United States Military Academy
USMA Digital Commons

West Point Research Papers

3-29-2019

Educating Future Multidisciplinary Cybersecurity Teams

Jean Blair
United States Military Academy, jean.blair@westpoint.edu

Andrew Hall
Army Cyber Institute, andrew.hall@westpoint.edu

Edward Sobiesk
Army Cyber Institute, edward.sobiesk@westpoint.edu

Follow this and additional works at: https://digitalcommons.usmalibrary.org/usma_research_papers

 Part of the Educational Methods Commons, and the Information Security Commons

Recommended Citation
J. R. S. Blair, A. O. Hall and E. Sobiesk, "Educating Future Multidisciplinary Cybersecurity Teams," in Computer, vol. 52, no. 3, pp. 58-66, March 2019. doi: 10.1109/MC.2018.2884190

This Article is brought to you for free and open access by USMA Digital Commons. It has been accepted for inclusion in West Point Research Papers by an authorized administrator of USMA Digital Commons. For more information, please contact nicholas.olijnyk@westpoint.edu.

Educating Future Multidisciplinary Cybersecurity Teams

Jean R.S. Blair, Andrew O. Hall, and Edward Sobiesk, U.S. Military Academy

We present a vision and the curricular foundations needed for the multidisciplinary cybersecurity teams of the future, which are made up of diverse cybersecurity experts, each contributing unique abilities and perspectives that emerged from their own discipline-centric methodological approaches. Examples demonstrating the effectiveness of current and emerging multidisciplinary cybersecurity teams are included.

Cybersecurity is inherently interdisciplinary at the individual level and multidisciplinary at the team level. The ubiquitous and increasingly complex nature of cyberspace necessarily demands application of expertise in so many disparate disciplines that a single cybersecurity curriculum cannot provide sufficient breadth and depth.

In this article, we present a vision for the cybersecurity team of the future, along with the disciplines and the multidisciplinary curricular foundations needed to produce such a team. We believe that, although many programs and curricula aspire to a multidisciplinary viewpoint, the current curricular models claiming to support a multidisciplinary perspective primarily integrate notions of other disciplines into an individual and are, therefore, more interdisciplinary in nature.

The cybersecurity team is driven by the assumption of ever-present, intelligent, adaptive, evolving adversaries—both human and artificial. The threats in cyberspace span from nation states to hacker collectives to industrial spies who target academia, governments, and industry. The risk decisions made to ensure success of the firm or organization cannot address only technical vulnerabilities. They must also holistically

Digital Object Identifier 10.1109/MC.2018.2884190
Date of publication: 2 April 2019

U.S. Government work not protected by U.S. Copyright.

address risk as well as the impacts of cybersecurity policies on people and processes.

Our viewpoint is consistent with the multidisciplinary approach briefly suggested by Conti and Raymond[1] as well as with the complexity of environments and disciplinary perspectives displayed in the case studies of Shakarian et al.[2] and Green.[3] Further, because of the critical interdependency between cybersecurity and success across core business areas, we feel members of the cybersecurity team will be involved throughout all business processes to determine acceptable risk; ensure business solutions, products, and services are designed, developed, and provided with full consideration of the latest security threats to the customers; and best protect the organization.

BACKGROUND

This article extends our 2015 and 2017 articles[4,5] that describe a holistic multilevel, multidiscipline approach to cybereducation used to achieve the goal of "providing all educated individuals a level of cybereducation appropriate for their role in society."[4] Our previous works reviewed established best practices and provided a foundation for viewing cybersecurity from a multidisciplinary perspective. They also provided tangible examples of how this is done both inside and outside the classroom at the U.S. Military Academy.

A highly informative and definitive description of the past, and potentially future, evolution of cybersecurity education, along with numerous relevant references, can be found in Parrish et al.[6] This 2018 Innovation and Technology in Computer Science Education (ITiCSE) report traces previous ITiCSE initiatives and other international efforts in the evolution of cybersecurity education to its current state today as a metadiscipline that is largely centered around computing. The report also covers the integration of cybersecurity into the various Association for Computing Machinery curricula recommendations, including the disciplines of computer science, information systems, information technology, computer engineering, software engineering, and cybersecurity itself, and the impact of these curricular recommendations on ABET accreditation criteria. The report advocates for an interdisciplinary perspective toward cybersecurity and provides a generic competency model that could be used across all disciplines to specify the cybersecurity competencies needed in the 2030s.

Many distinct, well-established professions have begun to frame how their profession's knowledge, principles, practices, and skills need to progress and evolve given the exponentially growing cyber-enabled threats and opportunities in the world. Some professions have established task forces to address this. For example, see the well-thought-out reports from the computing-focused National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework[7] and the Joint Task Force on Cybersecurity Education,[8] the Health Care Industry Cybersecurity Task Force,[9] and the Attorney General's Cyber Digital Task Force.[10] Leaders in other professions have proactively undertaken steps to frame key issues and make recommendations from their profession's perspective. For examples, see works coming from the international relations,[11] political science,[12] and organizational behavior communities.[13] These reports, for the most part, focus on discipline-centric issues and recommendations. As such, the resulting reports deeply address how individuals might apply what is currently considered to be the professions' knowledge, principles, practices, and skills; many describe how cyberthreats could cause a disaster if the profession, society, and government do not guard against such attacks.

Business, government, and higher education in general have acknowledged for some time that teams of diverse individuals are likely to do better and accomplish more than teams of people with similar backgrounds. Of particular interest is that cybersecurity itself is a discipline that crosses traditional disciplinary boundaries. It is the dynamic blending of people and processes from diverse disciplinary backgrounds that clearly realizes what Johansson[14] describes as the *Medici Effect*—breakthrough innovations happen at the boundaries or intersections between different fields and cultures. Despite acknowledging that innovation occurs at the boundaries, current educational curricular guidelines focus on adding broader knowledge and skills within an individual. These efforts are interdisciplinary in that they support a personal approach to problem solving and knowledge development that requires synergy across disciplines within an individual. In the long term, the adding of breadth in an individual cannot scale and necessitates a tradeoff with depth of expertise.

Our work is motivated by the need to develop the skills in each cybersecurity team member to effectively work with experts who have a background in complementary disciplines so that the team can collectively accomplish more than the sum of their individual contributions. This is what we

call *multidisciplinary*, a process that involves a team of individuals with diverse disciplinary backgrounds and perspectives working together to develop solutions that can be created only by truly integrating aspects of many disciplines in innovative ways at a team level. Only with this approach will we start to build teams that can begin to actually address the inherently complex current and future cybersecurity issues.

A VISION FOR MULTIDISCIPLINARY CYBERSECURITY TEAMS

The cybersecurity team of the future will be intrinsically multidisciplinary, composed of internal and external expertise (consisting of both people and artificial intelligence) from multiple diverse relevant fields. The people involved will have a proclivity for combining their deep areas of expertise with others on the team who possess complementary deep knowledge, abilities, and experiences. Because of cybersecurity's interdependencies across core business functions, members of the cybersecurity team will examine each business process to determine acceptable levels of risk. They will also protect the organization by ensuring that business solutions, products, and services are designed, developed, provided, and maintained with full consideration of the latest security risks to the customers.

Each member of the team will address security tasks within his or her own specialized domain and readily provide essential unique contributions to team efforts to successfully manage risk in the presence of ever-evolving cyberthreats and respond to new cybersecurity opportunities and challenges. Each member individually, and the team as a whole, will adapt, use, and integrate automation and emerging technologies to optimally employ human–machine collaborations. There will be a synergy across the multidisciplinary team that enables its members to collectively combine individual disciplinary contributions to create innovative solutions and perspectives that would not otherwise be possible, including procuring just-in-time expertise as needed. Together, the team will identify, utilize, and develop innovations that facilitate stability and operational success across the organization, society, or nation state.

These diverse cybersecurity teams will be of variable size and experience levels, with each team's composition as unique as its members. In larger organizations, the team may be mainly in-house cybersecurity experts across computing, mathematics, statistics, artificial intelligence, electrical engineering, cognitive science, law, organizational management, political science, international relations, marketing, and possibly core business operations. Smaller organizations will most likely have a core team that matrixes support from across the organization, with contracted support to round out capability. In either case, individuals will fulfill their role by applying and lending expertise in their field. The following list of disciplines and roles is not definitive but is rather meant to inspire a realization of the depth of the required multidisciplinary effort. Although a single individual may have knowledge and skills in several of these areas, the diversity and number of disciplines preclude any one individual from having a deep knowledge in all of these areas.

Computing

There are likely several, or even many, cybersecurity computing professionals with various areas and levels of expertise and responsibility. Some will have deeply technical positions, while others will be more broadly involved in the cybersecurity team. Computing professionals will include 1) individuals with primary expertise in computing (e.g., computer science, information technology, network engineering, and information systems) complemented with substantive knowledge and abilities on cybersecurity principles and practices who team with 2) individuals with a broader and deeper cybersecurity background complemented with sufficient knowledge and abilities in computing fundamentals. All computing professionals will work closely with the rest of the cybersecurity team to provide software and networking defenses that comply with laws, policies, and regulations; effectively use artificial intelligence and other emerging technologies; capitalize on fundamental principles of communication media of the day; and make it easy for workers in the enterprise to use the systems, adhere to policies regarding their employment, and judiciously assume an acceptable amount of risk.

Operations research

Operations research includes elements from mathematics, statistics, systems engineering, economics, and computing. These diverse fields will collectively provide professionals with expertise across a vast range of subjects including cryptography, mathematical foundations of what can and cannot be computed in a timely fashion, game theory, project management, optimization, machine learning, and quantum computing. They will play a significant role in evaluating levels of risk as well as simulating and modeling the impact of cybersecurity team

solutions based on potential technical and human behaviors. They will work with the artificial intelligence experts, computing professionals, cognitive scientists, marketing professionals, lawyers, and political scientists to provide valuable, legal, and intelligent use of data analytics.

Artificial intelligence and data science

These experts will play a crucial role on the cybersecurity team, working closely with the computing and operations research professionals to refine and improve their automated tools so that the human–machine defenses and opportunities can be used across all disciplines to combat the ever-increasing automated and intelligent capabilities of adversaries. They will develop, train, update, and evaluate machine learning recommendation systems that provide the kind of advice and guidance that customers currently get from companies such as Amazon or Netflix. These systems will undoubtedly also be used for numerous other tasks such as quality assurance.

Electrical and computer engineering

Electrical and computer engineers provide expertise on hardware, communications systems, network infrastructure, and photonics. They will develop or ensure the security of everything from chips to hardware components, embedded processes, sensors, drives, controllers, computer architectures, communication systems, and other disciplinary equipment and concepts. In particular, with the increased presence of the Internet of Things (including many sensors and devices within humans), this currently underrepresented domain will be critical.

Cognitive science and psychology

Cybersecurity cognitive scientists and psychologists will address issues related to human factors, human–machine interfaces and teaming, human behavior, talent assessment, team performance, and team communication. They will also provide explanations for and remove bias from artificial intelligence, develop effective training materials, and understand human limitations in decision making. They will create models to analyze work flow and estimate cognitive load as well as predict human behavior.

Law

Cybersecurity lawyers provide legal and ethical expertise related to issues involving privacy, security, contracting, intelligence, and surveillance at the local, state, national, and international levels. In military domains, they will possess knowledge on the intersection of cybersecurity with the Law of Armed Conflict, Geneva Conventions, and other issues related to sovereignty and international norms. Cybersecurity lawyers will also provide knowledge and expertise on public–private partnerships and information sharing among various government agencies and the private sector. As in-house counsel, they may, among other things, proactively engage with the team and enterprise about liability, law suits, and intellectual property to ensure that both the cybersecurity solutions/practices and the enterprise services are in compliance, including as products are developed. From inside both government agencies and private companies, they may work to influence and change government policies, laws, and international agreements to facilitate stronger cybersecurity practices for both the public and private sector.

Political science and international relations

These policy professionals provide a wide variety of expertise in strategy and policy issues, ranging from defense and deterrence to escalation and influence campaigns. They will bring broad knowledge of current and past events, with a clear understanding of the impact of cyber events on people, and on the private and public sectors, as well as the complex interplay between those impacts. They will actively work at understanding what the cybersecurity team is considering doing, describing potential unintended consequences and working with the management and marketing professionals developing internal policies as well as strategies for incentivizing behaviors. The cybersecurity international relations experts will provide strategy, policy, and cyberthreat intelligence expertise at the nation-state level. They will help the team understand how differing values, laws, ethics, and perspectives will impact operations that cross national boundaries. They will be the experts in evaluating and crafting means to influence cultures and their behavior and in understanding how these contribute to cooperation and conflict in cyberspace. They will maintain diplomatic and global security perspectives and help the organization increase trust and cooperation across international boundaries. Together with the political scientists, international relations experts will work with marketing and management to develop information-sharing policies and partnership practices that facilitate mutually maintaining

security and bringing a broader perspective on the full range of levers of national power, how nations use them to coerce or compel one another, and how they can either lead to success or unintended consequences.

Business

The impact of cybersecurity is felt throughout the organization. Each of the key departments within a modern corporation—i.e., operations, finance, and marketing—leverage modern information technology systems, with success or failure inextricably linked to cybersecurity. Business specialists will team with computing professionals who may still be learning the business processes of the organization. There is also now a realization that hacking attacks are sometimes a combination of relatively simple security exploits adapted to create public embarrassment or damage. These individuals will lead the efforts to identify such vulnerabilities and prevent such incidents. Depending on the organization, they may be from a mix of professions, such as public affairs and communications, engineers, health professionals, transportation experts, financial wizards, intelligence gatherers, members of the military, or government employees.

Management

Leadership of the cybersecurity team of the future is still an open question. As with chief information officers, it is unclear whether a technical, business, or interdisciplinary background will provide the preponderance of leaders. It is also unknown whether leadership of future cybersecurity teams will evolve from the chief information security officer position and whether it warrants a board-level position. It is clear, however, that leaders of future cybersecurity teams will have to be masters of putting together and mentoring great teams, perhaps in a manner similar to the abilities of general managers and head coaches of successful professional sports teams. Leadership of the cybersecurity team will also work with several other interested parties to facilitate and conduct information sharing, both internal and external to the organization.

EACH MEMBER MUST NOT ONLY BE EDUCATED IN AN APPROPRIATE CYBER-FOCUSED DISCIPLINE BUT ALSO MUST BE WELL EDUCATED IN THE SKILLS NECESSARY TO BE AN EFFECTIVE CONTRIBUTOR AND FACILITATOR ON A DIVERSE MULTIDISCIPLINARY TEAM.

Delineating responsibilities in multidisciplinary cybersecurity teams

Although it may be possible for the cybersecurity team to be distributed throughout the organization (i.e., each individual being embedded in a section that has people with their expertise, as in the law department, the cyber operations department, the human resources department, and so on) and then provide matrixed support to respond to cyber incidents, the best organizations will work together proactively to reduce cyber risk and create habitual relationships. Few organizations will be able to provide lawyers or marketers who are 100% dedicated to a cybersecurity team. We recommend that, if individuals on the cybersecurity team have split responsibilities, their contribution to the cybersecurity team must be clearly delineated. For smaller organizations, some expertise might need to be external or contracted.

CURRICULAR FOUNDATIONS FOR THE CYBERSECURITY TEAM

The premise of this article is that cybersecurity is so complex and inherently multidisciplinary that to contribute effectively to a cybersecurity team, each member must not only be educated in an appropriate cyber-focused discipline but also must be well educated in the skills necessary to be an effective contributor and facilitator on a diverse multidisciplinary team. Today's educational systems generally are designed to give an individual a discipline-centric foundation, often stretching the student to work on teams that include other members from closely related disciplines. Many also get at some level of interdisciplinary skills—which requires synergy across disciplines within an individual. This is in contrast to deliberately developing multidisciplinary skills—an approach that requires working together with individuals with dissimilar disciplinary backgrounds to develop solutions that can be created only by truly

integrating aspects of the various disciplines in innovative ways at a team level. These skills are arguably more important for the cybersecurity professional than having rudimentary awareness of the other disciplinary facets of cybersecurity. In what follows, we propose desired multidisciplinary-focused outcomes of graduates from any cybersecurity-related higher-education degree and then briefly discuss how a faculty and curriculum might develop those characteristics in the students. Each discipline's body of knowledge likely includes some requirements for abilities related to the legal and ethical issues as well as communication skills and team skills. The focus here is on the portions of those skills that the cybersecurity professional needs to work with others across disciplines.

The most essential multidisciplinary-focused knowledge, skills, and abilities for a cybersecurity team member are consistent with the directions in higher education of the last decade and encompass many of the key components in the Association of American Colleges and Universities VALUE rubrics. These rubrics include

1. integrative and applied learning
2. teamwork
3. critical thinking
4. creative thinking
5. inquiry and analysis
6. intercultural knowledge and competence (to a lesser extent).

See Rhodes[15] for the details of these rubrics.

To be an effective member of a cybersecurity team, graduates of a higher-education cybersecurity-focused degree program should exhibit skills and behaviors, such as the following. The cybersecurity graduate

- *actively seeks input*: has a propensity to garner relevant issues and limitations from each of the other disciplinary experts before and during any work in progress, including efforts to evaluate the level of risk; actively seeks critical feedback on the level of success and areas for improvement after implementing a cybersecurity solution
- *listens and pursues full understanding*: carefully listens to other team members, asks questions, and persists until both are confident that the relevant cybersecurity issues are understood and both agree on acceptable risk and what the next steps ought to be
- *effectively communicates to others*: effectively communicates to other members of the team critical relevant issues from one's own disciplinary perspective
- *addresses conflict*: directly addresses conflict to help manage and resolve issues, usually helping strengthen both the cybersecurity solution and the team
- *facilitates synergy*: is interested in and appreciative of each team member's unique strengths and disciplinary background; engages teammates and constructively builds on their contributions; suggests ways to synthesize contributions
- *recognizes and exploits innovation*: is forward thinking; recognizes novel solutions and unique ideas; extends, transforms, and integrates innovative ideas to create new improved solutions
- *thinks critically*: views a situation from both micro and macro levels and discerns potential impacts; is respectful and constructive while questioning assumptions; formulates recommendations based on logic and informed evaluations
- *promotes and practices resiliency*: is agile; recovers swiftly and appropriately; is a consequential contributor to effective teamwork during recovery
- *capitalizes on interrelationships*: is cognizant of the interrelationships among authorities, policies, laws, personal responsibilities, and ethics associated with information-based activities; facilitates integration by fellow cybersecurity team members.

In total, a cybersecurity-related curriculum that is designed to develop students into valuable members of cybersecurity teams should develop both the skills just described and the knowledge, skills, and abilities relevant to the cyber-focused host discipline. Previous works on cybersecurity education and other articles in this issue address the curricular foundations relevant to the cyber-focused degree in a host discipline, and Parrish et al.[6] propose a general model that can help all professions describe cybersecurity competencies within their given discipline. Our article calls for integrating into those curricula developmental experiences that prepare graduates for multidisciplinary interactions.

There are several detailed works that each describe one or more ideas for how to develop and assess some of the skills listed previously (for example, see Wagner[16] on developing creative and innovative thinkers). To be most effective at teaching these multidisciplinary skills, the curriculum should

include learning experiences that give the students practice working with people with different disciplinary and cultural backgrounds. Ideally, these types of experiences would be strategically placed throughout the curriculum, leading to a large culminating open-ended team project.

The faculty members who deliver the curriculum will need to have had multidisciplinary experiences themselves. How they get this is likely to vary widely, but, without having had some set of experiences that helps them understand and appreciate the skills needed to effectively work with people who have very different disciplinary expertise, it is unlikely that they will be able to succeed in developing those skills in their students.

EXAMPLES OF MULTIDISCIPLINARY CYBERSECURITY TEAMS

The 60-person Army Cyber Institute (ACI) is a concrete example of the power and value of successful multidisciplinary cybersecurity teams made up of experts from different fields. Located as part of the U.S. Military Academy at West Point, New York, the ACI has researchers and faculty spanning eight different academic departments: behavioral sciences and leadership; electrical engineering and computer science; English and philosophy; history; law; mathematical sciences; social sciences; and systems engineering. The ACI's unique mix of civilian academics with active-duty military officers promotes a blend of basic and applied research that advances the body of knowledge while also creating internal and external partnerships to conduct applied research that brings pragmatic value and sets future direction.

One ACI example of a research initiative that creates synergies across multiple disciplines and domains is Jack Voltaic—the ACI's research dedicated to protecting critical infrastructure.[17] Jack Voltaic is a series of multiday, multisector, public–private events that explore preparation, prevention, and response during simulated cyberspace-physical attacks on a large city. Exercises have been conducted thus far in New York City and Houston. The 2016 New York City event involved about 20 organizations and 100 participants. The 2018 Houston event involved about 40 organizations and 400 participants. The New York City event was co-led with Citigroup (a financial institution) and the Houston event with AECOM (a national engineering company).

Overall, the critical infrastructure sectors involved included communications, defense industrial base, emergency services, energy, financial services, government facilities, health care, and transportation systems. The design of the event included three components: governance coordination, a facilitated tabletop exercise for midlevel managers, and a virtual environment component in which operators encountered a notional adversary.

Prior to the Jack Voltaic research efforts, a challenge recognized within the U.S. critical infrastructure communities was that too many of their preparations were siloed within their own sector. The true purpose and value of the Jack Voltaic research are that it forces communication and coordination across sectors, including encountering many boundary issues and assumptions. These unique events each simultaneously engage multiple areas of expertise, creating an environment in which leaders from different domains must collaborate with one another to resolve crises. In each of the two past Jack Voltaic events, the domains spanned many disciplines including computing, electrical and computer engineering, operations research, political science and international relations, law, business, cognitive science, public affairs, and management.

A second ACI example of multidisciplinary efforts succeeding is research that explored the vulnerability equities process in which "offensive equities are weighed against potential harms caused by delayed disclosure or nondisclosure of zero-day vulnerabilities."[18] The power behind this research and publication was the collaboration between a lawyer who is an expert on national policy for cyberethics, privacy, security, and surveillance and an intelligence officer who had served in operational cyberassignments and possessed a computing and engineering background. This research not only spanned the deep expertise of both these individuals but also covered the intersection and boundaries of their disciplines, which are so often either ignored or misunderstood.

Overall, almost all outreach, partnerships, and research conducted by the ACI are multidisciplinary in nature. These efforts are aided by the fact that several other U.S. Military Academy faculty members from across various departments are actively conducting cyber research and cyber educational initiatives in conjunction with the ACI.

The multidisciplinary paradigm also correlates well with cybersecurity colleagues from the private sector with whom we have spoken. The market need for multidisciplinary cybersecurity teams has created an environment

in which innovative cyber solution companies have arisen.

GRIMM is a private-sector cybersecurity company that provides another concrete example of a successful multidisciplinary cybersecurity team. The roughly 60 internal GRIMM employees come from a mix of technical and social science backgrounds. The company maintains a holistic, multidisciplinary perspective and organizes in a matrixed manner, pulling in expertise based on the needs of the situation. GRIMM founder Bryson Bort emphasized that "innovation and compromise happens at the edge."[19]

Recently, GRIMM solved a high-level fraud challenge for one of the world's largest banking institutions by pulling together in-house policy, government, criminal-tracking, technical, and strategic minds. Combining deep in-house expertise in developing technologies with the understanding of policy and strategic implications, GRIMM was able to swiftly identify a single source of fraud risk for the bank. This approach saved the bank more than US$90 million in fraud avoidance (a figure determined after the fraud trend turned toward the now-prepared bank) as well as countless millions of dollars in fines and legal fees. In this example, it was the multidisciplinary skills across the team that enabled its members to quickly solve a complex problem with a combination of technical and nontechnical approaches.

In this article, we argued that cybersecurity is inherently both interdisciplinary at the individual level and multidisciplinary at the team level. We submit that the ubiquitous and ever-increasingly complex nature of cyberspace requires breadth and depth beyond that which can be included in a single cybersecurity curriculum. We presented a vision for the cybersecurity team of the future, along with the disciplines and the multidisciplinary curricular foundations needed to produce such a team. We noted that, while many programs and curricula aspire to a multidisciplinary viewpoint, the current curricular models claiming to support a multidisciplinary perspective primarily integrate notions of other disciplines into an individual and are therefore more interdisciplinary in nature. We believe that effective and stable cybersecurity can be achieved and maintained only by teams of experts from multiple disciplines, focusing their efforts against omnipresent, intelligent, adaptive, and ever-changing human and autonomous adversaries. Because of the critical interdependency between cybersecurity and success across core business areas, we feel that members of the cybersecurity team will be involved throughout all business processes to determine acceptable risk; ensure that business solutions, products, and services are designed, developed, and provided with full consideration of the latest security threats to the customers; and best protect the organization.

Future work will involve fully integrating content and experiences into the various cybersecurity-focused educational systems that develop the much-needed multidisciplinary attributes and culture. Ideally, students will be taught these skills, given constructive feedback after practicing them, and provided with an opportunity to experience a true multidisciplinary cybersecurity team effort. Another interesting avenue for future work would be to holistically pull together the bodies of knowledge (curricular models) for cybersecurity-focused degrees in the different disciplines and to use those to help educators in each of the disparate fields better understand how their graduates will interact with other members of the cybersecurity

ABOUT THE AUTHORS

JEAN R.S. BLAIR is a professor of computer science at the U.S. Military Academy and is currently the distinguished professor for innovation in the Department of Electrical Engineering and Computer Science. Her research interests include computing and cybersecurity education, the design and analysis of algorithms for combinatorial problems, graph algorithms, and parallel computing. Blair received a Ph.D. in computer science from the University of Pittsburgh. Contact her at jean.blair@westpoint.edu.

ANDREW O. HALL is the director of the Army Cyber Institute at the U.S. Military Academy and teaches in the Department of Mathematical Sciences. His research interests include human resources and manpower planning, Markov decision processes, machine learning, and mathematical finance. Hall received a Ph.D. in management science from the University of Maryland. Contact him at andrew.hall@westpoint.edu.

EDWARD SOBIESK is the senior civilian faculty member in the Army Cyber Institute and is a professor of computer and cyber science in the Department of Electrical Engineering and Computer Science at the U.S. Military Academy. His research interests include online privacy and usable security, computing and cybersecurity education, artificial intelligence, and complex interdependence. Sobiesk received a Ph.D. in computer and information sciences from the University of Minnesota. Contact him at edward.sobiesk@westpoint.edu.

team. Both of these directions reinforce the concept that cybersecurity is a metadiscipline spanning many traditional boundaries.

ACKNOWLEDGMENTS

We would like to acknowledge and profoundly thank the talented and diverse group of cybersecurity professionals who generously shared their expertise and perspectives to shape and inform the content of this article. These included Robert Barnsby, Nathaniel Bastian, Erica Borghard, Bryson Bort, Judy Esquibel, Jason Healey, Maxim Kovalsky, Paul Maxwell, Clay Moody, Stephanie Pell, Aryn Pyke, Roy Ragsdale, and Robert Thomson.

The views expressed in this article are those of the authors and do not reflect the official policy or position of the U.S. Military Academy, the Department of the Army, the Department of Defense, or the U.S. Government.

REFERENCES

1. G. Conti and D. Raymond, *On Cyber: Towards an Operational Art for Cyber Conflict*. New York: Kopidion Press, 2017.
2. P. Shakarian, J. Shakarian, and A. Ruef, *Introduction to Cyber-Warfare: A Multidisciplinary Approach*. Waltham, MA: Syngress, 2013.
3. J. Green, *Cyber Warfare: A Multidisciplinary Analysis*. New York: Routledge, 2015.
4. E. Sobiesk, J. Blair, G. Conti, M. Lanham, and H. Taylor, "Cyber education: A multi-level, multi-discipline approach," in *Proc. Conf. Information Technology Education*, Chicago, IL, 2015, pp. 43–47.
5. A. Hall and E. Sobiesk, "Integration of the cyber domain at the United States Military Academy," in *Proc. Int. Workshops: Realigning Cybersecurity Education*, Australia, 2017. doi: 10.1145/3293881.3295778.
6. A. Parrish et al. "Global perspectives on cybersecurity education for 2030: A case for a meta-discipline," in *Proc. Conf. Innovation and Technology in Computer Science Education*, Larnaca, Cyprus, 2018.
7. National Initiative for Cybersecurity Education (NICE), "NICE Cybersecurity Workforce Framework." Accessed on: Nov. 8, 2018. [Online]. Available: https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework
8. Association for Computing }Machinery (ACM). (2017). "Cybersecurity curricula 2017." ACM, New York. [Online]. Available: https://www.acm.org/education/curricula-recommendations
9. Health Care Industry Cybersecurity Task Force. (2017). Report on improving cybersecurity in the health care industry. U.S. Dept. Health and Human Services, Washington, D.C. [Online]. Available: https://www.phe.gov/preparedness/planning/CyberTF/Pages/default.aspx
10. U.S. Department of Justice (U.S. DoJ). (2018). "A report of the Attorney General's cyber digital task force." U.S. Dept. of Justice, Washington, D.C. [Online]. Available: https://justice.gov/cyberreport
11. New York Cyber Task Force, "Building a defensible cyberspace." Accessed on: Sept. 7, 2018. [Online]. Available: https://sipa.columbia.edu/ideas-lab/techpolicy/building-defensible-cyberspace
12. Secretary of Commerce and the Secretary of Homeland Security, "Supporting the growth and sustainment of the nation's cybersecurity workforce: Building the foundation for a more secure American future," Accessed on: Sept. 7, 2018. [Online]. Available: https://www.dhs.gov/publication/supporting-growth-and-sustainment-nations-cybersecurity-workforce
13. European Union for Network and Information Security, "Cyber security culture in organizations." Accessed on: Sept. 7, 2018. [Online]. Available: https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations
14. F. Johansson, *The Medici Effect*. Boston: Harvard Business Review Press, 2017.
15. T. Rhodes, *Accessing Outcomes and Improving Achievement: Tips and Tools for Using the Rubrics*. Washington, D.C.: Association of American Colleges and Universities, 2009.
16. T. Wagner, *Creating Innovators: The Making of Young People Who Will Change the World*. New York: Scribner, 2012.
17. Army Cyber Institute and AECOM, "Jack Voltaic 2.0 Executive Summary." Accessed on: Sept. 7, 2018. [Online]. Available: https://cyber.army.mil/
18. S. Pell and J. Finocchiaro, "The ethical imperative for a vulnerability equities process and how the common vulnerability scoring system can aid that process," *Connecticut Law Rev.*, vol. 49, no. 5, pp. 1549–1589, 2017.
19. B. Bort, private communication, Nov., 2018.

IEEE COMPUTER SOCIETY DIGITAL LIBRARY
Access all your IEEE Computer Society subscriptions at
computer.org/mysubscriptions