Transforming the Next Generation of Military Leaders into Cyber-Strategic Leaders: The role of cybersecurity education in US service academies

Francesca Spidalieri
Jennifer McArdle

Information communication technologies (ICTs) have become the foundation—both the bone marrow and connective tissue—of modern militaries. Satellites, precision guided munitions, nuclear launch systems, helicopters, and any number of other weapon platforms are reliant on ICTs for their operational capability and connectivity. No modern military can enter the battlespace without some reliance on cyberspace for their land, sea, air, space, or information operations. Moreover, the 'battlespace' is no longer reserved solely for 'war time'. Cyberspace has blurred the lines between traditional conflict and peace, and states are finding themselves in a position of protracted, low-level conflict in the cyber realm. While this conflict often takes the form of cyber crime, cyber espionage or service disruption, the specter of a large-scale armed conflict conducted wholly or partially in cyberspace, continues to rise. [1] And while cybersecurity is not solely a defense challenge, the US military's increasing reliance on cyberspace, alongside the growing array of cyber threats and vulnerabilities, has made securing this space and establishing a competitive advantage on the modern battlefield a leading priority for any military in the 21st century.

In response to the proliferation of cyber threats, the White House raised the US Department of Defense (DoD) FY2016 cyber budget to $9.5 billion, an 11 percent increase in spending over FY2015. [2] The recently published DoD Cyber Strategy seeks to strengthen the US' cyber defense and deterrence posture by building cyber capabilities and organizations around three critical cyber missions: the defense of DoD networks, systems, and information; the defense of the US and its interests against cyber attacks of significant consequence; and the provision of cyber capabilities to support military operations and contingency plans. Despite a stated emphasis on defense and deterrence, the document also highlights the wide arsenal of DoD's offensive cyber capabilities that could be employed in the event of a conflict. [3]

Francesca Spidalieri is the Senior Fellow for Cyber Leadership at the Pell Center for International Relations and Public Policy at Salve Regina University, where she leads the Cyber Leadership Research Project and the Rhode Island Corporate Cybersecurity Initiative (RICCI). Francesca has been appointed by Governor Gina Raimondo to the Rhode Island Cybersecurity Commission, and serves also as subject-matter expert for the Potomac Institute for Policy Studies' Cyber Readiness Index Project, the Center for Internet Security's Roles & Controls Panel, and the Ponemon Institute. Her academic research and publications have focused on cyber leadership development, cyber risk management, cyber education and awareness, cybersecurity workforce development, and the professionalization of the cybersecurity industry.

She holds a B.A. in Political Science and International Relations from the University of Milan, Italy; and an M.A. in International Affairs and Security Studies from the Fletcher School at Tufts University.

Strategy and funding alone, however, are not sufficient to achieve a fully capable military force. The military must also have highly-trained, cyber-capable personnel and leadership prepared to meet tomorrow's challenges today.[4] As Representative Jim Langevin stated:

> The greatest challenged faced by the Department of Defense—and the entire government enterprise—is human resources. Technological dominance is meaningless without a skilled workforce capable of operating at the highest level of their field. In this area, we are falling short.[5]

This article addresses the role that US service academies play in developing not only future cyber forces, but also a pipeline of qualified cyber-strategic military leaders, who have the knowledge necessary to confront a wide array of cyber threats and establish both a competitive and security advantage in the modern battlespace. In the future, *every military leader must be a cyber-strategic leader.* In particular, this study surveys current efforts by the US Coast Guard Academy, the US Air Force Academy, the US Military Academy, and the US Naval Academy to prepare all their future officers for the challenges of operational- and strategic-level leadership in an age of persistent cyber threat.[6] This survey provides an overview of the level of exposure to cyber issues that cadets and midshipmen receive during their undergraduate studies at the service academies, and to what extent they graduate with an adequate understanding of the cyber challenges facing their respective services. Lastly, this article identifies some of the gaps in the existing curricula and offers preliminary recommendations to include a stronger cybersecurity component into current programs.

Jennifer McArdle is a Fellow in the Center for Revolutionary Scientific Thought at the Potomac Institute for Policy Studies. She leads a program on simulation and virtual reality for next generation warfare and also serves as a subject matter expert on the Potomac Institute for Policy Studies' Cyber Readiness Index Project. Her academic research focuses on potentialities for inadvertent escalation from "cyber warfare," national security, and military innovation. Her work has featured in outlets such as Real Clear World, The National Interest, National Defense Magazine, GovInfoSecurity, among others.

Ms. McArdle is a Ph.D. candidate in War Studies at King's College London. She holds a M.Phil in Politics from the University of Cambridge and a B.A. in Political Science and Justice Studies, summa cum laude, from the University of New Hampshire.

The Next Generation of Military Leaders Must Also Be Cyber-Strategic Leaders

The growing scope, pace, volume, and sophistication of cyber threats, and the development of cyber tools as technical weapons have been accompanied by another realization: there are few people, whether civilian or military, equipped with knowledge sufficient to protect the nation's critical infrastructure and sensitive information, improve resiliency, and leverage information technology for strategic advantage.[7] As a result, government efforts to provide cyber training for civilian and military personnel, and to create a specialized cyber workforce have become increasingly important to national security.[8]

Indeed, out of the FY2016 DoD cyber budget, $500 million have been specifically allocated for the implementation and support of Cyber Mission Forces (CMF) tasked with training and supporting cyber personnel, both civilian and military.[9] CMF, unveiled in 2013, plans to add approximately 6,000 people split between three cyber forces, each with specific missions: defense of the nation from foreign adversaries; cyber support of the combatant commands; and protection of military networks and, when authorized, other infrastructure.[10] Thus, DoD's main efforts in this area have been largely focused on training cyber warriors, those highly specialized individuals with extensive technical training who can engage in the defensive and offensive cyber operations critical to mission effectiveness.[11] As Secretary of Defense Ash Carter noted during a recent speech in Silicon Valley, the CMF are far more valuable than the technology they use, and the DoD's "first strategic goal is building [these] Cyber Mission Forces."[12]

Compounding the shortage of highly trained cyber forces, are the increasing scale, complexity, and continuous growth of DoD networks that are providing new avenues for adversary exploitation. In 2011, the DoD cyberspace architecture was already the largest in the world, including over 15,000 networks and seven million computing devices spread across hundreds of installations globally.[13] Today, the networks continue to expand adding new features and assimilating new technologies, such as mobile devices and cloud computing.[14] Moreover, the weapons platforms that are critical to national security and deterrence: nuclear weapons, cruise and ballistic missiles, helicopters, fighter aircraft, and any number of other systems including precision guided weapons are dependent on the reliance and functionality of microelectronics, or chips, which make up the cyber hardware of the system.[15] Thus, every member of the US military regardless of whether they are in the infantry, surface warfare, logistics, maintenance, or even the chaplaincy will need some degree of cyber know-how. ICTs are already intrinsically linked to most components of military careers and missions. As the Deputy Director of the Army Cyber Institute, Dr. Fernando Maymí, stated "it will be impossible for any future leader not to acknowledge cyber issues in their decision-making process."[16] Therefore, it is increasingly important that all military leaders, regardless of their specialty, have the requisite knowledge, technical acumen, and strategic vision to lead their Soldiers, Sailors, Airmen, and Marines into a battlespace that is increasingly dominated by technology.

> This article identifies some of the gaps in existing service academy curricula and offers preliminary recommendations to include a stronger cybersecurity component into current programs.

Yet, while DoD's efforts to create a capable cyber workforce are commendable, we cannot expect the new cyber forces to be the only ones in charge of preventing, mitigating, and containing cyber threats, nor will advanced technology alone be sufficient to protect all of DoD's networks and digital assets. There needs to be a concerted effort to develop a new generation of cyber-strategic leaders who will lead, manage, and oversee cyber defense and cyber operations in this dynamic and ever-changing digital environment. 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, complimented by an appreciation of military ethics, strategic studies, political theory, organizational theory, history, international law, international relations, and additional sciences.[17] Indeed, future cyber-strategic leaders should extend beyond so-called "cyber warriors." Every future military leader must be a cyber-strategic leader.

The Role of the Service Academies in Preparing Leaders for an Age of Persistent Cyber Threat

The first step in the creation of both cyber warriors and a new cadre of cyber-strategic leaders is education, both at the undergraduate and graduate level. However, as the National Research Council has observed, “cybersecurity is a complex subject whose understanding requires knowledge and expertise from multiple disciplines, including but not limited to computer science and information technology, psychology, economics, organizational behavior, political science, engineering, sociology, decision sciences, international relations, and law.”[18] Universities, colleges, and in this case service academies, are best fit to serve as incubators of cyber-strategic leaders, “bringing together theory and doctrine, with methodology, tools, and implementation.”[19] Cyber-strategic leadership, in fact, is not the same as, nor does it replace, the specific technical skills, knowledge, and abilities required to develop, administer, and defend the cyber environment. Rather it is a different and complimentary set of skills, knowledge, and attributes essential to future generations of leaders whose physical institutions nevertheless exist and operate in, through, and with the digital realm.

> In the future, every military leader must be a cyber-strategic leader.

Service academies and war colleges in particular ought to play a key role in educating future and current 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 of the study of cybersecurity. In fact, 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. Only a truly comprehensive education will help foster the requisite military leadership needed to fight and win in a deeply cybered and conflict prone world.[20]

Despite the pressing need to educate future cyber-strategic leaders across the whole range of social institutions and military services, few American universities, colleges, and academies offer courses or degree programs that combine cybersecurity technology, policy, law, economics, ethics, and other social sciences, and even fewer encourage collaboration among departments and other academic institutions to optimize their efforts and insights available for cross-fertilization.[21] Current cybersecurity programs, should be expanded and incorporated into all major technical and non-technical academic programs if we are to create a new cadre of cyber-strategic leaders spanning different sectors of society.

Efforts are already underway at military academies to educate and train select groups of students in information assurance, and cyber operations and to fill the ranks of the new cyber corps. In 2012, for instance, service academies founded a "Military Academy Cyber Education Working Group," which consists of members from the four main US service academies: the US Coast Guard Academy, the US Air Force Academy, the US Military Academy, the US Naval Academy, the Naval Postgraduate School, the Air Force Institute of Technology, US Cyber Command, and the National Security Agency (NSA). This group has sought to develop a body of knowledge for undergraduate cyber education for future officers, cyber leaders, and technical personnel.[22] Some of the academies are also involved in the Cyber Education Project (CEP), a other effort by computing professionals at different academic institutions to "develop undergraduate curriculum guidelines and a case for accreditation for educational programs in the cyber sciences."[23] Despite these efforts, however, most of the existing academic programs remain highly technical and rarely pursue broader multi-disciplinary approaches commensurate with the complexity of cybersecurity. Indeed, there remains much to be done to fill this education gap and establish standardized core curricula in information technology and cybersecurity for all service academies.

What we need are the "academies of cybersecurity," where different aspects of cybersecurity are an integral component of any cadet, midshipmen, and officer's military education and training, while also being fully integrated with more traditional missions. Service academies and professional military education are instrumental in creating a new cadre of cyber-strategic leaders. After all, these institutions are designed specifically to educate, train, and produce the future top military leaders and strategists who will have the skills, knowledge, and strategic acumen needed to take leadership roles on the battlefield, as well as in government agencies, and other military installations. There exists no group with a more urgent need for understanding cyber-related 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.[24]

Methodology[25]

This study summarizes current efforts by US service academies to include information technology or cybersecurity education in their curricula. It seeks to highlight those cyber components already present in updated curricula, review program effectiveness in promoting the study of cybersecurity and cyber warfare, and identify existing curriculum gaps in this field. This article does not provide an in-depth analysis of specific courses or an extensive audit of particular programs; rather, it offers an overview of the progress, or lack thereof, made by service academies to integrate information technology and cybersecurity into their programs and extracurricular activities.

The survey findings are based on data collected between November 2015 and February 2016. The data was obtained through a combination of interviews with service academy faculty and staff, in addition to material drawn from their websites. The results stem from the responses to four main curriculum and extracurricular questions, and the use of a modified Likert approach [26] to evaluate the level of exposure students receive to cybersecurity issues in each of the service academies, and the opportunities offered to deepen their knowledge in the field. Respondents were asked whether their institution offered: 1) dedicated degree majors and/or core courses in information technology and cybersecurity; 2) elective courses in information technology and cybersecurity open to all students, regardless of major; 3) the possibility for cadets or midshipman to cross-register and enroll in other elective courses in information technology and cybersecurity at other schools; and 4) occasional seminars, conferences, war gaming exercises, or other training opportunities in cybersecurity and/or cyber operations. The modified Likert scale used to derive a notional ranking of the academies 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 added, and each service academy 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 article.

> There needs to be a concerted effort to develop a new generation of cyber-strategic leaders who will lead, manage, and oversee cyber defense.

The authors assume that if a service academy requires all students to take at least one core course in ICT and cybersecurity, all cadets or midshipman will receive at least a basic understanding and the practical tools needed to manage the information security needs of their armed service and leverage ICTs for strategic advantage. If the academy offers elective courses in ICT or cybersecurity, cadets and midshipman interested in these topics will at least have the opportunity to explore the interlinkages between ICT, cybersecurity, and military readiness. If cybersecurity issues are covered as part of broader courses, we assume that students will gain a general understanding of the cyber challenges and opportunities specific to that field of study. Finally, if the academy offers occasional cyber-related seminars, conferences, war gaming exercises, visits to cyber units within different services, and the option of participation in cyber competitions, cadets and midshipman will have the opportunity to explore cybersecurity in more depth, and with a greater level of hands-on practicality. 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 persistent in cyberspace beyond their own personal experience.

In addition, the study indicates whether the service academies have received the NSA/Department of Homeland Security (DHS) designation as a Center of Academic Excellence in Information Assurance Education (CAE/IAE) and Research (CAE/R).[27] The goal of these programs is to reduce vulnerability in the national information infrastructure by promoting higher education and research in IA, and producing a growing number of professionals with IA expertise in various disciplines. Students attending designated schools are eligible to apply for scholarships and grants through the DoD Information Assurance Scholarship Program and the Federal Cyber Service Scholarship for Service Program.

SERVICE ACADEMIES SURVEY

Service Academy	City	State	Likert Scale Average Score (Max = 4)	NSA/DHS Certification*
United States Air Force Academy	Colorado Springs	CO	3	CAE/IAE
United States Coast Guard Academy	New London	CT	2.5	N/A
United States Military Academy	West Point	NY	3.5	CAE/IAE
United States Naval Academy	Annapolis	MD	4	CAE/IAE

* Indicates academy NSA/DHS designation as a Center of Academic Excellence (CAE) in Information Assurance Education (IAE) and/or Research (R).

United States Air Force Academy	Colorado Springs, CO
Likert Score: 3/4	NSA Cert: CAE/IAE

The Air Force was the first branch to recognize cyberspace as an operational domain, and to incorporate large portions of the Air Force's intelligence units for network warfare along with the communications units under the 24th Air Force (a component of Air Force Space Command). This operational warfighting organization is tasked with executing full spectrum cyberspace operations.[28] Consequently, the US Air Force Academy (USAFA) incorporated some aspects of cybersecurity and cyber warfare education in its curricula, and has tried to align its offerings with the new career paths and fields created for Airmen.

Recently, USAFA instituted a new computer network security major designed specifically to help cadets better understand and gain proficiency in cyberspace.[29] The new major focuses on computer programming, embedded systems, networks, telecommunications, computer systems, computer investigations, and cyber operations. Although this program is highly technical and targeted at students aspiring to develop cyber expertise—either working in the cyber domain or becoming pilots with an in-depth knowledge of the software systems that underpin aircraft and weapons systems—students are also required to take one course on either strategy, political science, or cyber law. Moreover, the major includes a capstone project where students participate in a final hands-on exercise that includes red and blue team forces competing against military and external institutions, as Major Michael Chiaramonte explained.[30]

In addition, all cadets, regardless of their major, are required to take an Introduction to Computing course during their freshman year, which covers cybersecurity, cyber hygiene, cyber threats, and the supporting role of information technology in the planning and execution of national and military strategy. All cadets also take an electrical engineering course, which includes four lessons on cybersecurity. USAFA offers a few cyber-related electives, enabling students to delve deeper in other non-technical areas such as cybersecurity policy and politics, cyber law, military strategic studies, information and cyberspace operations, and, soon, digital forensics (the course is scheduled to start in Fall 2016). While the academy does not currently allow students to take additional courses on cybersecurity at other schools, they are considering offering this opportunity in a hybrid online format.

Moreover, cadets interested in this field can join the school's extracurricular cyber warfare club and the cyber competition team to gain further exposure to a variety of cyber threats facing military and government networks, and to get hands-on experience with simulated offensive and defensive cyber operations. Every year, students on the cyber team participate in numerous competitions and various capture the flag exercises against graduate students and professionals worldwide, frequently ranking among the top 10 percent of teams.

Finally, USAFA's Center of Innovation provides additional opportunities for some students to study malware and other complex computer security issues alongside faculty and researchers from Intel Corporation (the center serves as a testing ground for Intel Corporation's most promising new technologies).[31] The Center has recently started to explore how disruptive technology innovations can change the way the military operates, and how innovations in cyberspace can revolutionize cybersecurity for both the military and businesses.

From the information provided, all students at the Air Force Academy receive at least a basic foundation and understanding of information technology and cyber warfare during their freshman year, and have the opportunity to be further exposed to the cyber risks that may impact mission capabilities and effectiveness through cybersecurity competitions and events. Those particularly interested in the study of cyberspace and cyber operations can pursue a Bachelor of Science degree in computer and network security. However, this is a challenging program that requires strong quantitative and analytical skills and a predisposition for computer programming. Given the time demands and stressors of academy life, only a limited number of dedicated students actively pursue this degree.

United States Coast Guard Academy	New London, CT
Likert Score: 2.5/4	NSA Cert: N/A

The US Coast Guard Academy (CGA) educates future leaders to serve in a multi-mission maritime force, tasked with providing critical services in protection of natural resources, maritime mobility, and national defense. A new core curriculum has recently been approved for the class of 2021, which will require all cadets, regardless of their major, to enroll in a cybersecurity fundamentals core course. However, at present, CGA only offers core courses with a cybersecurity focus for students in specific majors. For example, electrical engineering majors with a key competency in computers are required to take a Computer and Network Security course. The course expands on the skills, knowledge, and abilities acquired during the pre-requisite courses on Introduction to Computer Programming and Computer Communications and Networking, which introduce students to the fundamentals of computer and network security, including threats, vulnerabilities, exploits, intrusion protection systems, firewalls, cryptography, and mechanisms to mitigate risks. The course is also offered as an elective to electrical engineering majors with a systems emphasis. Students that partake in the course also have the opportunity to place “their education into practice as participants in the NSA’s annual Cyber Defense Exercise (CDX),” in which students from service academies design and build computer networks and defend them against intrusions by the NSA and the Central Security Service (CSS).[32] Likewise, students enrolled in the management major are required to take a Management Information Systems course, which prepares managers to function in a technological environment. Students are taught about the structure of information systems, management of computing technology, data processing, and information assurance.[33] Cadets can also choose to take two electives, either Information Technology in Organizations or Cybersecurity Crisis Management. The first elective provides students with an in-depth examination of fundamental technological and management issues relevant to information technology management in the Coast Guard, including computer architecture, network theory, and system administration.[34] The second course is a newly developed course, which “provides students with an interdisciplinary approach to understanding key systemic challenges associated with effective leadership and management of cyber-related incidents,” as Dr. Kimberly Young-McLear explained.[35] Although the course is offered in the management department, it is open to all majors. Topics include legal, policy, network defense, business continuity planning, and risk management. The course also features guest speakers and lecturers from the Coast Guard and other governmental agencies. Students in the course, as well as selected students from other majors, have the opportunity to participate in a two-day cybersecurity seminar in Washington D.C. offered through the Coast Guard Academy's Institute for Leadership. During this field trip, cadets are provided cybersecurity guidance from senior government officials at the White House, Pentagon, Coast Guard Headquarters, and the National Cybersecurity and Communications Integration Center (NCCIC).

In addition, all students in their senior year are required to take a Public Management Consulting course, which provides students with an experience-based project to apply management and business principles, including cyber-related ones, to their final capstone. For instance, the management department has provided several opportunities for students to work on cybersecurity and information technology-related capstones. Clients have included DHS, Coast Guard Port and Facilities Compliance, and the Surface Forces Logistics Center.[36]

Other majors offer additional elective courses that cover some cybersecurity and/or information assurance topics as part of the broader course curriculum. For example, students in the government program have the option of taking an Intelligence and Democracy course, which examines various functions of intelligence from a human and technical perspective, and a Strategic Intelligence: Collection and Analysis course that explores how the Intelligence Community operates, from both a technical and human level.[37] Moreover, CGA participates in the Service Academy Exchange Program (SEAP) that allows cadets to participate in a semester-long exchange program with one of the other service academies. While this program is not specifically focused on cybersecurity, students could theoretically take a cybersecurity course offering at another academy to fulfill an elective requirement at CGA. Cadets also have the opportunity to take courses at the nearby Connecticut College to enhance the available offerings, as Dr. Kelly Seals explained.[38]

> Only a truly comprehensive education will help foster the requisite military leadership needed to fight and win in a deeply cybered and conflict prone world.

In 2015, CGA developed a new initiative to raise awareness among cadets of the importance of maintaining cybersecurity. The new cyber defense awareness training module is a three-day Cyber Range for all cadets to take part in during their second class summer. Cadets are trained in cybersecurity issues and have the opportunity to be exposed to live malware and experience the effects of poor cyber hygiene in a safe, segregated network environment.[39] The academy's cadets have also recently formed a cyber team and participated in the annual CyberStakes competition, a DoD program originally launched by the Defense Advanced Research Projects Agency (DARPA) to build cyber proficiency in service academy midshipmen and cadets.[40] The CGA 'hacking' team offers cadets the opportunity to deepen their knowledge of computer networks while earning sports credits for their participation.[41]

Finally, the academy offers occasional conferences and guest lectures on cybersecurity. In the spring of 2015, for instance, the academy held a day-long cyber symposium with external cybersecurity experts from the military, government, academia, and industry. Topics ranged from cyber resiliency and the US maritime transportation system, to cyber intelligence policy, to insider threats.[42]

In brief, cadets at the Coast Guard Academy have the opportunity to be exposed to cybersecurity and information assurance through multiple extracurricular activities, and some courses depending on their major. CGA has recently made additional efforts to increase opportunities for cadets to acquire "the cybersecurity knowledge, skills, and abilities necessary to operate within the cyber domain and to be leaders in protecting maritime critical infrastructure and the maritime transportation system."[43] As part of this effort, more courses could be offered outside of the electric engineering and management programs that explore the legal, ethical, economic, and policy implications of cybersecurity, and cadets could be encouraged to enroll or audit additional cybersecurity electives outside their major.

United States Military Academy	West Point, NY
Likert Score: 3.5/4	NSA Cert: CAE/IAE

The US Military Academy at West Point is dedicated to educating and training future Army officers with a focus on leadership development through academic, military, and physical education. All cadets are required to complete a core curriculum of 26 courses, which includes an introductory course in computing and information technology during their freshman year. While not entirely focused on cybersecurity, this course has a self-defense and protection focus and seeks to train students on mechanisms by which they can be responsible citizens in cyberspace. As the 2016 course catalog notes, the "core curriculum includes a computer science thread to ensure that every academy graduate is comfortable with and capable of using computers in an Army dependent on technology."[44] Additionally, as part of the core curriculum, every cadet is required to select a core-engineering component that consists of three tailored engineering courses. One of the options is a cyber engineering sequence, which has become one of the more popular options among cadets.

West Point also has a number of computing and engineering majors that include substantive cybersecurity components. As Dr. Fernando Maymí explained, "although West Point does not offer a cybersecurity major, we strive to foster a cybersecurity focus within the population of cadets who are majoring in computer science, information technology, electric engineering, systems engineering, and mathematics." [45] Students who are not majoring in one of these more technical majors are also required to take a second intermediate-level information technology course, which devotes a third of the classes to information assurance and security. The course culminates in a series of lessons that allow students to conduct computer reconnaissance, defense, and offense within a virtual network environment. [46] Furthermore, cadets can select a minor in cybersecurity, which includes courses in Cyber Security Engineering and Cyber Operations, among others. The cyber operations course offers a mature multi-disciplinary approach to cyber warfare, by covering the entire spectrum of legal, political, and ethical implications of information communication technology, cyber techniques, and attacks. [47] For cadets with an interest in cybersecurity, West Point also lines up a Senior Research Project (fall and spring semester) with a focus on software and systems development. The goal is that by the time those cadets graduate, typically about 15 per year, they will be ready to take operational assignments in this field. [48]

All students interested in cyber-related matters can take additional courses in technical disciplines or choose from a set of multi-disciplinary electives that include cyber warfare, law, ethics, digital forensics, and policy issues. This multi-disciplinary approach to the study of cybersecurity is the cornerstone of West Point's strategy with the academy striving to include a stronger cyber component in most of its academic programs. While West Point does not offer students the ability to cross-register at other schools to include additional courses in cybersecurity in their curriculum, it does encourage students to apply for semesters abroad with a variety of foreign universities, and to participate in the SEAP exchange programs with another service academy. Theoretically cadets could augment their West Point education with courses in cybersecurity during their time abroad or through the SEAP program. [49]

Outside of formal course offerings, West Point offers a wide variety of extracurricular activities to enhance cadets' experience and exposure to cybersecurity-related issues. For instance, the Cyber Research Center, housed in the Department of Electrical Engineering and Computer Science, provides research and educational opportunities for cadets and faculty to delve deeper into cyber-related subjects, including information assurance, information warfare, and forensics. The Center is involved throughout the year in annual cadet programs such as a cadet senior design capstone project management, an annual Cyber Defense Competition, cadet trip sections, annual summer internships, and cadet mentorships. [50] Cadets have the opportunity to participate in the Cadet Competitive

Cyber Team (C3T); a competitive academic team whose primary mission is to prepare for, and compete in, undergraduate cybersecurity competitions. C3T has participated in the Service Academy Cyber Stakes, sponsored by DARPA, and various capture the flag exercises, such as the 10th Annual NYU-Poly Cyber Security Awareness Capture the Flag competition.[51] In addition, a local chapter of the Association for Computing Machinery Security, Audit and Control (SIGSAC) Club is open to all students and provides cadets hand-on cyber experience in a secure (air gapped) environment.[52]

Moreover, West Point hosts a distinguished lecture series with cybersecurity luminaries, including senior military, and government officials and executive-level guest speakers from the US private sector, to discuss cyber threats to national security and the economy. Similarly, core and elective courses with a cybersecurity component often include guest lecturers. Those special lectures are usually scheduled during a common lecture hour so that participation can be opened to cadets that are not enrolled in those courses. For example, last year they hosted General Michael Hayden, former NSA and Central Intelligence Agency Directory, and Dr. Chris Soghoian, Chief Technologist at the American Civil Liberties Union, for a discussion on privacy issues and bulk data collection.[53]

West Point offers a wide variety of extracurricular activities to enhance cadets' experience and exposure to cyber-security-related issues.

Finally, West Point is home to the Army Cyber Institute (ACI), whose mission is to develop intellectual capital and impactful cybersecurity partnerships for the Army and the nation to further cyberspace defense. Unlike the Cyber Research Center, the ACI is outward facing; they work with academia, government agencies, and industry in order to identify and build partnerships between individuals and organizations with cybersecurity challenges and potential solution sets.[54] The ACI runs a Cyber Leader Development (CLDP) program, which provides cadets an additional 800+ hours of impactful experiences outside the classroom through one-on-one mentorship, internships, conferences, clubs, and seminars. Cadets in CLDP have the opportunity to pursue advanced training—learning how to hack and defend networks—through SANS, Cisco, and other organizations during their spring break. CLDP includes field trips to the NSA, where cadets participate in a series of day-long discussions on cyberspace issues at the secret-level. At present, 160 cadets are enrolled in the program.[55]

The US Military Academy provides several opportunities for students to develop knowledge and skills in information technology and cybersecurity. West Point has taken a multi-disciplinary approach to cybersecurity and recognizes the need for all military officers and decision-makers to have a basic understanding of the macro and micro implications of cyber issues. Despite their current efforts, however, cyber education has yet to be incorporated in all academic departments. Nonetheless, opportunity exists at West Point—particularly through the ACI—to deepen engagement with all faculty and departments, and offer additional cybersecurity and information assurance coursework in other academic focal areas (majors and minors). Moreover, as West Point develops more cybersecurity offerings, such as cyber ethics and cyber law, an inter-disciplinary major could be created that spans the technical and social science communities.

United States Naval Academy	Annapolis, MD
Likert Score: 4/4	NSA Cert: CAE/IAE

The US Naval Academy (USNA) provides academic and professional training for midshipmen that will become professional officers in the US Navy and Marine Corps. The academic programs at USNA are focused "especially on science, technology, engineering, and mathematics (STEM), in order to meet the current and future highly technical needs of the Navy." [56] All midshipmen receive a Bachelor of Science upon graduation regardless of their major due to the technical content of the core curriculum.

In 2013, USNA became the first service academy, or university for that matter, to offer a dedicated Cyber Operations major at the undergraduate level, in addition to the more technical majors in Information Technology, Computer Science, and Computer Engineering. While fundamentals of the program will remain the same, the new Cyber Operations major has been designed to be updated and adapted over time as new technological innovations continue to develop, and to ensure students stay up to date with the latest technologies, explained Andrew Phillips, USNA Dean and Provost. [57] The Naval Academy's Class of 2016 will be the first to graduate with the Cyber Operations degree. USNA was also the first of the service academies to require all students to take two mandatory courses in cybersecurity, an introduction during their freshman year, and a more in-depth elective that includes cyber policy and economics during their junior year. The two core courses provide a comprehensive overview of the principles behind the use, function, and operations of computers, networks, and applications with an emphasis on cybersecurity. "Both courses also include laboratory hours to emphasize some of the concepts into practical applications," explained Captain Paul Tortora, Director of the USNA Center for Cyber Security Studies. [58]

Students interested in cyber-related issues can also choose from a variety of dedicated electives (regardless of their major), from more technical courses, such as Cyber Physical

Systems, Computer Networks with Security Applications, and Cryptology and Information Security, to more policy and strategy based, such as Cyber War Strategy, Information Technology and International Politics, Cyber Planning & Policy, Cyber Law & Ethics, Emerging Technologies, and Social Engineering, Hacktivism, and Info Ops in Cyber.[59] While most of these electives have prerequisites, the individual instructors can waive them should the student already possess the requisite knowledge.[60] Through these courses, students can gain a thorough understanding of the information system; the technical, social, policy, and institutional aspects of cybersecurity; the political and economic frameworks of cyber power; the legal and ethical challenges of cyber operations; the social engineering techniques and non-standard approaches employed by cyber threat actors to gain technical, military, economic, and intellectual advantages in cyberspace; and the effects of information technology on both the national and international political systems; and other aspects of the information revolution on the relations among nations. In addition, the cyber policy class runs a tabletop cyber exercise as part of the final class segment, both for students in Cyber Operations and Political Science, and International Relations majors.

Select senior students have an opportunity to cross-register at other schools to pursue additional cybersecurity courses, but only during their final/Spring semester. USNA has a Trident Scholar Program, which allows students to carry out independent study and local research, and a Voluntary Graduate Education Program (VGEP), which provides an opportunity for high-achieving midshipman to accelerate their undergraduate degree and take graduate classes at local elite universities, such as John Hopkins, Georgetown University, and the University of Maryland, during their final year. However, students must first finish all their undergraduate requirements and then be able to complete their graduate study within 7 months of graduation.[61] In addition, USNA enrolls about 10 to 15 students in SANS cybersecurity courses when available, typically during school breaks such as Spring Break or over the summer. Students majoring in Cyber Operations also have the opportunity to complete summer internships with civilian software and Internet companies as well as the NSA.

Beyond the classroom, midshipman can take advantage of the numerous cyber-related conferences, seminars, and small-scale cyber competitions hosted at the USNA. The Naval Academy also has a very active cyber competition team, which participates in a broad spectrum of cyber competitions, capture-the-flag events, and the annual NSA-sponsored CDX exercise. The USNA team won the last CDX exercise in the spring of 2015, and was recognized by President Obama at the White House, and also met with members of the National Security Council for cybersecurity discussions.[62]

USNA has also received $120 million in federal funding and a $1 million gift from Microsoft to build and equip a new cyber center (expected to be completed by late 2018) that will feature 206,000 square feet of secure classrooms, research labs, lecture halls, state of the art technology, and the Academy's first Sensitive Compartmented Information Facility, or SCIF, a secure space that will allow for the discussion and management of classified materials.[63] The new building will be the home for the academy's Center for Cyber Security Studies, which provides support for the development of the cybersecurity curriculum, and for all the programs that contribute to knowledge, study, and research of cyber warfare at the USNA.[64]

Finally, USNA recently signed a new three-year, federally funded research partnership with the University of Maryland, Baltimore County, which will expand opportunities for both students and faculty to work on five major cybersecurity projects, including research to: detect hacks; strengthen the security of cloud-storage systems; develop hardware to detect anomalies and signal breaches; fortify defenses of social-media systems; and protect cell phones without burdening users.[65]

All midshipmen at the US Naval Academy receive at least a basic understanding of the full spectrum of cybersecurity issues from technical to strategic leadership, and the practical knowledge needed to integrate cyber capabilities and cyber operations with the broader needs and missions of the US Navy. In fact, although the core curriculum at the USNA seems highly focused on science and technology, it has actually incorporated a significant number of policy, legal, sociological, and institutional components to the study of cybersecurity. Together with the more technical aspects of cybersecurity, the various programs and extracurricular activities at the Naval Academy are preparing the next generation of cyber-strategic leaders for the Navy and a select group of naval officers with an in-depth expertise and experience in cybersecurity and cyber warfare. In addition, the academy's location in Maryland—a valued contributor to national cybersecurity and a trendsetter among states leading the cyber pack—and its proximity to the state's world-class educational institutions, leading federal assets, and a dynamic private sector are providing students and faculty additional research, training, and educational opportunities in this field.[66] Despite the clear strengths of the USNA programs, continuous emphasis should be placed on integrating an even more robust cybersecurity component into broader midshipman coursework.

> Only then will this new cadre of cyber-strategic military leaders be able to harness the right tools, people, strategies, and balance of offensive and defensive capabilities.

Conclusion and Future Direction

The use of ICTs has become the most dominant trend in interstate competition in the 21st century, whether in times of peace, tension, or open conflict. ICTs have become the foundation of modern militaries—from the hardware and software that underpin all military platforms, to the communication systems used to move information to commanders and troops, to the digital devices needed to control weapons systems, assure situational awareness, gather intelligence, and project force. Today, no modern military can enter the battlespace without some reliance on ICTs and cyberspace.

Given this undeniable and critical reliance on cyberspace for achieving military success, all future military leaders must be comfortable operating in this space, from both a human and technical perspective, and understand the challenges, threats, and opportunities it presents. Strong cybersecurity skills, the ability to obtain, process, analyze, manipulate, and correlate data, and the knowledge necessary to leverage cyberspace for strategic advantage will be the deciding factor for military success and resiliency. For these reasons, every future military leader must be a cyber-strategic leader. These individuals need not have specific training in engineering or programming, but must be equipped with a deep understanding of the cyber context in which they operate, combined with an appreciation of military ethics, law, strategic studies, political theory, organizational theory, international relations, and additional sciences. Only then will this new cadre of cyber-strategic military leaders be able to harness the right tools, people, strategies, and balance of offensive and defensive capabilities.

Military academic institutions, both at the undergraduate and graduate level, must be the incubators of future cyber-strategic leaders. This survey has highlighted an increased effort by the US service academies to develop new content for cybersecurity education at the undergraduate level, include cyber components in existing curricula and extracurricular activities, and prepare cadets and midshipman to lead in an age of persistent cyber threat. These efforts are commendable, especially in comparison to the much slower or nonexistent integration of cybersecurity components in undergraduate programs across American civilian universities. Despite these laudable developments, however, the survey has also shown that more progress is still needed to educate all future military officers about the complexities of cybersecurity. Many of the service academies already provide cyber-related coursework for students pursuing more technical career paths. These efforts, however, must extend to all students, both in technical and non-technical career paths. Moreover, classroom study is only part of the equation. Extracurricular activities provide cadets and midshipman valuable hands-on experience. Cybersecurity-related internships and clubs can increase students' professional network, develop their cyber expertise, and provide them with opportunities to implement classroom lessons-learned in a real world environment. These activities should be expanded to cater to technical and non-technical students. In so doing, the service academies will reorient their educational objectives and outcomes to better reflect the reality of the modern battlefield. By equipping all their graduates with the knowledge necessary to confront a wide array of cyber threats, the service academies will play a vital role in ensuring that the US military is able to establish both a competitive and security advantage on this new and increasingly critical "battlespace."

The views expressed are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

NOTES

[1] Martin C. Libicki, "Crisis and Escalation in Cyberspace," *RAND Project Air Force (2012), and Jason Healey, A Fierce Domain: Conflict in Cyberspace, 1986 to 2012,* (Arlington, VA: Cyber Conflict Studies Association, 2013).

[2] "Middle Class Economics,"*The President's Budget Fiscal Year 2016,* August 7, 2015, https://www.whitehouse.gov/sites/default/files/omb/budget/fy2016/assets/fact_sheets/cybersecurityupdated.pdf

[3] "The Department of Defense Cyber Strategy," *US Department of Defense* (April 2015), 4-5.

[4] For an overview of military readiness, see: Todd Harrison, "Rethinking Readiness," *Strategic Studies Quarterly* 8.3 (Fall 2014).

[5] Rep. Jim Langevin, "Column: Cyber dominance meaningless without skilled workforce," *Federal News Radio,* October 12, 2012, http://federalnewsradio.com/congress/2012/10/column-cyber-dominance-meaningless-without-skilled-workforce/.

[6] While the authors recognize that there are other academic institutions training students who will be commissioned in the US military, the study focuses solely on the four main US service academies: US Coast Guard Academy, US Air Force Academy, US Military Academy, and US Naval Academy, because these academic institutions are designed exclusively for the purpose of commissioning future military officers into their respective services. For instance, while the US Merchant Marine Academy is a federal service academy whose graduates may accept a commission in the US military, this academic institution is primarily charged with training personnel for the US merchant marine; a fleet of US civilian and federally owned merchant ships managed by the government or private sector. Students here can, however, choose to commission into a branch of the military after graduation.

[7] Francesca Spidalieri, "Joint Professional Military Education Institutions in an Age of Cyber Threat," *Pell Center Report,* (August 7, 2013), 1.

[8] Department of Defense, "Cyber Operations Personnel Report," *Report to the Congressional Defense Committees* (April 2011).

[9] "Pentagon's Cyber Mission Forces Takes Shape," *Federation of American Scientists,* September 10, 2015, https://fas.org/blogs/secrecy/2015/09/dod-cmf/, and "Middle Class Economics," *The Presidents Budget Fiscal Year 2016,* August 7, 2015, https://www.whitehouse.gov/sites/default/files/omb/budget/fy2016/assets/fact_sheets/cybersecurity-updated.pdf.

[10] William Welsh, "Cyber warriors: the next generation," *Defense Systems,* 23 January 2014, https://defensesystems.com/Articles/2014/01/23/Next-generation-cyber-warriors.aspx?Page=1. For an overview of the current state of CMF recruitment and training, see: Bill Matthews, "Military Battles to Man its Developing Cyber Force," *GovTech Works,* September 16, 2015, https://www.govtechworks.com/military-battles-to-man-its-growing-cyber-force/.

[11] "Jennifer J. Li and Lindsay Daugherty, "Training Cyber Warriors: What Can Be Learned from Defense Language Training," *RAND* (2015), ii.

[12] Secretary of Defense Speech, "Drell Lecture: Rewiring the Pentagon: Charting a New Path on Innovation and Cybersecurity," *US Department of Defense,* April 23, 2015, http://www.defense.gov/News/Speeches/Speech-View/Article/606666.

[13] Robert M. Gates, "Department of Defense Strategy for Operating in Cyberspace," *US Department of Defense,* (July 2011), 1.

[14] Daniel Goure, "Six Steps to Securing DoD's Networks for the 21st Century," *Real Clear Defense,* 12 August 2015, http://www.realcleardefense.com/articles/2015/08/12/six_steps_to_securing_dods_networks_for_the_21st_century__108352.html.

[15] If tampered, malicious microelectronics or chips underlie weapons platforms, they can operate as hidden "back doors" for espionage or sabotage. Malicious hardware, in fact, can be inserted into a chip after the design phase, but prior to its fabrication, thus making it challenging to detect. This is a risk for all weapons platforms, including those that are "air-gapped" or "off the grid." For more information on the use of microelectronics in modern military platforms, see: Jennifer McArdle, "Hardware Security in the US-Indian Cyber Dialogue," *The National Interest,* June 30, 2014, http://nationalinterest.org/feature/hardware-security-the-us-indian-cyber-dialogue-10770, and Defense Science Board, "High Performance Microchip Supply," *Task Force Report* (2005).

NOTES

16. Authors' interview with Dr. Fernando Maymí, Deputy Director of the Army Cyber Institute at West Point and Assistant Professor in the Department of Electrical Engineering and Computer Science, December 14, 2015.

17. Spidalieri, "Joint Professional Military Education Institutions in an Age of Cyber Threat," 2013.

18. National Research Council, "At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues," *The National Academic Press* (Washington, D.C.) 2014.

19. Jan Kallberg and Bhavani Thuraisingham, "Cyber Operations: Bringing from Concept to Cyber Superiority," *Joint Force Quarterly 68,* no.1 (January 2013), 53-58.

20. *Cybered conflict* differs from *cyber war* or *cyber battle.* The latter is fully technological and could, in principle, be conducted entirely within a network. It is normally a component of the former. "Cybered conflicts are those nationally significant aggressive and disruptive conflicts for which seminal events determining the outcome could not have occurred without 'cyber' (meaning networked technologies) mechanisms at critical junctures in the determining course of events." 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,* The Aspen Institute (Washington, D.C.), 63.

21. "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), 3.

22. Edward Sobiesk, Jean Blair, Gregory Conti, Michael Lanham, and Howard Taylor, "Cyber Education: A Multi-Level, Multi-Discipline Approach," *US Military Academy,* (September/ October 2015), 44.

23. "Cyber Education Project," http://www.cybereducationproject.org.

24. Spidalieri, "Joint Professional Military Education Institutions in an Age of Cyber Threat," 2013.

25. This methodology is adapted from a methodology developed and employed in 2013 to assess military graduate programs that offer Joint Professional Military Education (JPME). The results provided an overview of the efforts by JPME institutions to include information technology and cybersecurity into their curricula. For more information, see: Spidalieri, "Joint Professional Military Education Institutions in an Age of Cyber Threat," 2013.

26. The Likert scale is commonly used in survey research. This approach is usually used to measure respondent's attitudes by asking the extent to which they agree or disagree with a particular question or statement.

27. NSA and DHS set up criteria for the designation of universities or academic departments, both civilian and military, as Center of Academic Excellence in Information Assurance Education (CAE/IAE) and Research (CAE/R). The designation is valid for five academic years, after which the school must successfully reapply in order to retain its CAE designation. The list of CAE academic institutions can be found at: https://www.nsa.gov/ia/academic_outreach/nat_cae/institutions.shtml.

28. "24th Air Force Fact Sheet," http://www.24af.af.mil/library/factsheets/factsheet.asp?id=15663.

29. Don Branum, "Academy Introduces Computer Network Security Major," *US Air Force,* August 12, 2014, http://www.af.mil/News/ArticleDisplay/tabid/223/Article/494118/academy-introduces-computer-network-security-major.aspx.

30. Authors' interview with Major Michael V. Chiaramonte, Assistant Professor, Department of Computer Science, US Air Force Academy, December 9, 2015.

31. "Center of Innovation," *US Air Force Academy,* http://www.usafa.edu/df/dfe/dfer/centers/coi/.

32. "Catalog of Courses (2015-2016)," *US Coast Guard Academy,* 52-54 and 92. The Central Security Service is a DoD agency established to integrate the NSA and the Service Cryptologic Elements (SCE) of the US Armed Forces in the field of signals intelligence, cryptology, and information assurance at the tactical level. For more information, see: National Security Agency/Central Security Service, https://www.nsa.gov/about/central_security_service/css_insignia.shtml.

33. "Catalog of Courses," *US Coast Guard Academy,* 80 and 154.

34. *Ibid,* 80 and 157. For more information on course, see also: LCDR Joseph Benin and CDR Kelly Seals, "Rising to Today's Challenges: Cyber Education and Training at the Coast Guard Academy," *Around the Academy* (October 2015), 35-36.

NOTES

35. Authors' interview with Dr. Kimberly Young-McLear, Coast Guard Lieutenant and member of the Permanent Commissioned Teaching Staff, February 27, 2016.

36. *Ibid.*

37. "Catalog of Courses," US Coast Guard Academy, 69 and 110-111.

38. Authors' interview with Dr. Kelly Seals, Coast Guard Commander and Section Chief and Program Chair for the Electrical Engineering Department, February 26, 2016.

39. Joseph Benin, "US Coast Guard Academy host cyber symposium," *The Coast Guard Blog for Maritime Professionals,* April 24, 2105, http://mariners.coastguard.dodlive.mil/2015/04/24/4242015-u-s-coast-guard-academy-hosts-cyber-symposium/, and LCDR Joseph Benin and CDR Kelly Seals, "Rising to Today's Challenges: Cyber Education and Training at the Coast Guard Academy," *Around the Academy* (October 2015), 38-40.

40. Cheryl Pellerin, "Service Academy CyberStakes Proves Worth as Learning Tool," *US Department of Defense,* February 16, 2016, http://www.defense.gov/News-Article-View/Article/656181/service-academy-cyberstakes-proves-worth-as-learning-tool.

41. Julia Bergman, "Cyber team forms at the Coast Guard Academy," *The Day,* January 17, 2016, http://www.theday.com/article/20160117/NWS09/160119264.

42. "Coast Guard Academy Cyber Symposium," *US Coast Guard Academy Symposium Agenda,* March 26, 2015.

43. Benin and Seals, "Rising to Today's Challenges," (2015), 34.

44. Office of the Dean, "Academic Program, Class of 2017: Curriculum and Course Descriptions," *US Military Academy West Point* (2016), 18.

45. Fernando Maymí, authors' interview, 2015.

46. Sobiesk et al., "Cyber Education: A Multi-Level, Multi-Discipline Approach," (2015): 45.

47. Office of the Dean, "Academic Program, Class of 2017" (2016), 131.

48. Fernando Maymí, authors' interview, 2015.

49. *Ibid.*

50. "Welcome to the Cyber Research Center," *US Military Academy,* http://www.usma.edu/crc/SitePages/Home.aspx, and authors' interview with Dr. Fernando Maymí, 2015.

51. Cadet Competitive Cyber Team, C3T," *US Military Academy West Point.*

52. Sobiesk et al., "Cyber Education: A Multi-Level, Multi-Discipline Approach," (2015), 46.

53. Fernando Maymí, authors' interview, 2015.

54. *Ibid.*

55. "Cyber Leader Development Program (CLDP) Overview," *US Military Academy,* http://www.usma.edu/acc/SitePages/CLDP.aspx, and authors interview with Dr. Fernando Maymí, 2015.

56. "Academics: Majors," *US Naval Academy,* http://www.usna.edu/Academics/Majors-and-Courses/index.php.

57. Mike Hoffman, "Naval Academy Launches Cyber Operations Major," Defense Tech, June 8, 2013, http://www.defensetech.org/2013/06/08/naval-academy-launches-cyber-operations-major/.

58. Authors' interview with Captain Paul Tortora, Director of the USNA Center for Cyber Security Studies, November 23, 2015.

59. "Academics: Course Listing," *US Naval Academy,* http://www.usna.edu/Academics/Majors-and-Courses/course-description/All-Courses.php.

NOTES

60. Paul Tortora, authors' interview, 2015.

61. *Ibid.*

62. Nathan Wikes, "USNA Midshipmen Recognized by President Obama for Achievement," *Official Website of the US Navy,* May 7, 2015, http://www.navy.mil/submit/display.asp?story_id=86982.

63. Meghann Myers, "Naval Academy gets $120 million for new cyber center," *Navy Times,* December 18, 2014, http://www.navytimes.com/story/military/capitol-hill/2014/12/18/naval-academy-annapolis-cyber-building/20592213/, and "Microsoft Supports Naval Academy's Center for Cyber Security Studies Building with Gift of $1Million," *PR Newswire,* September 24, 2015, http://www.prnewswire.com/news-releases/microsoft-supports-naval-academys-center-for-cyber-security-studies-building-with-gift-of-1-million-300148581.html.

64. "Center for Cyber Security Studies," *US Naval Academy,* http://www.usna.edu/CyberCenter/.

65. Tim Prudente, "Naval Academy, UMBC partner to develop cyber security defenses," *Capital Gazette,* September 27, 2015, http://www.capitalgazette.com/news/naval_academy/ph-ac-cn-cyber-security-0926-20150924-story.html.

66. Francesca Spidalieri, "State of the States on Cybersecurity," *Pell Center Report* (November 2015), 14, http://pellcenter.org/wp-content/uploads/2015/11/Pell-Center-State-of-the-States-Report.pdf.