



## Cybersecurity Workforce Preparedness: The Need for More Policy-Focused Education<sup>1</sup>

By Jessica L. Beyer and Sara R. Curran

With the Internet of Things, the computerization of critical infrastructure and other essential processes, the ubiquity of computational technology has increased societal vulnerability. The complexity of cybersecurity questions has grown exponentially as attacks from foreign powers, cybercriminals, and hacktivists have risen. However, as individuals who can translate these politically-based technical challenges into policy have become more essential, degree programs focusing on cybersecurity policy have remained scarce.

This report addresses the need to include cybersecurity policy training as a part of

cybersecurity workforce development. Specifically, we argue that more programs are needed across the country that produce graduates capable of answering questions such as:

- What existing policies address pressing cybersecurity threats? Where are there gray areas exploitable by malicious actors?
- Who has jurisdiction when a major cybersecurity attack occurs?
- What redundancies, contradictions, and gaps are revealed when examining local, state, and federal cybersecurity policy?

- What are the legal obligations towards citizens, clients, or partners when companies or governments are faced with tackling cybersecurity problems?
- What new challenges does the Internet of Things (IoT) bring to the existing domestic and international policy landscapes?
- What new organizational jurisdiction issues does IoT pose?
- What are the different cyberattack strategies of foreign powers, how can we predict their use, how might we hone our attribution methods, and how should the U.S. respond?
- What geopolitical risk information can inform cybersecurity threat preparedness?
- What international legal agreements help and hinder tackling cybercrime, including extradition, data sharing, and investigative cooperation?
- What types of bilateral and multilateral cybersecurity agreements exist and how effective are they?
- As U.S. commerce grows increasingly reliant on IoT technology and the accumulation of related data, how should the U.S. government and corporations navigate the movement of data within and across borders?
- How do we explain the patterns of cyberattack by a nation-state on another nation-state?
- What lessons can be learned from other countries' cyber-strategies?

Individuals who can answer these questions often occupy crucial positions, translating between

policymakers and companies in emergencies and in everyday work, working on behalf of national security, managing cybersecurity-focused software engineers, creating cybersecurity education, deciding company information security, and shaping cybersecurity policy. However, most working in this field come to it in their mid-careers and are self-trained, creating a shortage of workers. As an industry member who works with us stated, "The best we can get is someone with either 80 percent policy knowledge and 20 percent technology knowledge or vice versa—if we could even just push that to 70/30 it would be helpful."

More comprehensive degree programs and certificate opportunities are needed that stand at the cross-section of policy and cybersecurity—creating opportunities for students in technical fields and social science fields alike. These programs must focus on applied experiences working on real problems as defined by external partners from government and industry, simulations and scenarios, and opportunities for making public arguments about cybersecurity policy to leaders in all sectors—government (agencies and elected officials); small, medium, and large businesses; nonprofit organizations; and civil society groups.

## The Cybersecurity Workforce Shortage

While one of the major areas of cybersecurity weakness is professionals with the technical experience to secure our critical infrastructure, there is also a shortage of individuals who can move between the technology and policy world. The individuals who can navigate between the technology and policy worlds will be able to translate between them, shape sound policy

based on a deep understanding of technology and connections in the technology industry, and help navigate overlapping jurisdictions, competencies, and individual rights-based concerns.

Cybersecurity is becoming an increasingly diverse field, consisting of as disparate employment categories as information assurance specialist, computer systems analyst, information and technology manager, law enforcer, policy analyst, and software engineer (NICCS, n.d.; Williams, 2016). One of the fastest growing and urgently identified shortages is at the nexus of cybersecurity policy and technology. Cyber Seek, an interactive tool created with support from National Initiative for Cybersecurity Education (NICE) among others, is meant to help address the cybersecurity workforce gap through illustrating where and what type of cybersecurity jobs are open. As of July 2017, Cyber Seek listed 348,975 jobs as open with a very low supply of workers ready to fulfill these positions. 124,427 of these positions were under the NICE Cybersecurity Workforce Framework Category of “Analyze” and there were 96,430 positions under the “Oversee & Govern” category. Both of these categories are precisely for individuals who can navigate at the nexus of technology and policy with the skills defined by the NICE framework.

## Limited Educational Programs

From corporate boardrooms, to the creation and growth of chief information officers and chief information security offices, to IT managers, there is tangible evidence of the need for individuals who can provide insight and advice about cybersecurity policy (Slaughter & Weingarten, 2016; Damouni, 2016). However, there are limited cybersecurity education opportunities.

Limited cybersecurity educational opportunities are the major cause of the cybersecurity workforce shortage across job types, particularly for undergraduates. In addition to the general shortage of cybersecurity programs, most existing educational programs target mid-career professionals or individuals with undergraduate degrees in hand while Cyber Seek’s research finds that the majority of cybersecurity positions do not require an advanced professional graduate degree.

There are very few undergraduate degrees in cybersecurity, unless one includes information assurance in computer science programs—programs that already are struggling to meet demand. Using the University of Washington’s prestigious Computer Science & Engineering department as an example, its degree program currently estimates that it can only admit one out of every three qualified students into the undergraduate major because there simply is not physical space to house more students. They also serve 5,000 non-majors annually. To attempt to admit more qualified students, they are raising money to build a larger building (Langston, 2015).

Within computer science degree programs where students may focus on cybersecurity technology, students will be exposed to very little policy training. Similarly, cybersecurity training guidelines such as those approved by the Department of Homeland Security (DHS) and National Security Agency (NSA) certified National Centers of Academic Excellence in Cyber Defense (CAE-CD) include only one knowledge unit focused on policy. The policy knowledge unit is meant to, “provide students with an understanding of information assurance in context and the rules and guidelines that control them.”

It includes learning about HIPAA/FERPA, the Computer Security Act of 1987, the Sarbanes-Oxley Act of 2002, the Gramm-Leach-Bliley Act, the Children's Online Privacy Protection Act, Payment Card Industry Data Security Standards, the US Patriot Act, the Americans with Disabilities Act—Section 508, Bring your own device issues, and two very broad categories titled "State, US, and International Standards/Jurisdiction" and "Laws and Authorities." While many of the knowledge units contain very broad categories of required information—such as "legal information" within the "Cyber Threat" category—the lack of specificity in concept categories such as "state, US, and International Standards/Jurisdiction" make it unclear what content and skills programs should provide and what students will actually learn from these knowledge units.

If a non-computer science student wanted to focus on cybersecurity policy, or if a computer science student wanted to add a specialization in policy, there are limited opportunities to do so in the U.S. A review of the top 20 public policy schools in the United States reveals that only four have science and technology programs, all at the graduate level. Of these, only two focus on information policy (University of Michigan and Carnegie Mellon University) and of those, only Carnegie Mellon explicitly focuses on cybersecurity policy. Of the top 20 law schools, only Yale, Harvard, Stanford, and NYU have any focus on information policy. Information schools have more cybersecurity programs that focus on policy, but even among information schools it is only the minority that have programs, all graduate, that focus on cybersecurity—Drexel University, Georgia Institute of Technology, Pennsylvania State University, and University of Pittsburgh.

Most other prominent cybersecurity policy courses are offered through various centers and initiatives, but lack a formal degree at the end or an organized pedagogy that links content and skills across courses. For instance, such associated, but limited, courses exist at Berkeley, Harvard, MIT, Stanford, and the University of Washington.

### *Case Study: Washington State Higher Education*

Using Washington State as a case study, there are six schools that are designated Department of Homeland Security (DHS) and National Security Agency (NSA) certified National Centers of Academic Excellence in Cyber Defense (CAE-CD). To earn this designation, they conform to standardized cybersecurity educational best practices. To be designated as a CAE-CD school, degree programs must closely align with specific cybersecurity-related knowledge units.

Washington State's six schools are: University of Washington, Bothell; University of Washington, Seattle; University of Washington, Tacoma; Highline College; City University of Seattle; and Whatcom Community College. The programs offered are listed below:

- University of Washington, Bothell offers a M.S. in Cyber Security Engineering program. Students entering this program are expected to have previously obtained a B.S. in Computer Science and Software Engineering or equivalent.
- University of Washington, Seattle offers B.S. and M.S. computer science degrees. It also offers a Professional & Continuing Education Program Certificate in Information Systems Security. The certificate is designed for, "software developers and analysts, or people

with system, database, security or network administration experience.” The Information School has a cybersecurity track available to both its Masters and undergraduate students that includes some policy components.

- University of Washington, Tacoma has a Masters of Cybersecurity & Leadership program, which is designed for individuals with at least three years of work experience. It particularly focuses on training military member as they transition out of the military.
- Highline College offers an Applied Bachelor of Science degree in Cybersecurity and Forensics. The degree is open to any student but admissions preference is given to students with an A.S. in Computer Information Science, Information Technology, or Web Development (including some computer information science courses).
- City University of Seattle offers an M.S. degree in Information Security. Students can elect to focus in “Cyber Security Environment,” which is focused on cybersecurity policy issues such as cyber warfare, cyber-crime, e-government, and intellectual property.
- Whatcom Community College offers an A.S. and a B.S. degree in cybersecurity and its program is defined by the CAE-CD guidelines as well as draws upon the NICE guidelines.

With the exception of City University of Seattle’s M.S. degree in Information Security and the University of Washington’s Information School, Washington State cybersecurity education is either entirely focused on computer science-based programs or Master’s level degrees.

## Bridging the Gap in Cybersecurity Policy

There is a critical need for more professionals versed in cybersecurity policy. While technical training that provides “boots on the ground” skills for critical infrastructure protection is deeply needed, it cannot be at the expense of training individuals who can navigate existing policy and recommend appropriate solutions to pressing cybersecurity problems. Such individuals will fulfill key roles inside and outside the private sector. We recommend a cybersecurity policy certificate model that can be shared across universities and is available to technical and non-technical students as well as undergraduates to graduate students.

Policy focused educational opportunities should be available to undergraduates, as well as graduates, so as to more quickly create a cybersecurity workforce. Current educational efforts across cybersecurity target graduate students. Even if undergraduate students never enter the cybersecurity workforce, coursework available to them will increase the cybersecurity literacy of the general population and bring information security practices into other professions.

Any coursework should involve extensive applied experiences, rather than only book and theoretical learning. And, stakeholders in cybersecurity policy should be involved in the creation of coursework and evaluation of student work. Such inclusion would guarantee that there is no gap between what is taught in school and what is needed outside schools. Significant applied experience would include working on real problems as defined by external partners, simulations and scenarios, and opportunities for making public arguments about cybersecurity policy.

The certificate should incorporate the National Centers of Academic Excellence in Cyber Defense Knowledge Units—making students conversant in the technology even if they were not computer science students. Coursework should cover the Policy Knowledge Unit and related units such as “Cyber Threats.” Students would not need computer science degrees to understand and be conversant in the implications of different types of attacks, such as Distributed Denial of Service attacks—likewise, computer science students would be able to discuss the complexities of international Internet governance as it relates to elements such as the Wassenaar Agreement.

The certificate would allow undergraduate and graduate students to focus on cybersecurity policy, increasing the number of professionals with diverse educational backgrounds with cybersecurity policy expertise. A cybersecurity policy program would have the additional benefit of diversifying the technology workforce. Experts in increasing women’s involvement in cybersecurity (another recognized problem) have pointed out that creating more pathways into cybersecurity professions might be a way to diversify the workforce (Slaughter & Weingarten, 2016). Finally, it could help reduce the student pressure on computer science departments, outsourcing policy related teaching to policy experts—thereby strengthening both.

## Sources

Cyber Seek. Accessed August 1, 2017 at <http://cyberseek.org/>

Damouni, N. (2014). “Exclusive: U.S. Companies Seek Cyber Experts for Top Jobs, Board Seats.” Reuters.com. May 30, <http://www.reuters.com/article/us-usa-companies-cybersecurity-exclusive-idUSKBN0EA0BX20140530>

Langston, J. (2015). “Microsoft dedicates \$10M Gift to New UW Computer Science & Engineering Building.” UW Today. June 12, <http://www.washington.edu/news/2015/06/12/microsoft-dedicates-10m-gift-to-new-uw-computer-science-engineering-building/>

National Initiative for Cybersecurity Careers & Studies. “Interactive National Cybersecurity Workforce Framework.” Accessed September 1, 2016 at <https://niccs.us-cert.gov/training/framework>

Slaughter, A. & Weingarten, E. (2016). “Anne-Marie Slaughter: The National Security Issue No One is Talking About.” Time.com. April 12, <http://time.com/4290563/women-in-cybersecurity/>

Williams, T. (2016). “An Inside Look at the Fast-Growing IT Industry’s New and Emerging Jobs.” Goodcall.com. April 5, <https://www.goodcall.com/news/an-inside-look-at-the-fast-growing-it-industrys-new-and-emerging-jobs-05612>





## Endnotes

- 1 The authors gratefully acknowledge early research support from Stacia Lee. We are also grateful for helpful comments on earlier drafts from Joyce Noonan, Agnes Kirk, Bobby O’Brien, Ben Merkel, the Jackson School of International Studies Cybersecurity Initiative Working Group, Sarah Castro, the audience members at the Wilson Center/ Jackson School Bridging the Gap Cybersecurity conference in February 2017 and at the Washington Trade Alliance of Greater Seattle/Jackson School Cybersecurity conference in June 2017. Research for this project was supported by a grant from the Carnegie Corporation of New York and the Jackson Foundation. Thank you to Jennifer Butte-Dahl and Reşat Kasaba for their leadership and providing the venue to this research through the International Policy Institute.

---

*The opinions expressed in this article are those solely of the author.*

## The Wilson Center

-  [wilsoncenter.org](http://wilsoncenter.org)
-  [facebook.com/WoodrowWilsonCenter](https://facebook.com/WoodrowWilsonCenter)
-  [@TheWilsonCenter](https://twitter.com/TheWilsonCenter)
-  202.691.4000

## Digital Futures Program

-  [wilsoncenter.org/program/digital-futures-project](http://wilsoncenter.org/program/digital-futures-project)
-  [digitalfutures@wilsoncenter.org](mailto:digitalfutures@wilsoncenter.org)
-  [facebook.com/WilsonCenterDFP](https://facebook.com/WilsonCenterDFP)
-  [@WilsonCenterDFP](https://twitter.com/WilsonCenterDFP)
-  202.691.4002



## Jessica Beyer

Jessica Beyer is a lecturer in the University of Washington's Jackson School of International Studies and co-directs the International Policy Institute's Cybersecurity Initiative.



## Sara Curran

Sara Curran is Professor of International Studies, Sociology, and Public Policy and Governance at the University of Washington. With Dr. Beyer, she co-directs the International Policy Institute's Cybersecurity Initiative.

Woodrow Wilson International Center for Scholars  
One Woodrow Wilson Plaza  
1300 Pennsylvania Avenue NW  
Washington, DC 20004-3027