber-attacks. That is the reality. But while there may be no single panacea, a confluence of technical, economic, legal, ethical, political, diplomatic, and strategic solutions can complement each other to help achieve cybersecurity. As soldiers, sailors, airmen, and marines learn to turn their attention from incoming missiles to cyber weapons, a technology-centric education will be insufficient to counter and mitigate current and future cyber threats.¹³ This is not to say that a cyber workforce with specific

technical skills needed to develop and administer the cyber environment—the so-called next generation of “cyber warriors”—is unimportant. Rather, a new cadre of cyber-strategic military leaders will also be needed to lead, manage, and oversee cyber defense and cyber operations. These individuals do not necessarily need specific training in engineering or programming, but they must have a deep understanding of the cyber context in which they operate, compounded with an appreciation of military ethics, strategic studies, political theory, institutional theory, international law, international relations, and additional sciences. A broader education and focus on imaginative thinking will also be needed to devise strategies and policies not narrowly grounded on U.S. perception of opportunities and vulnerabilities in cyberspace, but that instead take into consideration how peer competitors may leverage the cyber realm and cyber capabilities for their advantage. Only a truly comprehensive education will help foster modern military leadership and enable them to harness the right tools, people, and strategies, and balance of offensive and defensive cyber capabilities.

Evolution involves change. As Albert Einstein wrote, “No problem can be solved from the same level of consciousness that created it.”¹⁴ As we enter an age of persistent cyber threats, a world where capability and influence may soon be measured not in kilotons but in kilobytes, strong cybersecurity skills, the ability to obtain, analyze, manipulate, and correlate data, and the knowledge necessary to leverage cyberspace advantages to create effective strategies, policies, and laws will be the deciding factor for success and resiliency.

Universities stand poised to serve as incubators of these non-technical cyber leaders, “bringing theory and doctrine, with methodology, tools, and implementation.”¹⁵ They ought to play a key role in educating civilians and members of the military on the unique aspects of cybersecurity, fusing knowledge, intellectual capacity, practical skills, and optimizing their campus-wide resources to devise comprehensive curricula that synthesize technical, policy, sociological, and legal components in the study of cyber threats. They have the knowledge and authority to make that a reality. But as underscored in our recent report, “One Leader at A Time: The Failure to Educate Future Leaders for an Age of Persistent Cyber Threat,” many of America’s non-technical graduate programs are generally failing to prepare their graduates—and ultimately the nation—for leadership of critical institutions.¹⁶ Even professional military institutions studying national security and strategy have only recently begun to integrate cybersecurity education in their curricula, despite more than a decade’s worth of experience suggesting that networks and information technologies are both essential to operations and vulnerable to attack.¹⁷

Changing the Culture of Senior Military Institutions

No captain of a ship would say: “*I don’t know anything about the ocean, but I hired somebody to drive the ship.*”¹⁸ Similarly, future generations of military and government officials who have to navigate a digitized world need to have a broader understanding of cyberspace and the ability to make military and policy decisions based on knowledge of cybersecurity risks and potential impacts. In particular, it is essential that military institutions of higher learning are aligned with the strategic goals of the nation’s cyber defense strategy and clearly understand the underpinnings of the digital



battlefield. For military leaders, knowledge of cyberspace and cyber warfare must be accompanied by the ability to implement fundamental and overarching strategies to mitigate cyber threats, think strategically and imaginatively, and develop the reciprocal trust and confidence needed between echelons to plan and conduct joint military operations.

Most of these military leaders pursue their Joint Professional Military Education (JPME)—a requirement for becoming a Joint Staff Officer and promotion to senior ranks—at one of the U.S. military graduate schools before obtaining upper level command positions in the armed services or government agencies. JPME is designed to provide a deep understanding of how the unified commanders, Joint Staff, and Department of Defense (DoD) use the instruments of national power to develop and carry out national military strategy, develop joint operational expertise and perspectives, and hone joint warfighting skills.¹⁹ Joint professional military education, however, does not necessarily mirror the strategic environment within which military leaders operate—an environment where cyber threats are increasing at a faster rate than our ability to counter them—and may not provide military members with all the skills needed to tackle these threats.²⁰ Whereas a core curriculum covering the range of military roles, capabilities, processes, and functions along with developing critical thinking skills is typically not in question in JPME institutions, their crux today is how to expand student thinking to encompass broader perspectives, the complexities residing in the strategic environment—including in cyberspace—and the broad range of issues they face in the operating environment, including cyber threats. What poses a particular challenge is the lure to apply traditional military thinking when discussing cyber warfare and the consequent belief that the military can carry out cyber operations based on doctrines and intellectual underpinning of land battle as traditionally taught. As eloquently explained by Dr. Jan Kallberg and Dr. Bhavani Thuraisingham:

Carl von Clausewitz assumed that the soil, woods, heights, and rivers of the Napoleonic battlefield were fixed. In a Clausewitzian world, the battle commander could understand and study the battlefield, and by objective permanence, the intended battlefield would be there the next day ready for battle.... In cyber, the map and terrain that form the battlespace change continuously in real time and beyond our imagination as new nodes are discovered and a kaleidoscope of network patterns occurs and disappears.... If we assume that we have control of the situation and knowledge of our enemy's positions and the full extent of the map, with our defense focused on hardened strongpoints, then we are fighting the digital cyberwar with tools of analogue positional warfare.²¹

Thus, traditional military theories and traditional rules of war—which require identifying opponents, their locations, goals, tools, motivations or propensities to act before, during or even after an attack—may not be directly translatable when planning and responding to cyber operations.²² If the Stuxnet virus, deployed against the Iranian nuclear program, was a blueprint for a new way of attacking large scale societal infrastructure without direct personal involvement and showed the world “the new face of 21st century warfare: invisible, anonymous, and devastating;”

Conficker—the largest known computer worm infection to date that spread globally through militaries, government, and institutions, opening backdoors to hidden remote controllers in millions of computers worldwide—possibly created the largest cyber army in the world still waiting for their mission. The lessons from these ever-changing cyber threats need to be learned, traditional military paradigms ought to be reviewed in light of the changing character of the operating environments, and more options for national cyber defense need to be developed and continuously tested.²³

During recent Senate testimony, General Alexander expressed his aspiration to “increase the education of our future leaders by fully integrating cyber in our existing war college curricula,” where most of the JPME training occurs, and that “this will further the assimilation of cyber into the operational arena for every domain.”²⁴ General Alexander continued by saying that “ultimately we could see a war college for cyber to further the professional military education of future leaders in this domain.” This last conclusion, however, continues to further the notion that cyberspace is a separate domain from land, sea, air, and space—instead of a man-made, dynamic substrate encompassing the physical domains—and that it will require a distinct war college to train a separate specialized military cyber workforce.²⁵

As previously stated, achieving cybersecurity is more than a technical issue and it demands cyber-strategic leadership across the whole range of societal institutions and military services. What we need is the ‘war colleges of cybersecurity’, where cyber is an integral component of any officer’s military education and training and it is taught as fully integrated with missions in the physical domains. Military institutions of higher learning should be instrumental in creating this new cadre of cyber-strategic military leaders. After all, these institutions are designed specifically to produce senior officers who have the skills and knowledge needed to take on leadership roles in the battlefield, as well as in government agencies and other organizations, and construct effective strategies to protect the nation’s security and independence. There exists no group with a more urgent need for understanding cyber issues, honing the ability to lead, manage, and oversee cyber operations, and being prepared to act with little or no reliable information—if adversaries are able to degrade or deny their access to cyberspace.

This study surveys current efforts by military postgraduate programs in the United States to prepare officers for the challenges of operational and strategic level leadership in an age of cyber threats. The survey focuses specifically on JPME institutions—which traditionally develop strategic and operational leaders across the armed services—to assess what level of exposure to cyber issues their students receive and to what extent they graduate with an adequate understanding of the cyber challenges facing their respective services. Lastly, the report identifies which of these programs still needs to include a cybersecurity component into their curricula. For each institution, the study indicates NSA-designation as Center of Academic Excellence in Information Assurance Education (CAE/IAE) and research (CAE/R)—if awarded—and a modified Likert approach with score (0 to 4) to evaluate the opportunities offered to prepare graduates on broad systematic cyber threats and cyber warfare.²⁶



Methodology

This study summarizes our survey findings of current efforts by military postgraduate programs teaching JPME to include information technology and cybersecurity education in their curricula. It seeks to identify best practices, review program effectiveness in promoting the study of cybersecurity and cyber warfare, and identify existing curriculum gaps in this field. This report does not provide an in-depth analysis of specific courses or an extensive audit of particular programs; rather, it offers a global snapshot to present the progress, or lack thereof, made by each JPME institution to integrate an information technology and cybersecurity component into their curricula.

The survey findings are based on data collected between March and June 2013 from each educational institution. This data was obtained through a combination of interviews with academics and university staff, in addition to material drawn from school websites. The results stem from the responses to four main curriculum questions and the use of a modified Likert approach to evaluate the level of exposure students receive to cybersecurity issues in each of these institutions and the opportunities offered to deepen their knowledge in this field. Respondents were asked whether their institution offers: 1) core courses in information technology, with at least part of the course dedicated to cybersecurity; 2) elective courses in information technology and cybersecurity; 3) the possibility for their students to enroll in other elective courses in information technology and cybersecurity at other schools or departments; 4) occasional seminars, conferences or training opportunities in cybersecurity and cyber operations. The modified Likert scale used to derive a notional ranking of the institutions analyzed assigns a number (0 to 1) to each response as follows: Yes = 1; Not specifically, but... = 0.5; No = 0. The answers are then summed up and each institution receives an overall score on a 0 to 4 scale, 4 being the highest score they can receive. The specific responses are also discussed in more detail in this report.

In instances where respondents did not provide an answer to all four questions, we made our own assessment based on the information available from that program's website. The assumption behind this approach is that if JPME institutions offer a dedicated core course in IT and cybersecurity, all service members in the program will most likely receive the broader education and practical knowledge needed to manage the information security needs of their armed service and leverage information technology for strategic advantage. If it offers elective courses in IT and cybersecurity, students interested in the topic will have at least the opportunity to gain an understanding of the cyber-context and explore cyber related issues. If cybersecurity issues are covered as part of broader courses, students will gain a general understanding of the cyber challenges and opportunities in that specific area of study. If the school offers occasional seminars, conferences or wargaming exercises encompassing cybersecurity issues, students will have a chance to be exposed to understanding cyber threats and how they can affect military operations. If none of these opportunities are provided, we assume that graduates of these programs do not gain a thorough understanding of the challenges, opportunities, and threats of the digital age beyond their own personal experience.



Recognizing that the inclusion of cybersecurity technology, strategy, and policy components may still be a work in progress for some of these institutions, we hope that our findings will add value to other efforts to integrate cybersecurity education and training in military postgraduate programs and serve as useful tools for academic and professional institutions considering various approaches towards cybersecurity leadership development.

Joint Professional Military Education Institutions Survey

| JPME Institution | City | State | Likert Scale Average Score (Max = 4) | NSA Certification* |
|--------------------------------|------------|-------|--------------------------------------|--------------------|
| National Defense University | Washington | DC | 3.5 | E |
| U.S. Naval War College | Newport | RI | 3.0 | N/A |
| Naval Postgraduate School | Monterey | CA | 3.0 | E, R |
| U.S. Air Force Air War College | Montgomery | AL | 2.0 | N/A |
| Marine Corps War College | Quantico | VA | 1.0 | N/A |
| U.S. Army War College | Carlisle | PA | 0.5 | N/A |

* Indicates university NSA designation as a Center of Academic Excellence in Information Assurance Education (E) and/or Research (R).

National Defense University

Washington, DC

Likert Score: 3.5/4

NSA Cert: CAE/IAE

The National Defense University (NDU) is the premier center for joint professional military education, dedicated to preparing military and civilian leaders to better address national and international security challenges. Some aspects of cybersecurity and cyber warfare education have been integrated at different levels in the curricula of all five NDU colleges—the National War College, the Information Resources Management College (iCollege), the Industrial College of the Armed Forces, the Joint Forces Staff College, and the College of International Security Affairs. “As the largest of the five colleges at NDU, the iCollege serves as the university’s expert in cyber and IT leadership, [and] it is open to the larger DoD, federal government, U.S. and international communities,” explained Patricia Coopersmith, Director of Outreach and International Relations. “The iCollege’s mission is to prepare military and civilian leaders to optimize information technology management and secure information dominance within cyberspace,” she continued.

NDU iCollege offers a multi-disciplinary approach to cyber issues and approximately 50 courses focused on cyber, IT leadership, and related topics in residence and online throughout the academic year. NDU iCollege professors cover a range of areas in each cyber-related course, including policy, process, governance, law, tools, partnerships (industry and international), culture, organizational change, and collaboration. In particular, “the Cyberspace Integration and Integrated Operation (CI&IO) Department focuses on information assurance, cybersecurity, and the supporting role of information integration in the planning and execution of national and military strategy,” explained



faculty member, Lieutenant Colonel Sean Kern.²⁷ Graduates pursuing the iCollege's Masters in Government Information Leadership can choose from a broad array of courses in different departments to acquire specific knowledge and skills in information resources management-related fields of study. Students specifically focusing on the cyber curriculum must pick three of the seven courses available in this concentration, with the course "Cyberspace in the 21st Century" required.

The iCollege offers also a robust electives program to all NDU students, enabling them to delve deeper into areas that are covered in the core programs, from information security management, to cyberspace strategies, transnational cyberspace policies, and cyberlaw.²⁸ Among the most popular courses offered throughout the year is "Information Assurance and Critical Infrastructure Protection," a course focused at the public policy and strategic management level which provides a foundation for analyzing the information security components of information systems and critical infrastructure and assuring the confidentiality, integrity, and availability of critical information assets. Similarly, the course "Global Strategic Landscape" prepares students to evaluate the various components of national security strategy and "integrating cyber as a tool of national power," explained faculty member, Colonel Nate Allen.²⁹ In addition, the iCollege CI&IO Department administers two dedicated graduate certificate programs: (1) a Cyber Security (Cyber-S) Certificate Program, consisting of nested certificates that emphasize cybersecurity issues and fundamental approaches to the protection of the nation's information infrastructure; and (2) a multi-disciplinary Cyber Leadership (Cyber-L) Certificate Program, that examines the nature of organizations and the people who collaborate using shared information to operate, while securing, protecting, and defending knowledge capital and cyber assets.

As a NSA-designated Center of Academic Excellence in Information Assurance Education, NDU iCollege works to integrate key learning objectives of the National Cyber Strategy into curricula made available to the entire university, and operates two cybersecurity labs—or "experiential learning classrooms," as described by Lieutenant Colonel Kern. The Cyber Attack/Defend Lab serves to examine computer and network defense through exercises in intrusion techniques, mitigation, and forensics. The Supervisory Control and Data Acquisition (SCADA) Lab simulates realistic exploits and protections of various industrial control systems, such as electrical, oil, gas, water, and transportation grids. "These classrooms are intended to expose students to attack, defend, and SCADA issues at a managerial level, although there is a hands-on component," continued Lieutenant Colonel Kern.

Furthermore, the iCollege has formed academic partnerships with nearly 40 other accredited universities across the United States for credit acceptance into several IT and cyber-related Master's and Doctoral Degree programs. Finally, the iCollege hosts occasional Cyber Challenges Competitions and international cybersecurity conferences (although, recent government budget issues have temporarily put these conferences on hold). For regular iCollege courses, faculty members occasionally conduct small seminars, workshops, and other educational activities to address specific cyber-related issues and topics, and invite executive-level guest speakers from the U.S. private sector to introduce best practices.



From the information provided, graduates of NDU iCollege clearly receive a comprehensive, national/strategic cyber education in the full spectrum of cybersecurity issues from technical to strategic leadership, and the practical knowledge needed to successfully navigate cyberspace and promote its integration with the physical domains. However, it remains surprising that the other NDU colleges have not integrated more aspects of cyber education in their curricula, and that only those graduates already predisposed to cybersecurity issues will take advantage of the opportunity to attend iCollege elective courses and other cyber-related events. This seems to be a choice on the part of NDU to promote the iCollege as their primary institution for the study of information technology and cyber operations, and it is unclear if the other colleges will incorporate a stronger cybersecurity component in the future.

U.S. Naval War College

Newport, RI

Likert Score: 3/4

NSA Cert: N/A

The U.S. Naval War College (NWC) prides itself for being a leader in developing concepts towards operationalizing cyber warfare, cyberspace operations, and cyber conflict in joint military operations and planning paradigms. Although none of the courses in the NWC core curriculum—which provides the backbone for JPME—is exclusively dedicated to information technology or cybersecurity, aspects of cyber education have been integrated across the full range of NWC in-residence academic programs, as part of both JPME and the M.A. in National Security and Strategic Studies curricula. As Captain Roy Petty, coordinator of the Information Operations, Command and Control Warfare and Battlespace Awareness area of study, explained: “all core courses now include at least one lecture on the information environment and specific cyber issues.”³⁰ Faculty members try to bring cyber issues into the curriculum at the outset of every course, because “if you don’t your adversary will,” continued Captain Petty. Students interested in cyber-related issues can also choose from a set of dedicated electives, such as “Cybersecurity: Cybered Conflict, Response to Surprise, and Emerging Indicators of Global System Change,” “IO and Cybered Warfare: Current Issues in the Information Environment,” and “Net-Centric and Cyber Operations.” Through these courses, students gain a thorough understanding of the information systems upon which cyberspace is built, the technical, social, and institutional structure of the Internet, its key players, major risks, and emerging trends, the national and international level institutional, policy, and legal responses to cyber threats, the role of information integration in the planning and execution of national and military strategy, and the key elements of network centric warfare and information operations. NWC graduates may also have the opportunity to attend one of Professor Michael Schmitt’s lectures on the *Tallin Manual on the International Law Applicable to Cyber Warfare*, which examines how extant international law norms apply to this “new” form of warfare.³¹

Beyond the classroom, students may have the opportunity to support research projects in the summer months and work alongside faculty members who have published journal articles and papers contributing to the body of cybersecurity literature. Among this research work are a comprehensive analysis of security resilience strategy in response to surprise attacks in a cybered world, an empirical study on the implications of cyber challenges for the structures, processes, and perspectives of security organizations, and an investigation of the roles that technology played in the 2011 Libyan Revolution.



In 2011, NWC established a Center for Cyber Conflict Studies (C3S) to facilitate and coordinate information sharing within the college and advance the interdisciplinary study of the challenges presented by cyber warfare, cyberspace operations, and cybered conflict in the 21st century. Even if not an integral part of the JPME education, NWC also organizes regular cyber-focused events and operational simulations for students, joint and fleet commanders, and representatives of DoD and various government agencies. The war gaming exercises often integrate cyberspace with traditional military operations, allowing participants to explore potential capabilities of cyber operations in future warfare, and learn more about cyber command and control (C2) challenges, the processes, authorities, and legal issues of cyber operations.

Finally, NWC has partnered with the University of Rhode Island and Brown University on cybersecurity issues, particularly those at the intersection of technology, policy, law, and national strategy. Although still in its incipient stages, this Rhode Island Academic Collaboration on Cybersecurity Technology and Policy (CCTP) is supposed to encourage the sharing of information on degree programs and courses offered at these institutions, publications produced, and seminars, colloquia, and conferences being planned.³²

From the information collected, NWC students interested in cyber matters, especially those in the Information Operations, Command and Control Warfare and Battlespace Awareness area of study, have various opportunities to be exposed to cybersecurity and cyber warfare issues and gain the knowledge necessary to integrate cyber capabilities and information activities with other U.S. government actions. The various cyber-related academic and research initiatives delineated above could offer the NWC curricula many ways in which to integrate an even more robust cyber curriculum across the different departments.

Naval Postgraduate School

Likert Score: 3/4

Monterey, CA

NSA Cert: CAE/IAE, CAE/R

The Naval Postgraduate School (NPS) offers graduate degree programs in a wide variety of disciplines to officers of all U.S. military services, civilian employees of the government, a limited number of DoD contractors, and selected international students from allied nations through its four schools: the School of Business and Public Policy; the School of Engineering and Applied Science; the School of Operational and Information Sciences; and the School of International Graduate Studies. Thanks to a long-standing partnership between NPS and the U.S. Naval War College, NPS students are able to complete their JPME certification while pursuing their degree at NPS. The JPME core courses are aligned with those offered through the NWC program in Newport and administered through the NWC's Monterey satellite office (or College of Distance Education). Thus, NPS students can take the NWC core courses—all conveniently offered in each quarter—in conjunction with their degree requirements on campus, which often include the NWC courses as part of their curricula.

As for the cyber components of NPS curricula, the school has integrated aspects of information technology and cybersecurity education at different levels in all four schools. Cyber education at NPS varies widely from MBAs with a focus on managing information systems and infrastructure,



to technical masters degree programs and certificates entirely dedicated to cybersecurity and cyber operations. The School of Operational and Information Sciences, for example, offers a M.A. in Identity Management and Cyber Security, and a wide array of cyber-related courses (although they are all strongly focused on mathematical, scientific, and technical skills).

In 2011, NPS established a Cyber Academic Group (CAG), an interdisciplinary association of faculty primarily from NPS scientific departments—Computer Science, Electrical and Computer Engineering, Defense Analysis, Operations Research, Mathematics, and Information Sciences—dedicated to building the school’s cyber program curricula, and helping further collaboration in the field. CAG’s objective is to enable NPS students to understand both how to defend networks from penetration and to employ cyber capabilities to ensure an advantage in future operations. A rigorous set of cyber-related courses and research lead to a master’s of science degree in cyber systems and operations or a master’s of science in applied cyber operations. The four-quarter resident program in applied cyber operations “allows students to look at a different aspect of cyber than what they are accustomed to in their careers. Cyber is a team activity and our students are working together, particularly through their capstone projects, to expand their knowledge and capabilities,” described Cyber Academic Group Chair, Dr. Cynthia Irvine.³³ Moreover, the group runs a Cyber Battle Lab, home to NPS semi-annual Cyber Wargames, which fosters interdisciplinary cyber education and research ranging from high-level strategy to machine-level reverse engineering.

CAG, and the departments of Computer Science, Electrical and Computer Engineering, Applied Mathematics, respectively, offer other graduate certificate programs in cybersecurity fundamentals, cybersecurity defense, cyber operations infrastructure, cyber wargaming, cyber warfare, cyber systems, and mathematics of secure communication. In addition, NPS hosts regular conferences, seminars, and symposia on cyber threats, cyber operations, and cyber warfare. Finally, as a NSA-designated Center of Academic Excellence in both Information Assurance Education and Research, NPS is committed to educate the nation’s future cyber workforce.

In principle, NPS could be at the forefront of efforts to create a new cadre of military leaders able to address a broad range of cyber operations within the Navy’s vision, from computer network attack, defense, and exploitation, to cyber analysis, operations, planning and engineering, to cyber intelligence operations and analysis. However, the cyber curriculum at NPS remains very much focused on science and technology, and less so on the policy, sociological, legal, and institutional components of the study of cyber threats, which are also necessary to construct effective strategies and processes for operating in cyberspace.

U.S. Air Force Air War College, Air University

Montgomery, AL

Likert Score: 2/4

NSA Cert: N/A

The U.S. Air War College (AWC), part of the U.S. Air Force’s Air University (AU), educates officers to serve as strategic national security leaders with an emphasis on the air, space, and cyberspace domains. Although none of AWC core courses focuses on IT or cybersecurity, “cyberspace from the strategic level is covered in the Joint Force Capabilities block,” explained AWC student,



Lieutenant Colonel Samuel Bass.³⁴ The “Cyberspace Operations” course in this block covers key strategic and organizational challenges facing senior leaders in supporting military operations in, through, or by means of the cyberspace domain. Other aspects of cyber education have also been integrated across the three AWC academic departments and are part of both the JPME and the AU Master of Strategic Studies curricula. In particular, the AWC Department of Leadership and Warfighting is dedicated to developing senior leaders with the skills to plan, deploy, employ, and control U.S. and multinational forces throughout the range of military operations, including in cyberspace. “Several electives cover cyberspace at the strategic level,” continued Lieutenant Colonel Bass, including “Cyberspace Requirements for the Warfighter” and “Intelligence, Surveillance and Reconnaissance (ISR) Requirements for Cyberspace,” which examines the role of ISR and the legal issues in cyberspace. The “Cyberspace” seminar focuses on the integration of information operations (electronic warfare, network warfare, and especially influence operations) supporting a joint force commander. Most of these courses are taught at the classified level and are only open to U.S. personnel.

In 2005, the AWC established a Cyberspace and Information Operations Study Center to provide support for focused research and writing to students and faculty, coordinate the center academic program with sister services and interagency Senior PME, and link AU with the larger community of cyberspace and info-ops researchers and practitioners. Finally, AWC organizes various cyber-related “exercise scenarios, and each of the 16 seminars of AWC students includes a cyberspace operation officer to provide their perspective and expertise to officers from other career fields in the seminar,” added Lieutenant Colonel Bass.

In brief, AWC graduates interested in the study of cyberspace and cyber operations have the opportunity to be exposed to these topics, but the emphasis is very much on information warfare and the use of intelligence tools, and less so on other important aspects of cybersecurity.

U.S. Army War College

Likert Score: 0.5/4

Carlisle, PA

NSA Cert: N/A

The U.S. Army War College educates military, civilian, and international leaders to be critical thinkers and complex problem solvers in the global application of landpower. Various faculty members have published journal articles and papers on cyber as a new operational domain, cyber infrastructure protection, and cyberspace theory. Although there are no core courses exclusively dedicated to information technology and cybersecurity, courses on national security, military strategy, and contemporary military issues occasionally include cyber warfare and information exploitation in the operational environment (network-centric operations). The Center for Strategic Leadership and Development (CSLD) serves as the Army War College education center and high technology lab, focused on the study of strategic issues affecting the national security community—including cyber threats. CSLD used to offer two dedicated electives in “Cyber Warfare” and “Cyberspace Theory and Strategic Security Implications,” along with other courses focusing on technology applications and emerging threats to national security. However, the cyber courses seem to have been discontinued and the Army War College declined to comment on our survey. Thus,



it is unclear from the information collected if Army War College graduates receive a significant exposure to cyber matters and how they relate to joint military operations.

Marine Corps War College

Likert Score: 1/4

Quantico, VA

NSA Cert: N/A

The Marine Corps War College focuses on the development of leadership, warfighting, and staff operations capabilities of the nation's military forces, with an emphasis on maritime affairs. Although none of the core or elective courses focuses on information technology or cybersecurity, one of the classes in the "National Security and Joint Warfare" course is entirely dedicated to cybersecurity issues. As Dean of Academics Dr. James Anderson recounted, "this year for this class we had Lieutenant General Jon M. Davis, Deputy Commander for U.S. Cyber Command, speak to our students and address questions."³⁵ More generally, "cybersecurity is discussed at several points throughout the curriculum, with an emphasis on strategic-level issues vice technical, IT-related issues, and depending on the subject matter. For example, in classes on future war and china, cyber issues come up quite a bit," added Dr. Anderson. Finally, occasional events on cyber issues may be offered, but these opportunities are educational in nature. Thus, the Marine Corps War College has yet to incorporate a strong cybersecurity component to its curriculum and offer practical knowledge of the opportunities, challenges, and threats in cyberspace. This may be due in part to the Marines culture as an all-purpose, fast-response force focused on accomplishing specific missions more than handling cyber weapons, and the fact that they consider cyberspace not so much as their own warfighting domain but rather as a critical enabler for intelligence and command and control of forces and operations.³⁶ Another reason is that, as part of the Department of the Navy, Marines' cyber and network issues may be handled by Navy personnel. It was also recently reported that one-third of the 1,000 Marine Corps' cyber forces expected to be on staff by 2016 will be contractors.³⁷

Conclusion and Future Directions

Today, the battle for the hearts and minds of the people around the world is being waged in the information environment with weapons that use information instead of physical means to compel decision makers to act. Cyberspace, with its lack of traditional geometry, represents perhaps the most malleable of operating environments. It is paramount for 21st century military leaders to become comfortable working and fighting in this domain.³⁸

Cyberspace has changed the character of national power, the structure of the international system, and the more traditional aspects of security and military affairs. Cyber instruments are being used as offensive weapons and tools of national power, covert action, espionage, terrorism, and crime. And as Chris Inglis, Deputy Director of the National Security Agency, recently stated "it's almost impossible to achieve a static advantage in cyberspace—whether that's a competitive advantage or a security advantage—when things change every minute of every hour of every day. And it's not just the technology that changes; it's the employment of that technology; the operations and practices."³⁹



Modern militaries rely almost exclusively on cyberspace to move information to decision makers—commanders and troops—control their weapons systems, and assure their situational awareness. This increasing dependence on cyberspace, alongside the growing array of cyber threats and vulnerabilities, adds new elements of risk to the nation’s security. Strong cybersecurity skills, the ability to obtain, process, analyze, manipulate, and correlate data, and the knowledge necessary to leverage cyberspace advantages to create effective strategies will be the deciding factor for military success and resiliency. Military leaders must become comfortable with the features of this realm—both human and technical—and understand the challenges, threats, and opportunities presented in cyberspace.

Military institutions of higher learning must be an incubator of these non-technical cyber leaders, blending theory and doctrine, with methodology, tools, and implementation, and aligning their curricula with the strategic goals of the nation’s cyber defense strategy. Cyber-strategic leadership is not the same, nor does it replace, the specific skills required to develop and administer the cyber environment. Rather it is the set of knowledge, skills, and attributes essential to future generations of leaders whose physical institutions nevertheless exist and operate in, through, and with the digital realm. A new cadre of cyber-strategic military leaders need not have specific training in engineering or programming, but they must be equipped with a deep understanding of the cyber context in which they operate, compounded with an appreciation of military ethics, strategic studies, political theory, institutional theory, international law, international relations, and additional sciences in order to harness the right tools, people, strategies, and balance of offensive and defensive capabilities.

This survey has highlighted an increased effort by military graduate programs to develop new content for cybersecurity education, include cyber components in existing curricula, and prepare senior officers to lead in a fundamentally different cyber age. Moreover, the expansion of most of these graduate programs to not only U.S. military officers, but also DoD civilian employees, U.S. federal agencies (Dept. of State, FBI, DHS), and international officers is a positive development in creating a more diverse learning environment where these professionals can share information and knowledge about cyber threats and learn to think outside the box. These efforts are commendable, especially in comparison to the much slower or nonexistent integration of cybersecurity components in non-technical graduate programs across American civilian universities. Despite these laudable developments, however, the survey has also illustrated that there still remains a significant imbalance between the evident need to educate all military leaders about the complexities of cyberspace and the marginal role that cybersecurity and cyber operations still play in some of the JPME institutions evaluated. The different level of exposure to cyber education can be quite striking when comparing some of these graduate programs that, at least in theory, should offer similar joint professional military education curricula.

Thus, JPME institutions must reorient their educational objectives and outcomes to better align their curricula with the strategic goals of the nation’s cyber defense strategy, and develop effective joint operational expertise and perspectives for the cyber realm. These revised programs should

comprise the study of cyberspace as a complex socio-technical system, where strategic and operational surprise may change traditional principles of war and military consequences, and an analysis of all the complexities residing in this strategic environment.⁴⁰ Additional steps should include identifying specific knowledge and skills required by military leaders in the cyber age, and recognizing existing gaps in traditional military thinking and current curricula when discussing cybersecurity and cyber operations. Charting a path to fill these gaps, and integrating best practices, core curriculum tenets, and minimum standards will be needed to create a comprehensive plan that can address cyber issues confronting the modern military. Inputs and support from experts—academics, researchers, industry professionals, and government officials—who have championed the development of cybersecurity leadership and cybersecurity programs will be critical.

America's future security hinges on its ability to prepare leaders for the challenges of the digital age. Efforts to use cyberspace for malicious purposes have matured in scope and sophistication over the past two decades; this threat will only intensify as non-state actors continue to embrace its low cost to entry and states operationalize cyber instruments as offensive weapons and tools of national power. The next generation of military personnel will need to be a nimble force able to wage full spectrum warfare from counterinsurgency in remote outposts in Afghanistan's tribal regions to a cyber warfare campaign possibly initiated by a state or non-state actor.⁴¹

The question will not be whether or not the U.S. can develop the best and most powerful cyber capabilities to accomplish a certain feat but whether our military—and our nation's leaders—will be equipped with knowledge necessary to confront a wide array of cyber threats and establish both a competitive and security advantage on the modern battlefield. Placing more emphasis on fully integrating cyber in existing JPME curricula and furthering the assimilation of cyber into the operational arena for every physical domain is imperative, and military institutions of higher education can no longer ignore the urgent need to adequately prepare America's next military leaders to meet those challenges.

Endnotes

1. Jim Michaels, "Pentagon Expands Cyber-Attack Capabilities," *USA Today* (April 21, 2013), <http://www.usatoday.com/story/news/nation/2013/04/21/pentagon-expanding-offensive-cyber-capabilities/2085135/>
2. Glenn Greenwald, "Obama Orders US to Draw Up Overseas Target List for Cyber-attacks," *The Guardian* (June 7, 2013), <http://www.guardian.co.uk/world/2013/jun/07/obama-china-targets-cyber-overseas>.
3. Michael N. Schmitt, "Cyber Operations and the Jus in Bello: Key Issues," *Naval War College International Law Studies* (March 2, 2011), <http://ssrn.com/abstract=1801176>
4. James R. Clapper, "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community," Office of the Director of National Intelligence (March 12, 2013), *Introduction*.
5. Jim Michaels, "General Says Cyberthreats are growing," *USA Today* (March 12, 2013), <http://www.usatoday.com/story/news/nation/2013/03/12/cyber-threat-alexander/1982115/>
6. President Barack Obama, "Remarks by the President on Securing Our Nation's Cyber Infrastructure," The White House (May 29, 2009), http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure



7. Adm. James Stavridis, "The Dark Side of Globalization," *The Washington Post* (May 31, 2013), http://articles.washingtonpost.com/2013-05-31/opinions/39658000_1_chemical-weapons-mass-destruction-cartels
 8. Lt. Gen. Michael Flynn, Third Annual Cybersecurity Symposium at the University of Rhode Island (May 3, 2013).
 9. Eric Beidel, "Military Academies Look to Fill Nation's Cybersecurity Gaps," *National Defense Magazine* (January 2012), <http://www.nationaldefensemagazine.org/archive/2012/January/Pages/MilitaryAcademiesLooktoFillNation%E2%80%99sCybersecurityGaps.aspx>
 10. John O'Callaghan, "Top U.S. Admiral Puts Cyber Security on the Navy's Radar," *Reuters* (May 13, 2013), <http://www.reuters.com/article/2013/05/13/us-usa-defence-cyber-idUSBRE94COB320130513>
 11. Ellen Nakashima, "Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies," *The Washington Post* (May 27, 2013).
 12. Michael J. Gross, "Silent War: The Changing and Terrifying Nature of the New Cyber-Warfare," *Vanity Fair* (July 2013).
 13. Chris C. Demchak, "Resilience, Disruption, and a "Cyber Westphalia": Options for National Security in a Cybered Conflict World," in Nicholas Burns and Jonathon Price, eds, *Securing Cyberspace: A New Domain for National Security*, Washington, DC: The Aspen Institute (2012), 59-94.
 14. Nancy Brown et al., "Creating Cyber Warriors," *Proceedings* (October 2012), 28-32.
 15. Jan Kallberg and Bhavani Thuraisingham, "Cyber Operations: Bridging from Concept to Cyber Superiority," *Joint Force Quarterly* 68, no.1 (January 2013), 53-58.
 16. Francesca Spidalieri, "One Leader at A Time: The Failure to Educate Future Leaders for an Age of Persistent Cyber Threat," *Pell Center Report* (March 26, 2013).
 17. Rhode Island Academic Collaboration on Cybersecurity Technology and Policy (September 13, 2011), <http://www.cs.brown.edu/people/jes/cyberpolicy.html>.
 18. Author's interview with Dr. Chris C. Demchak, U.S. Naval War College (May 24, 2012).
 19. U.S. Naval War College, Joint Professional Military Education, <http://www.usnwc.edu/Academics/Joint-Professional-Military-Edu.aspx>
 20. Dan McCauley, "The JPME Saga of Joe Etudiant," *Small Wars Journal* (April 1, 2013), <http://smallwarsjournal.com/jrnl/art/the-jpme-saga-of-joe-etudiant>
 21. Kallberg and Thuraisingham, "Cyber Operations," 54.
 22. Chris C. Demchak, "Hacking the Next War," *The American Interest*, vol. 8, no. 1 (September/October 2012)
 23. Chris C. Demchak, "Resilience, Disruption, and a "Cyber Westphalia," 62.
 24. Amber Corrin, "Service Academies Ramp Up Cyber Training," *FCW* (April 26, 2013), <http://fcw.com/articles/2013/04/26/cyber-training-academy.aspx>
 25. Chris C. Demchak, "Resilience and Cyberspace: Recognizing the Challenges of a Global Socio-Cyber Infrastructure (GSCI)" in Louise K. Comfort, ed., *Journal of Policy Analysis*, special issue "Designing Disaster Resilience and Public Policy: Comparative Perspectives, Part II," 14:3 (June 2012), 254-269.
 26. The National Security Agency (NSA) sets up the criteria for the designation of universities or academic departments as Center of Academic Excellence in Information Assurance Education (CAE/IAE) and CAE IA Research (CAE/R). The designation is valid for five academic years. The list of CAE institutions can be found at http://www.nsa.gov/ia/academic_outreach/nat_cae/institutions.shtml.
- The Likert scale is commonly used in survey research. This approach is usually used to measure respondents' attitudes by asking the extent to which they agree or disagree with a particular question or statement.
26. Author's interview with Lt. Col. Sean Kern, military faculty at National Defense University iCollege (April 18, 2013).
 28. For more information on the National Defense University iCollege' course offerings, see: http://www.ndu.edu/icollege/pdf/AY14/iCollegeSchedule_AY14.pdf
 29. Author's interview with Col. Nate Allen, military faculty at National Defense University iCollege (April 18, 2013).



30. Author's interview with Capt. Roy Petty, military faculty at the U.S. Naval War College (May 6, 2013).
31. The Tallinn Manual on the International Law Applicable to Cyber Warfare, written at the invitation of the NATO Cooperative Cyber Defence Center of Excellence by an independent 'International Group of Experts', is the result of a three-year effort to examine how extant international law norms apply to this 'new' form of warfare. Professor Michael N. Schmitt, Chairman and Professor in the Department of Law at the U.S. Naval War College, served as Director of the International Group of Experts tasked with crafting the Tallinn Manual.
32. For an overview of the specific activities that each of the CCTP institutions will undertake and their focus areas, see: <http://www.cs.brown.edu/people/jes/cyberpolicy.html>
33. Kenneth Stewart, "Cyber Ops Master's Degree Turns Senior Enlisted Into Cyberwar Specialists," Naval Postgraduate School of Public Affairs (June 7, 2013), http://www.navy.mil/submit/display.asp?story_id=74706
34. Author's interview with Lt Col Samuel Bass, student at the Air War College (May 15, 2013).
35. Author's interview with James Anderson, Dean of Academics and Deputy Director at the Marine Corps War College (May 2, 2013).
36. Dan Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," National Defense University
37. Aliya Sternstein, "Contractors to Handle Marines Corps' Cyber Arsenal," *NextGov* (June 10, 2013), <http://www.nextgov.com/defense/2013/06/contractors-handle-cyber-arsenal-marines/64607/?oref=ng-dropdown>
38. Richard Crowell, "War in the Information Age: A Primer for Cyberspace Operations in 21st Century Warfare," *Naval War College* (2010), 4.
39. Colin Clark, "NSA Deputy Warns Against Cyber Vigilantes; CISP Execution Must Be 'Exactly Right,'" *Breaking Defense* (May 22, 2013), <http://breakingdefense.com/2013/05/22/nsa-deputy-warns-against-cyber-vigilantes-cispa-execution-must-be-exactly-right>
40. One of the courses that offers such a systemic approach to the study of cyberspace, encompassing most of the topics discussed in this report, is: "Cybersecurity: Cybered Conflict, Response to Surprise, and Emerging Indicators of Global System Change," taught by Dr. Chris C. Demchak at the U.S. Naval War College.
41. Tim Hsia and Jared Sperli, "How Cyberwarfare and Drones Have Revolutionized Warfare," *The New York Times* (June 17, 2013) <http://atwar.blogs.nytimes.com/2013/06/17/how-cyberwarfare-and-drones-have-revolutionized-warfare/?smid=tw-share>



www.salve.edu/pellcenter

ABOUT THE PELL CENTER

The Pell Center for International Relations and Public Policy at Salve Regina University is a multi-disciplinary research center focused at the intersection of politics, policies, and ideas. Dedicated to honoring Senator Pell's legacy, the Center promotes American engagement in the world, effective government at home, and civic participation by all Americans.

PELL CENTER
for INTERNATIONAL RELATIONS
and PUBLIC POLICY

