NEW AMERICA

FIU FLORIDA INTERNATIONAL UNIVERSITY

November 2018

Cybersecurity Workforce Development: A Primer

Laura Bate

Last edited on October 31, 2018 at 1:58 p.m. EDT

Acknowledgments

The author would like to thank the many experts at New America and beyond who reviewed and offered feedback on early drafts of the paper. She would also like to thank Maria Elkin, Haelee Jo, Nayoon Kim, and Jessica Viteri for their various contributions to the paper and the research that lead to it. Particular thanks goes to Michael Prebil and the Center on Education and Skills at New America for their thoughtful responses to the author's innumerable questions on the finer points of workforce development. This project benefited greatly from their input, and any errors or omissions are entirely the fault of the author.

This paper was produced as part of the Florida International University - New America Cybersecurity Capacity Building Partnership (C2B Partnership).

About the Author(s)

Laura Bate is a policy analyst with the Cybersecurity Initiative at New America.

About New America

We are dedicated to renewing America by continuing the quest to realize our nation's highest ideals, honestly confronting the challenges caused by rapid technological and social change, and seizing the opportunities those changes create.

About Cybersecurity Initiative

The goal of New America's Cybersecurity Initiative is to bring the key attributes of New America's ethos to the cybersecurity policy conversation. In doing so, the Initiative provides a look at issues from fresh perspectives, an emphasis on cross-disciplinary collaboration, a commitment to quality research and events, and dedication to diversity in all its guises. The Initiative seeks to address issues others can't or don't and create impact at scale.

About FIU-New America C2B Partnership

The Cybersecurity Capacity Building (C2B) Partnership is a partnership between Florida International University and New America designed to develop knowledge and policies aimed at building the cybersecurity capacity in the workforce, at the state and local level, within the U.S. government and industry, and internationally.

Contents

Contents Cont'd

Key Points

What Are Cybersecurity Jobs?

Cybersecurity jobs are heterogeneous

The pool of cybersecurity jobs encompasses a broad range of work, which often overlaps with other fields. Acknowledging and delineating the variations in cybersecurity jobs allows policymakers and stakeholders to develop a greater variety of solutions tailored to different specific requirements. Some systems exist to do this, but further work remains.

Degree and experience requirements

Unthinking requirements for degrees and work experience artificially narrow the pool of potential employees. Bachelor's degrees should not be the only entry point into the field, especially in a field that prizes on-the-job experience. For jobs where a bachelor's degree is necessary or enables long-term career growth, conventional degrees can be improved by incorporating work-based learning.

Security clearances and jobs in U.S. government

The intelligence community and military offer some of the few entry points to cybersecurity career paths, but dependence on these pathways means problems with the security clearance process have an outsized impact on the workforce.

The future of cybersecurity jobs

Technological advancements will not fix the workforce gap. Rather, emerging technologies will change the nature of cybersecurity work and requirements for the workforce.

How Do We Teach Cybersecurity?

Organizing higher education around an interdisciplinary field

To develop cybersecurity expertise not just in computer science, but in areas like law, policy, healthcare, and finance, academic decision-makers and the policymakers who define incentives in higher education should consider cybersecurity not as a single, monolithic discipline within higher education, but rather a field that cuts across--and looks very different in--many disciplines.

Mandates for higher education: teaching, research, and sustainability

Cybersecurity can be difficult to teach in a classroom, which exacerbates tensions between competing priorities in higher education. Administrators must forge a path between the university's mandate to facilitate research and prepare students for their future jobs while also ensuring the institution's financial sustainability. Policymakers who set incentives for higher education must reward decisions that lead to a stronger cybersecurity workforce.

Learning cybersecurity outside of higher education

The existence of a diverse array of alternatives to conventional education could enable varying subsets of learners to successfully transition into cybersecurity jobs. These alternatives exist in varying degrees of maturity. Smart policies could guide the development of these alternatives towards best outcomes for students and employers.

Apprenticeships in cybersecurity

Policies to support the growth of apprenticeship as a model for cybersecurity education could have a profound, positive impact on connecting talented individuals with open jobs.

How Do We Measure and Communicate Competence?

Industry certifications

Certifications provide a theoretical framework that could be used to create an entry point into the field, but hiring patterns suggest that the certifications are used as a proxy for work experience more than an indicator of competence. Coupled with the expense of training and testing, this limits the effectiveness of certifications in creating additional entry points into cybersecurity jobs.

Other ways to demonstrate cybersecurity competence

Forums like online platforms and cybersecurity competitions could add to the number and variety of mechanisms for demonstrating competence, but they are not yet to the point of being effectively scalable. Carefully designed hiring policies and funding mechanisms could incentivize growth and best utility of these mechanisms.

What is the Role of Government in Cyber Workforce Development?

Is the U.S. government responsible for growing the nation's cybersecurity workforce?

The U.S. government has a unique responsibility to enable and incentivize growth in the cybersecurity workforce because an inadequate workforce exposes the nation to serious consequences for economic and national security.

What are the policy options available for building a stronger cybersecurity workforce in the United States?

Policymakers at a variety of levels of government can fund the development of research and programs, set their own spending priorities to support particular pathways, facilitate and incentivize opportunities for collaboration among stakeholders, lead by example, and more.

What can the United States learn from cybersecurity workforce development abroad?

Policymakers can look to other governments for examples of varying solutions to the cybersecurity workforce challenge, but they must recognize that many of these solutions cannot function properly in a U.S. context without significant adaptations.

The role of other stakeholders

Businesses and other actors across the cybersecurity community can and should recognize the benefits for their own long-term success in improving the overall state of the workforce, though it is unreasonable to expect them to act out of altruism alone to improve the alignment between cybersecurity education and jobs. Here too, policymakers can incentivize and educate to reduce friction in implementation of novel solutions.

Summary and Introduction

This report unpacks the many issues and questions that collectively make up "the cybersecurity workforce development challenge" in the United States. Our aim is to inform the discussion, make the case that the challenge warrants policy intervention, and highlight areas ripe for further research and policy intervention. We argue that filling cybersecurity jobs is critical for improving U.S. cybersecurity, but that no single action, effort, or theory will address the pervasive difficulties of filling cybersecurity jobs. Instead, lasting solutions will require a network of connected policies and community-wide efforts. Accordingly, the goal of the report is to expand on the range of policy options available rather than to advocate for any one solution. However, the discussion does consider the relative merits of different policies and will endorse those policies that offer particular promise.

Introduction

On March 7, 2017, a group of open-source designers called the Apache Software Foundation released an update fixing a dangerous flaw in Struts, one of their widely-used products. Within 24 hours, servers that had not yet been updated were already under attack.[1] As far as security updates go, this was a tricky one. Experts warned that "patching the security hole was labor-intensive and difficult" because Struts was so frequently and deeply integrated into websites.[2]

On March 9, credit reporting agency Equifax disseminated the official notification of the vulnerability to its internal teams, triggering the company's policy of required patching within 48 hours.[3] The patch was not installed. Equifax's systems—and the deeply sensitive data they held—were left vulnerable. On September 7, Equifax announced they had been victim to one of the internet's largest data breaches, exposing personal information on roughly half of the U.S. population.[4] Over the next two weeks, the company's stock plummeted.[5] Three weeks after the breach, the company's CEO resigned.[6]

Certainly, there were a mix of worrisome factors at play throughout this situation. Among those factors, the Equifax breach shows the critical importance of maintaining a cybersecurity team ready to tackle whatever the internet can throw at system. Currently, U.S. cybersecurity jobs are sitting unfilled by the hundreds of thousands. That is a lot of breaches—and worse—waiting to happen.

At industry conferences and in the halls of government, discussions on cybersecurity workforce development are increasingly prominent. However, stakeholders across the cybersecurity community tend to see "workforce development" not as a single problem to address, but rather as shorthand for a

broad range of issues and subtopics, which makes it especially difficult to evaluate and mitigate the root causes of the preponderance of unfilled cybersecurity jobs.

Lasting solutions will require a network of connected policies and community-wide efforts.

In many spheres, and perhaps reflecting the more conventional narrative, the overwhelming number of unfilled jobs in cybersecurity is a function of simply not having enough people in the education pipeline. Under this model, policy solutions include programs encouraging more middle school students—and especially girls—to pursue studies in science, technology, engineering, and mathematics (STEM); expanding computer science programs at four-year universities; and funding initiatives like CyberCorps[7] that are designed to attract students to cybersecurity and government service.

An alternative school of thought argues that the underlying cause of the seemingly unfillable jobs is not an inadequate supply of talent in the labor market, but rather that the cybersecurity community lacks effective mechanisms to match job seekers with job providers. Possible policy solutions under this second model hinge on better alignment between education and industry and include exploring new ways to measure and communicate workers' competence, greater educational focus on applied skills, and building opportunities for collaboration between educators and employers.

A third set of opinions holds that the constrained hiring environment incentivizes industry leaders to develop their own solutions to fill jobs or reduce the number of employees needed to meet critical functions. For example, increased use of managed service providers could allow employers to outsource their cybersecurity functions to specialized companies that can protect systems and resolve problems more efficiently—and with fewer workers—than each client company could on their own. Meanwhile, technological advancements may reduce the number of employees needed for certain functions like monitoring security logs. According to this logic, the constrained hiring environment itself could drive efficiency and innovation.

For better or worse, all three schools of thought are correct. With the estimated global shortfall of cybersecurity workers close to 3 million,[8] the scale of the problem is great enough that there are plenty of root causes for both narratives to

be accurate in their diagnosis. Beyond simply the size of the workforce, its demographic composition raises serious red flags. Women make up only 24 percent[9] of the cybersecurity workforce and people of color continue to be markedly underrepresented at senior levels,[10] suggesting serious lost opportunities for the cybersecurity industry. Given the need to diversify, expand, and realign, no single approach can address the various problems and incongruities that cause the unfilled jobs. The cybersecurity community needs solutions from a multitude of schools of thought, each of which can ameliorate some part of the larger issue.

→ DIVERSITY IN CYBERSECURITY

Lack of diversity is a particularly weighty topic when it comes to cybersecurity workforce development. New America runs a project dedicated to this issue called Humans of Cybersecurity, which we encourage readers to visit at **newamerica.org/cybersecurity-initiative/humans-of-cybersecurity**. However important, gender and racial diversity in the workforce is not explicitly discussed at length in this report. The topic warrants a report unto itself.

Increasing diversity in the cybersecurity workforce is a fundamental and cross-cutting goal in all aspects of cybersecurity workforce development. Accepting that conventional hiring practices and educational pathways have led the community to its current homogenous state, we conclude that creating alternative educational opportunities and entry points into the field serves to incorporate greater diversity, particularly when carried out in conjunction with efforts specifically targeted at increasing diversity in the workforce. Current talent pools—largely university computer science and engineering programs and the existing cybersecurity workforce—are overwhelmingly white and male. By finding different pools of talent and means for drawing them into the cybersecurity workforce, the community can not only grow more rapidly, but can also incorporate a broader demographic range (not to mention a broader range of work experience and neurodiversity). By seeking alternative pathways to cybersecurity education, this report endeavors to serve both ends, which makes the workforce not only larger, but also stronger.

Herein lies the challenge of U.S. cybersecurity workforce development: There is no single underlying problem, but rather an interconnected and multifaceted

array of issues that ties together K12 education, diversity and inclusion, higher education, industry certifications and competencies, military and intelligence recruitment, apprenticeship and work-based learning, veterans' employment, federal hiring practices, and much more. There are substantial and complex discussions to be explored in each and every one of these areas. The "cybersecurity workforce development conversation" is really a network of conversations. There is no one policy change that will resolve the issue. Solutions must rely on input from stakeholders from the whole economy, and will involve interconnected efforts across the entirety of the cybersecurity ecosystem.

Virtually the entire global economy has a stake in building a stronger cybersecurity workforce. Why then should policymakers make it their job to address this issue particularly? Amidst competing priorities and limited resources, what sets the cybersecurity workforce apart as a policy issue? The answer lies in national security and economic stability. Because different states, cultures, and government structures have different expectations and means for providing security and stability, the answer will vary across national contexts. This report focuses on the United States; however, many lessons will translate to other contexts, and there is much the United States can learn by observing other governments.

There is no doubt that many cybersecurity roles are intended to "provide for the common defence,"[11] though it is true that the national security implications of cybersecurity work vary across roles inside and outside of government. There is no official count of the number of cybersecurity workers working for the federal government,[12] much less in state and local governments. However, it is clear that the government is naturally positioned as a major consumer of cybersecurity talent because it must deliver the workers needed to serve not just the military and the intelligence community, but also the individual information security needs of each of the federal departments and throughout state and local governments. Strong national security relies on a ready supply of cybersecurity talent to fulfill missions like securing command and control systems in the military's theaters of operations, monitoring communication networks for violent extremism, protecting our democratic institutions, informing a robust conversation on internet security and privacy, and securing citizens' sensitive data.

A strong cybersecurity workforce is also critical to economic stability. Economic growth and innovation depends on fundamentals like secure financial transactions and reliable intellectual property rights. Banks must ensure they can safely hold and move financial assets, and inventors must protect their new designs to reap economic returns on their work. Data breaches and other cyberattacks are driving up the costs of doing business in an interconnected world. In a report examining possible economic futures, researchers outlined the problem rather starkly, saying that "annual cybersecurity costs in high-income economies like the U.S. have already begun to outweigh the annual economic

benefits arising from global connectivity."[13] Future economic prosperity depends on curbing the growing costs of cybersecurity, which in turn depends on having the workforce needed to prevent costly attacks. Because of the exigency of the economic and the national security cases for a strong cybersecurity workforce, developing that workforce is more than just an industry-wide challenge; it is grounds for policy intervention.

Developing the cybersecurity workforce is more than just an industry-wide challenge; it is grounds for policy intervention.

This report will explore critical questions in designing policy to enable and incentivize changes to spur growth in the cybersecurity workforce.

- **What are cybersecurity jobs?** Section One outlines different taxonomies and frameworks for understanding the diverse work lumped into the category of "cybersecurity." It also describes patterns in cybersecurity hiring and considers whether these patterns are effective for workforce development.

- **How do we teach cybersecurity?** Section Two will detail challenges in teaching cybersecurity in a conventional classroom environment and explore alternatives that may help address those challenges.

- **How do we measure and communicate competence in cybersecurity hiring?** Section Three explores this question.

- **What is the role of government in cybersecurity workforce development?** Section Four explores the U.S. government's obligation to building the cybersecurity workforce.

Finally, the report will conclude by outlining opportunities for further research.

This report presents a range of views on the topics above in order to best illustrate the state of these critical and complex debates. While there are no easy answers, some options are certainly better than others, and this report does take positions on which are the best options.

Section One: What are Cybersecurity Jobs?

Detailed research that monitors and quantifies the cybersecurity workforce is hard to come by. One of the few points that has been consistently measured is the very top-line number: How many people work in cybersecurity? In 2010, experts estimated that there were 2.28 million information security[14] professionals employed worldwide.[15] By 2015, there were 4.24 million professionals, almost almost twice as many as five years prior.

Observers soon started measuring not just the total number of professionals employed, but also projections of the future difference between open cybersecurity jobs and the expected number of workers entering the industry. In 2015, the anticipated global shortfall was expected to reach 1.5 million unfilled jobs by 2020;[16] in 2017, the estimate was 1.8 million by 2022;[17] and the estimated current-day gap is close to 3 million.[18] The trend is hard to ignore. However you define them, it is clear that unfilled cybersecurity jobs in the field are emerging at a dramatically increasing rate.

But other than indicating a need for more workers, what do those numbers really say? It is hard to infer much meaning simply because "the cybersecurity workforce" is a malleable term. Efforts to define and classify "cybersecurity jobs" are only just beginning to see common use, and as cybersecurity becomes an increasingly critical part of virtually every industry, the number of non-technical roles that require some amount of cybersecurity expertise is growing quickly.

Cybersecurity Jobs are Heterogeneous

> *The pool of cybersecurity jobs encompasses a broad range of work, which often overlaps with other fields. Acknowledging and delineating the variations in cybersecurity jobs allows policymakers and stakeholders to develop a greater variety of solutions tailored to different specific requirements. Some systems exist to do this, but further work remains.*

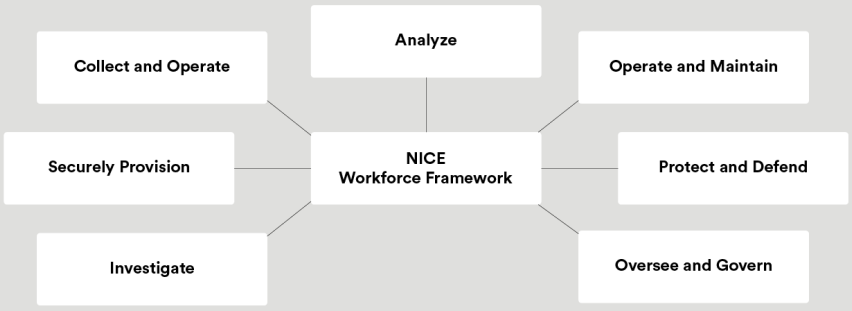
The National Initiative on Cybersecurity Education (NICE), an office within the National Institute of Standards and Technology, has undertaken the daunting task of standardizing the language and taxonomy used to describe work in cybersecurity. (Disclosure: Some of the Cybersecurity Initiative work is funded by NIST/NICE. They did not provide any financial support for this publication.) The NICE Cybersecurity Workforce Framework[19]—a self-described "non-prescriptive cybersecurity workforce dictionary"— was first posted for public

comment in 2012, and since has been informed by extensive outreach to the cybersecurity community.

In 2015, the anticipated global shortfall was expected to reach 1.5 million unfilled jobs by 2020; in 2017, the estimate was 1.8 million by 2022; and the estimated current-day gap is close to 3 million.

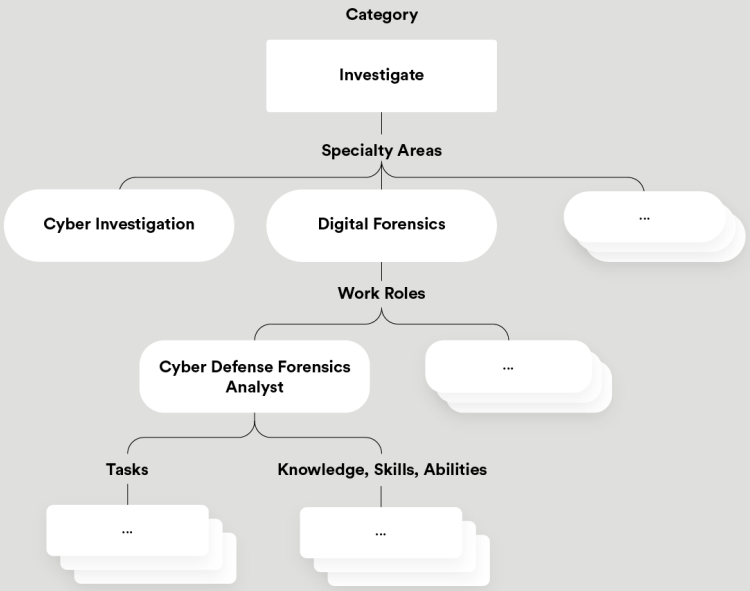
The framework sorts the industry into seven categories, depicted in Figure 1, which then divide into 32 specialty areas, which further separate into specific work roles, each detailed with tasks expected and the knowledge, skills, and abilities required to be successful in that specific work role. For example, "Investigate" is one of the seven categories defined. "Digital Forensics" is a specialty area within the "Investigate" category. "Cyber Defense Forensic Analyst" is a job role within "Digital Forensics," and one expected task is "Conduct[ing] analysis of log files, evidence, and other information to determine best methods for identifying the perpetrator(s) of a network intrusion."[20] These relationships are depicted in Figure 2.

Figure 1 | Overview of the Categories of the NICE Workforce Framework



NEW AMERICA

Figure 2 | An Example of the Levels of the NICE Workforce Framework



NEW AMERICA

The NICE framework helps provide a common lexicon, but it is not used universally. Many bureaucracies have legacy frameworks that do not map directly to the NICE framework, and the human resources restructuring necessary for implementation is seen as burdensome relative to the potential benefits of standardization. Other employers, particularly those that have deep experience in information security, prefer to stay with their own understandings of cybersecurity jobs. While this variation is not a bad thing, it makes it difficult to measure statistics and trends across the industry. Without that kind of empirical data, it is hard to design policies that respond to real-world demands.

There is another category of work that is not generally—and arguably *should* not always be—captured in the NICE framework, and may require its own taxonomy. Sometimes called "hybrid jobs,"[21] these are jobs that touch on cybersecurity, but are not, strictly speaking, based in the same discipline. The NICE framework addresses some of what might be called "hybrid jobs" (e.g. cybersecurity legal advisors, hiring managers, and instructors).

Trying to include all hybrid jobs would dilute the utility of the framework. Does one include a company executive in charge of risk management? Currently, this would not generally fall within the framework, but clearly this individual would

need to have a very firm understanding of the company's cybersecurity risk profile to perform their job effectively. Similarly, a legislative assistant who advises on national cybersecurity policy must also be cybersecurity experts in their own fashion.

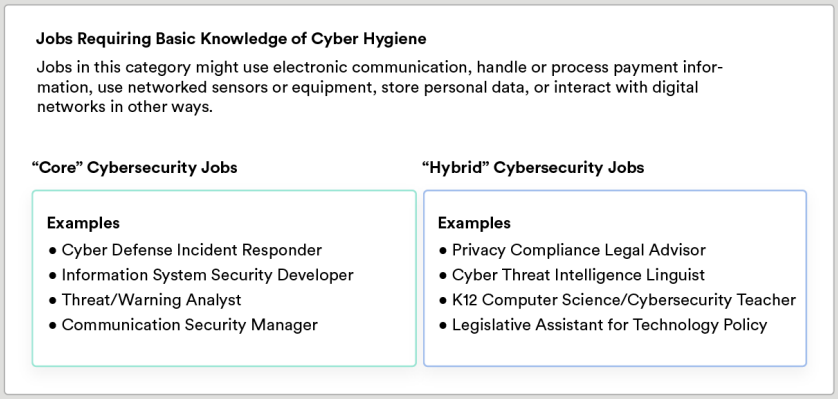
When any employee can accidentally fall for a phishing scam and expose that core product to harm, it becomes important for all employees to understand the basics of good cyber hygiene.

The converse is also true. In many cases, sector-specific knowledge is essential to enable a cybersecurity expert to work effectively. For example, cybersecurity in financial services is a discipline in its own right.[22] Experts in these jobs need to understand not just cybersecurity itself, but the nuances of the complex regulatory framework that protects everything from consumer data to the international banking networks that enable financial transactions.

Virtually every sector of the economy benefits from a certain amount of cybersecurity awareness. Networked information systems are critical to the core functions of most businesses. For example, Goldman Sachs CEO Lloyd Blankfein has famously declared, "We are a technology firm."[23] JPMorgan CFO Marianne Lake has expressed a similar sentiment,[24] and they are not alone. Increasingly, companies' core products are becoming their digital tools and systems. When any employee can accidentally fall for a phishing scam and expose that core product to harm, it becomes important for all employees to understand the basics of good cyber hygiene.

Clearly, not every employee with access to email should be considered a cybersecurity worker, for all that good cyber hygiene may be critical to success. It becomes increasingly difficult to know where to draw the line in terms of what is or is not considered part of the cybersecurity workforce. This report does not define a line separating "cybersecurity" from "not cybersecurity," but rather treats cybersecurity jobs as overlapping sets of roles ranging from the types of positions that fall within a conventional understanding of cybersecurity to experts with hybrid jobs—those positions where cybersecurity and another specialty are functionally inseparable—to virtually every position that benefits from increased cybersecurity awareness.

Figure 3 | Relationship between Types of Cybersecurity Jobs



NEW AMERICA

Degree and Experience Requirements

> *Unthinking requirements for degrees and work experience artificially narrow the pool of potential employees. Bachelor's degrees should not be the only entry point into the field, especially in a field that prizes on-the-job experience. For those jobs where a bachelor's degree is necessary or enables long-term career growth, conventional degrees can be improved by incorporating work-based learning.*

One of the challenges of evaluating the cybersecurity workforce is simply that very little data exists to use as a benchmark against which to measure changing trends. Organizations like (ISC)2 (The International Information System Security Certificate Consortium)[25] measure some high-level numbers like the total number of cybersecurity workers globally, and NICE, CompTIA, and Burning Glass have jointly built CyberSeek, a tool that monitors data on job postings in the United States that fall within the NICE workforce framework and the industry certifications that are in demand.[26]

Even with these resources, there are significant gaps in the data, often filled by anecdotes or assumptions. For example: How many jobs in other sectors or functions require significant cybersecurity expertise? How many cybersecurity experts were trained initially by the intelligence community or military? How many are trained in higher education institutions? How many learn in informal

settings—on-the-job or through self-teaching—and, without a degree, how do they market themselves to employers? To what extent are recent graduates hired into cybersecurity positions in the private sector? In the public sector?

Many narratives exist describing typical career paths and entry points into the cybersecurity job market. Observers might hear that most experts cut their teeth in government; experts are recruited into the private sector from capture the flag competitions (CTFs);[27] computer science graduates do (or do not) make good hackers. Most of these observations are based on intuition or anecdotes. The data to indicate which entry points, training programs, or hiring strategies are most effective—or even most common—is extremely limited.

The data that exists is most often drawn from job postings, which shapes the data itself. For example, a job posting may require years of work experience and a graduate degree, but an employer may not be able to find (or afford) someone with those qualifications, and may hire someone more junior with the expectation of training them. Thus accountings of requirements in job postings probably inflate the characteristics of workers in the field. However, job posting data remains the best proxy available for insight into what employers are seeking, and there are certainly notable points in the data. Among the key takeaways: 84 percent of job postings in the industry list a bachelor's degree as a minimum qualification, and 83 percent of job postings in cybersecurity require at least three years of work experience.[28] Requirements like this are increasingly facing criticism as unattainable, unrealistic, or unnecessary.[29] Or, as some have said more bluntly, "There is no cyber talent crunch; you're just hiring wrong."[30]

The data to indicate which entry points, training programs, or hiring strategies are most effective—or even most common—is extremely limited.

Of course, hiring requirements are not inherently bad. They allow hiring managers to focus in on a pool mostly likely to meet their needs. But are these requirements actually effective filters in cybersecurity? Setting aside the work experience requirement for a moment, the requirement for a degree creates problems both in terms of the number of graduates available and the applicability of the degrees to cybersecurity jobs.

As a question of numbers alone, there simply are not enough graduates to fill available jobs, particularly when recalling that the estimated global cybersecurity

labor shortage currently is close to 3 million unfilled jobs.[31] U.S. post-secondary institutions were expected to confer just over 1.8 million bachelor's degrees *total* —in all disciplines—in academic year 2017-2018.[32] There is little in the way of data to indicate of how many students in a graduating class are likely to seek jobs in cybersecurity, but as a point of comparison, in academic year 2015-2016,[33] 64,405 bachelor's degrees were awarded in computer and information sciences in the United States.[34] Even allowing for the fact that some 35 percent of U.S. cybersecurity employees come from other fields of study,[35] it is still quite clear that an adequate supply of graduates simply will not exist if current hiring requirements remain unchanged.

Not only will the supply of graduates be unavailable in terms of total numbers, experts are raising questions about whether or not a bachelor's degree really does make an employee more effective in the workplace. Across industries, researchers have documented "degree inflation," employers seeking candidates who hold degrees for positions that have traditionally been filled by workers without one.[36] President of Opportunity@Work Byron Auguste highlights an example of this trend among administrative assistants. "When only 20 percent of administrative assistants have a bachelor's degree but almost two-thirds of new job postings for admins require a B.A. to be considered, such practices make college degrees more of an arbitrary barrier than an inclusive bridge to middle-class work."[37] Information technology disciplines are coming to a similar realization, increasingly recognizing the presence of "middle-skill" jobs[38]— jobs that "require more education and training than a high school diploma but less than a four-year college degree."[39]

In cybersecurity, as in many other fields, hiring managers would benefit from asking whether a four-year degree is necessary for a given position, or whether on-the-job learning, career technical education through a community college, or other training options may be a better fit. Apprenti—an organization that works with industry partners to build apprenticeships and has led a U.S. Department of Labor-funded effort to expand apprenticeship in information technology—worked with their clients to determine what roles required a bachelor's degree. Of their mid-tier work roles (the overarching category that includes cybersecurity roles), they found that some 40 percent can be effectively filled by workers without a bachelor's degree.[40]

There is a strong argument that workers with diverse educational backgrounds, rather than a workforce comprised exclusively of graduates of four-year degree programs in STEM, are particularly well equipped for the challenges in cybersecurity.[41] Not all users of cybersecurity products approach security products and systems from the same starting point, so why should product designers? Rather, a workforce with a mix of degrees, informal education, and other experiences better represents the diverse population likely to use those products.

This is not to devalue a four-year degree (or any degree) in career development, nor to suggest that career and technical education (CTE) is the right answer in all cases. Some positions do require a bachelor's degree—or master's or doctoral degree. In some cases, a degree may ensure better long-term outcomes than CTE for an employee who seeks to advance to positions, particularly in management, that benefit from exposure to general education requirements.

Research shows a good economic case for incorporating a bachelor's degree as part of a long-term career. One review of studies showed a lifetime average present-value earnings benefit of $423,800 for those with a four-year degree.[42] Douglas Webber of Temple University found that "the typical college graduate will earn roughly $900,000 more than the typical high school graduate over their working life," but he strongly cautions that this is just an average.[43] For an individual pursuing work in cybersecurity, this suggests that earning a degree at some point in their career makes sense, at least from a statistical standpoint. From an industry perspective, requiring that degree in all cases—and particularly for entry-level jobs—creates problems.

Notably, only 23 percent of cybersecurity industry experts feel that educational programs are graduating students with the skills needed to be useful in the workplace. In surveys, experts indicate a preference for hands-on experience and certifications over a bachelor's degree.[44] This would seem to contradict the widespread minimum requirement of a bachelor's degree. Why require a degree if experience is considered more valuable? Some experts have attributed this seeming inconsistency to a lack of communication between subject matter experts initiating the hiring process and the human resources professionals actually posting the jobs. The researchers who conducted this particular survey suggest, "This contradiction indicates that a degree is more of a signal of general competence than an indicator of directly relevant cybersecurity skills."[45] Thus the degree becomes a means for signaling skills that are harder to quantify and demonstrate, like collegiality and perseverance. Regardless of the rationale that drives it, the degree requirement appears to be more of a default than a deliberate strategic choice, and warrants more explicit examination.

What, then, is the anticipated career pathway into the cybersecurity industry? As it currently stands, the typical requirement for four-year degrees and work experience means that the cybersecurity community is limiting their hiring search to college graduates, but providing no path for newly-minted graduates to get the experience needed to enter the field.

Security Clearances and Jobs in U.S. Government

The intelligence community and military offer some of the few entry points to cybersecurity career paths, but dependence on these pathways means that problems with the security clearance process have an outsized impact on the workforce.

There is anecdotal indication that some employers do hire entry-level professionals at a meaningful scale, particularly in federal government agencies and larger corporations that can afford their own internal training programs. On a systemic level, this model raises two questions. First, to what extent are these internal (and largely proprietary) trainings contributing to the overall workforce? Without adequate data on the size and retention rates of these workforces, it is hard to observe the impact of this pathway into the industry. Second, absent outside incentives, why would employers continue to bear the cost of internal training programs when employees may complete training and then leave for more lucrative positions with employers that elect to spend more on salaries and less on training?

Insofar as entry-level jobs can be found in the federal government, more than 10 percent of cybersecurity job postings require a security clearance.[46] Ten percent may not seem like an overwhelming portion of the market, but given that government training appears to be one of the few truly entry-level pathways into work in cybersecurity, bottlenecks here are particularly problematic. Because human capital is flowing in through government to feed not just public sector national security jobs, but the whole of the cybersecurity ecosystem, when potential new hires are deterred by the clearance process and encounter a cybersecurity job market with limited or unattainable alternative entry points, they are liable to seek out not just other employers, but other industries entirely. In this way, troubled hiring practices in national security roles have an outsized impact on the rest of the cybersecurity community.

Security clearances are a necessary part of national security work, but the current process is unduly slow[47] and would benefit from even the most basic reforms.[48] According to Senator Mark Warner, Vice Chairman of the Senate Select Committee on Intelligence:

> The U.S. government requires a well-functioning system for granting security clearances to make sure we have a workforce who can be trusted with our nation's secrets. But the current system, born in the

> wake of World War II, when classified documents lived on paper and Telex, is simply too time-consuming, too expensive and too complex.[49]

Even Director of National Intelligence Dan Coats has proclaimed that "The process is broken. It needs to be reformed."[50]

→ AUTHOR'S NOTE

How does military and intelligence training impact the workforce?

There is an interesting related question on whether limited retention in federal positions has a larger systemic benefit, behaving like a subsidy to the cybersecurity industry in the form of workforce development. Government invests in training talent that then moves on to private sector employment after a relatively short time in government. This is no doubt frustrating for government hiring managers, but does feed the larger community. An excellent area for future research would be to study this flow of talent to learn what percentage of the overall U.S. cybersecurity workforce is receiving its training from the military and intelligence communities. Furthermore, what are the costs of this to the federal government? What are the economic benefits to the rest of the cybersecurity community? What would comparable education cost if conducted outside of government?

Where the cybersecurity workforce is concerned, the long timeline of the security clearance process sets up several very harmful dynamics. First, as reporting from the Government Accountability Office (GAO) suggests, prospective employees may simply choose to avoid government service to avoid the wait times and uncertainty inherent in the process.[51] Second, this encourages contracting firms to lure cleared civilian and military employees away from their public sector jobs rather than pay to clear employees themselves. Third, the clearance cost and timeline discourages movement and interaction between private and public sector by making it hard for experts to transition in and out of cleared jobs over the course of their careers.

The realities of national security work are such that eliminating the necessity for security clearances will almost certainly never be possible. Security clearance reform, however, is a reasonable target. Advocates suggest that government agencies can move away from periodic reinvestigations and towards continuing

evaluation, "a process to review the background of clearance holders and individuals in sensitive positions at any time during the eligibility period."[52] Such monitoring is predominantly automated and occurs in real time. By monitoring records on an ongoing basis, a police arrest or other indication of worrisome circumstances is likely to come to light before a scheduled reinvestigation. In fact, certain parts of the Department of Defense and the Office of the Director of National Intelligence are already developing continuing evaluation programs.[53] Such practices could improve and expedite hiring, alleviating the bottleneck to accessing many cybersecurity jobs.

The Future of Cybersecurity Jobs

> Technological advancements will not fix the workforce gap. Rather, emerging technologies will change the nature of cybersecurity work and requirements for the workforce.

To further complicate the meaning of "cybersecurity jobs," savvy members of the cybersecurity ecosystem must also consider not just what these jobs are now, but what they will be in five, 10, and 20 years. The widely held belief is that automation will change at least some aspects of cybersecurity jobs. Those tasks and audits that can be done by an artificial intelligence (AI) program may decrease the overall quantity of work to be done, which some speculate will bring welcome relief for the often overtaxed workforce.[54]

Others point out that the introduction of these tools will also herald the advent of new AI-enabled threats, not to mention new targets.[55] This suggests that the overall workforce demand will not lessen so much it will as shift from one specialty to another. Future employees would need to be well versed in AI and machine learning tools. A survey by the Ponemon Institute suggests that many practitioners predict that "automation will increase the need to hire people with more advanced skills,"[56] making it even harder to meet the workforce needs of the cybersecurity industry. While technology may change the requirements for the workforce, it will not fundamentally change the challenge of connecting educational pathways with jobs that require experience on very specific tools.

The current system of cybersecurity education is inadequate for job seekers and employers, and without efforts targeted at broadening and realigning how we teach and hire cybersecurity skills, there is little reason to expect improvement. The barriers new employees must overcome to enter the field and gain their first years of experience push the cybersecurity community towards a tendency to hire experienced employees out of the public sector or competing firms,[57] which discourages employers from funding workforce training when that training is

quite likely to ultimately benefit a competitor when the employee is eventually poached. Full of self-defeating paradoxes, hiring assumptions determined by habit rather than intention, and spotty coordination between educators and employers, the cybersecurity community's current strategy for workforce development desperately needs a redesign.

Section Two: How Do We Teach Cybersecurity?

The default system for education in cybersecurity—a bachelor's degree—has much to recommend it; it is already the cultural norm throughout much of the upwardly-mobile American workforce. But the structure of a typical bachelor's degree program is not always ideal for teaching cybersecurity. Options outside of higher education—e.g. bootcamp-style training programs or the military—are also not universally appropriate. This conundrum offers a unique opportunity to pursue work-based learning options that would be remarkably innovative in the cybersecurity community.

This report does not delve into education at the kindergarten through twelfth grade (K12) level, but that is not to imply that it is irrelevant here. Research indicates that students' attitudes towards STEM tend to decline dramatically around the ages of 10-14.[58] Accordingly, a central challenge in long-term cybersecurity workforce development focuses on engaging students in STEM fields prior to and during that time frame, but the topic does not end there. In order to benefit from emerging interest in STEM fields, schools must have the teachers and resources to provide instruction in these areas. Only 40 percent of K12 principles say that their school offers a computer science class that teaches a coding language, but 90 percent of parents say that opportunities to learn computer science are a good use of school resources.[59] Clearly there is room to expand.

The structure of a typical bachelor's degree program is not always ideal for teaching cybersecurity. Options outside of higher education—e.g. bootcamp-style training programs or the military—are also not universally appropriate.

An interesting feature of discussions on K12 cybersecurity education is that the policy levers to shape priorities and incentives exist predominantly among state, local, territorial, and tribal governments. Meanwhile, an active community of stakeholders are working to develop mechanisms to encourage and promote education that could lead to long-term development of the cybersecurity workforce. This complex ecosystem overlaps with the discussion in this report. However, because the policy solutions are quite different at the K12 level, this

report acknowledges the important influence that these years have on later education and opportunities, and begins exploring the educational system at the level of higher education.

Organizing Higher Education around an Interdisciplinary Field

> *To develop cybersecurity expertise not just in computer science, but areas like law, policy, healthcare, and finance, academic decision-makers and the policymakers who define incentives in higher education should consider cybersecurity not as a single, monolithic discipline within higher education, but rather a field that cuts across—and looks very different in—many disciplines.*

Among the characteristics that make it difficult to teach in a degree program, cybersecurity is a "multidisciplinary problem, touching on policy issues, economic incentives, and public and business awareness and education, along with new technical challenges."[60] Programs that teach cybersecurity effectively must also incorporate elements from many fields, which could encourage innovative approaches from the outset. In theory, this basis in outside-the-box thinking could provide an excellent starting point for further innovation. This tends to be very difficult to implement in higher education systems historically segmented into different departments and colleges within a single university.

Where they *are* taught, cybersecurity programs are often folded into another field within computer science or engineering departments. This is appropriate insofar as cybersecurity exists within the context of technical systems—computers and networks—but it can also limit the growth of cybersecurity as an educational priority outside these departments or as an independent field. Organizations like ABET (Accreditation Board for Engineering and Technology) and the National Security Agency and Department of Homeland Security's Centers of Academic Excellence programs provide useful frameworks around the content to be taught, but do not answer these more fundamental questions about cybersecurity as a field of study.[61]

Computer science and engineering disciplines have historically been the focus of cybersecurity curriculum development. One particularly well-developed example of such an effort is the Joint Task Force on Cybersecurity Education, a "collaboration between major international computing societies."[62] The curriculum is meticulously developed and reviewed by academic experts. While the task force very clearly acknowledges cybersecurity's interdisciplinary nature, the curriculum is targeted at an understanding of the field that "advances cybersecurity as a new computing discipline and positions the cybersecurity curricular guidance within the context of the current set of defined computing

disciplines," which include computer engineering, computer science, information systems, information technology, software technology.[63] Quite sensibly, the Joint Task Force has housed this effort squarely in computing disciplines.

The curriculum development effort does not end here. Other academic disciplines could emulate this work. While the Joint Task Force has incorporated legal, economical, and political considerations into their curriculum guidance,[64] that incorporation does not replace curriculum development efforts for cybersecurity in each of those disciplines. The draft curriculum proposes teaching a reasonable array of policy principles for a student who expects to do research in a computer science department, but certainly not for a student interested in working for a legislator's office informing data privacy policy. Educating the future policy wonk requires a very different cybersecurity curriculum[65] and maybe even a different pedagogic framework.[66] Given that cybersecurity jobs are increasingly crossing into other domains like finance, healthcare, and law, the same could be said for any number of other examples.

Although some colleges and universities have taken on the challenge of developing such interdisciplinary programs, practical considerations like interdepartmental cost sharing, program equities, and the enduring assumptions about where cybersecurity coursework should be anchored often slow down the development of cybersecurity as a cross-cutting field, (or meta-field, as scholars have termed it[67]) applicable and accessible to many disciplines. The work that academics in computer science and engineering are doing to identify best practices in cybersecurity curriculums is invaluable and critical. However, such efforts should be part of a larger ecosystem of offerings that teach the aspects of cybersecurity most relevant to industries ranging from law to hospitality to medicine to policy and much more.

Mandates for Higher Education: Teaching, Research, and Sustainability

> *Cybersecurity can be difficult to teach in a classroom, which exacerbates tensions between competing priorities in higher education. Administrators must forge a path between the university's mandate to facilitate research and prepare students for their future jobs while also ensuring the institution's financial sustainability. Policymakers who set incentives for higher education must reward decisions that lead to a stronger cybersecurity workforce.*

Apart from the theoretical challenge of finding a home for cybersecurity programs in a university setting, the discipline also creates practical challenges.

Cybersecurity changes quickly. As *New York Times* reporter and Harvard University adjunct lecturer David Sanger puts it, "The hardest thing about teaching anything about cybersecurity is the same thing that's the hard part about writing and reporting about cybersecurity, which is, it's moving so fast."[68] This makes it difficult to keep conventional classroom education up-to-date, especially when curricula can take weeks and months to make and approve. Automated cybersecurity attacks "are happening in microseconds… so today all we can do is patch and pray," according to Dr. Arati Prabhakar, formerly the head of the Defense Advanced Research Projects Agency (DARPA) and of the National Institute of Standards and Technology (NIST). She adds, "we are looking for a fundamentally different way to get faster than the pace of the growth of the threat."[69] In an already rapidly developing industry, cutting edge technologies give way to newer tools in the span of weeks and months, a timeline prohibitively difficult to maintain in syllabi developed over much longer timelines.

As difficult as maintaining a current syllabus can be, finding teachers with experience to teach the most current techniques and tools is equally challenging. Applied courses are often taught by instructors and adjunct professors, but they are expensive to hire given competition for experts with these skill sets. Tenured faculty are generally focused on foundational research within a narrow specialty, not the newest bit of technology.

The hardest thing about teaching anything about cybersecurity is the same thing that's the hard part about writing and reporting about cybersecurity, which is, it's moving so fast.

Maintaining a focus on foundational education and research allows faculty to cultivate and attract top-tier graduate students to aid in that research, which fosters a fertile environment for the research and development that keeps cybersecurity on the cutting edge. Educators are also charged with the mandate that "students must be encouraged to think and learn, with the understanding that specific content isn't as important as it would be in training scenarios."[70] These functions are critically important to the university, to the general health of the cybersecurity research community, and to the workforce writ large, but do not answer the question of where students will learn the tools and skills that will be required to enter a career in industry.

This tension between a university's teaching and research mandates is part of a much larger conversation on the role of higher education in society. Should universities (and research universities in particular) exist to train the workers that will build the future economy, or should their purpose be to cultivate the hotbeds of innovation and deep research that fuel growth and stand as a hallmark of the U.S.'s comparative economic advantage? This question is not a central focus of this report, but understanding the role of the university is important context in considering the potential impact of higher education on the cybersecurity workforce.

Highlighting the crux of this uncertain role for institutions of higher education, Arizona State University (ASU) President Michael Crow and ASU Senior Research Fellow William B. Dabars emphasize that "the inherent limitations of the present model [of research universities] attenuate the potential of this set of institutions to educate citizens in sufficient numbers and address the host of challenges that beset the world."[71] They write about universities' limitations generally, but in the cybersecurity context, this line of thinking leads to real questions about whether universities can adapt to create capable workers in addition to highly trained researchers. In an industry that desperately requires both types of experts—and many types in between—developing a spectrum of educational offerings is a particularly valuable strategy. Much as the medical field has different educational paths for surgeons, pharmaceutical researchers, technicians, and nurses, a thriving cybersecurity community will require a breadth of educational paths.

The role of the university not only oscillates between research and teaching mandates. Economic considerations also factor into any university's operations. Given the demand from recent baccalaureate graduates and mid-career job changers for opportunities to break into a lucrative cybersecurity career, developing a professional master's in cybersecurity may seem like a sound investment for any university administration. However, higher education occasionally finds itself walking an uncomfortable tightrope when it comes to this type of professional graduate degree program.

Such programs are known for their profitability. Adjusted for inflation, tuition for an average graduate degree program in 1989 cost $6,603. In 2010, it cost $14,398.[72] This steep rise in cost reflects greater demand for such degrees, which has created a very tempting revenue stream for administrators at often funding-starved schools.[73] The resulting incentive structure can encourage universities to provide expensive professional graduate degrees designed for profit[74] rather than beneficial student outcomes. With so little data available on what kind of education or training yields best long-term student outcomes in a cybersecurity career—not to mention lukewarm industry attitudes towards skills learned in the classroom rather than on the job—universities offering a professional master's in cybersecurity must carefully weigh financial priorities and social responsibility.

Learning Cybersecurity Outside of Higher Education

The existence of a diverse array of alternatives to conventional education could enable learners to successfully transition into cybersecurity jobs. These alternatives exist in varying degrees of maturity. Smart policies could guide the development of these alternatives towards best outcomes for students and employers.

Anecdotally, many cybersecurity employees in industry are trained in either the military or the intelligence community, rather than passing through academia. Statistics describing the exact scale of this pattern are hard to come by. There are good reasons why military and intelligence agencies would be reluctant to publish personnel statistics, but consequently it is very difficult to know what proportion of the cybersecurity workforce passes through government service. The Global Information Security Workforce Study says 16 percent of hiring managers prefer to recruit among former and active military, and 30 percent of the workforce comes from a non-technical background, which can include "business, marketing, finance, accounting, or military and defense."[75] An especially useful question to answer would be what percentage of the workforce was trained in the military or intelligence community, and what are the long-term work roles and outcomes for those individuals.

Bootcamps and skills-based short courses provide other potential pathways into the workforce. They have a long history of teaching workplace-relevant skills from stenography to coding.[76] Despite this long history, not all examples are positive. Some bootcamps face criticism for over-promising and under-delivering,[77] a trend that warrants a note of caution among proponents of skills-based courses.

Cybersecurity bootcamps do not have the numbers seen among their coding bootcamp cousins, but they are already gaining a profile as a viable alternative training option.[78] It is uncertain whether they will remain on this promising trajectory or struggle with the challenges that have beset many coding bootcamps. Among these coding camps, surveys indicate 60 percent of bootcamp completers already had a bachelor's degree, and graduates averaged 6.8 years of work experience,[79] which does not seem to be the entry-level path to success one might hope for. The same study indicated that 43 percent of coding bootcamp students were women,[80] suggesting that this pathway may help break down longstanding gender imbalances in information technology (IT) disciplines. The previous year, the same study indicated that 79 percent of students had at least a bachelor's degree, and they averaged 7.6 years of work

experience,[81] perhaps suggesting a trend towards a more viable entry-level pathway. What this means for cybersecurity bootcamps is unclear.

While skills-based short courses may remain problematic for early-career job seekers, they do offer some promise to workers transitioning from other less-engaging or less-lucrative careers and for employers seeking to upskill their current workforce. For example, they could allow IT support staff to specialize in network security or other cybersecurity disciplines.

In the United Kingdom, industry association CompTIA has already invested in this market with support from the U.K. government. Their Cyber Ready retraining program targets a wide range of applicants (e.g. parents, IT hobbyists, graduates) to provide them with the skills needed to enter cybersecurity careers. [82] Such programs could expand in the United States to offer a means for non-cybersecurity professionals to make their way into the industry.

The digitized options in education and training also offer upskilling and training options outside the classroom. While experts debate whether massive open online courses (MOOCs) will replace conventional college degrees more generally,[83] providers remain optimistic about online education's promise for upskilling and retraining.[84] In cybersecurity, the popularity of these programs has driven rapid growth for specialized providers (e.g. Maryland-based Cybrary).[85] Data-driven insight into what this means for the long-term outcomes of students and workers trained through such programs would be an excellent area for future research.

Apprenticeships in Cybersecurity

Policies to support the growth of apprenticeship as a model for cybersecurity education could have a profoundly positive impact on connecting talented individuals with open jobs.

Given the challenges of teaching cybersecurity in a conventional higher education setting, and recalling that survey data suggests industry experts do not feel that students are graduating with the skills needed to be successful in their new roles,[86] what is the preferred training option? Information on what is missing from classroom education is largely anecdotal, and suffers from a community-wide lack of metrics on what exactly employers find useful in the workplace, but the emphasis on practical experience as a part of the learning process is a frequent refrain across the industry.[87]

Applied skills are often omitted in classrooms in favor of the theoretical principles that undergird the rapidly-changing tools used in workplaces.

Teaching those evolving tools raises concerns that they may be obsolete by the time a student graduates. The approach is entirely appropriate when training future academics—a key component of any university's mandate—but when training future industry workers (or public sector employees) this strategy ultimately relies on employers teaching new graduates the skills needed to be productive in the workplace. Employers, in turn, opt not to hire new graduates because they have no training on the tools and techniques most immediately relevant to their work.

To bridge this gap, some educators and policymakers are turning to apprenticeships. Individual apprenticeship programs can vary drastically on a case-by-case basis, but include four criteria:

- Paid, structured, on-the-job training combined with related classroom instruction;
- Clearly defined wage structure with increases commensurate with skill gains or credential attainment;
- Third-party evaluation of program content, apprenticeship structure, mentorship components, and quality standards; and
- Ongoing assessment of skills development culminating in an industry-recognized credential.

The pool of existing registered programs in cybersecurity is still small, likely consisting of fewer than a few dozen programs with active, paid apprentices focused specifically on cybersecurity. A joint project at New America is tracking the emergence and development of these programs. Data on the programs of which we are aware is available at [link]. Early proponents of the model advocate for its ability to tailor learning to precisely fit workforce needs,[89] as well as its ability to adapt to a rapidly-changing environment.[90]

Information on what is missing from classroom education is largely anecdotal, and suffers from a community-wide lack of metrics on what exactly employers find useful in the workplace.

Degree programs in higher education are not obsolete or without utility. Indeed, many innovative and forward-thinking programs have emerged out of universities and community colleges. Moving away from or dismissing incumbent educational systems misses a critical opportunity to harness good work already being done. One argument in defense of conventional degree programs is their long-standing popularity in the United States. In order for cybersecurity workforce solutions to be effective, they need to be scalable to the order of tens- and hundreds-of-thousands of people. Higher education has the capacity to reach that magnitude. However, existing systems can be augmented to better suit workplace needs, thus creating more pathways to a career in cybersecurity.

Scholars are already considering ways that otherwise conventional higher education pathways could be augmented to incorporate hands-on training in workforce development more generally by melding registered apprenticeship programs with bachelor's degrees.[91] Instead of choosing between degrees and apprenticeships, Mary Alice McCarthy, director of the Center on Education and Skills at New America asks, "How about both?"[92] In cybersecurity, augmenting the higher education system with work-based learning mechanisms would generate not just greater numbers of available workers, but would create the options students need to be successful in the long term and the diversity of experience and education that industry badly needs. Incorporating on-the-job training would make not just a larger cybersecurity workforce, but a better one.

These adaptations to current educational and training systems are not the responsibility of the education community alone. Industry has an equal interest and mandate to prepare new talent for their future roles. Involvement in education allows employers to indicate the skills they need in their future employees. Employers must also necessarily be involved in any apprenticeship or other work-based learning system because the learning will take place in their workplaces. Accordingly, employer buy-in on two fronts—(1) meaningful and ongoing communication with educators and (2) the professional development and incentive structures to accommodate learners and reward mentorship—will be critical to success in developing the cybersecurity workforce.

Section Three: How is Competence Measured and Communicated?

As any hiring manager can tell you, approaching a stack of resumes without a clear idea of the specific qualifications needed for the job is a recipe for inconsistent, inefficient, and potentially biased hiring practices. But when standard indicators of learning (like university degrees) often do not correlate well with the knowledge, skills, and abilities most directly relevant to the workplace, what *should* hiring managers be looking for when they sort through a stack of applicant resumes? The answer depends on context. The following section will explore how employers and jobseekers use industry certifications and other tools to communicate competence, highlighting that each method's overall utility depends on the way in which they are used.

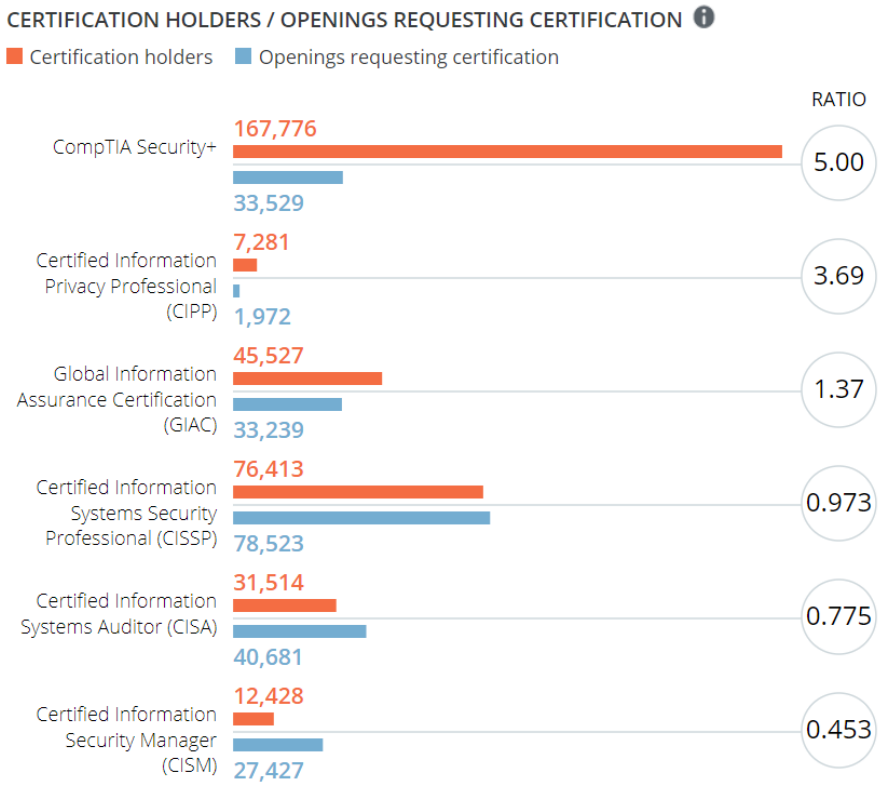
Industry Certifications

> *Certifications provide a theoretical framework that could be used to create an entry point into the field, but hiring patterns suggest that the certifications are used as a proxy for work experience more than an indicator of competence. Coupled with the expense of training and testing, this limits the effectiveness of certifications in creating additional entry points into cybersecurity jobs.*

Industry certifications are one alternative measure of competence already widely in use in cybersecurity. In fact, 35 percent of job postings call for industry certifications to demonstrate competence.[93] Cybersecurity has a wealth of certifications denoting different levels of technical ability, so much so that knowing which to pursue can be a challenge for cybersecurity experts (and soon-to-be-experts). Industry associations like CompTIA, training providers like the SANS Institute, and professional organizations like the International Information System Security Certification Consortium (more widely known as (ISC)2), ISACA, and the International Council of Electronic Commerce Consultants (EC-Council) each have their own suite of credentials with different certifications for different levels of expertise, specific skill sets, or particular vendors or products.

The Cyberseek website jointly developed by NICE, CompTIA, and Burning Glass monitors popular certifications as a ratio between holders of certifications and number of job postings requesting those certifications.[94] As of this writing, there are 78,523 open positions in the United States requesting candidates with a CISSP certification, and 76,413 current certification holders.[95] There are more open

positions seeking CISSP holders than there are CISSP holders in total—the vast majority of whom, of course, are already employed.



Supply and demand of cybersecurity certificates.

Source: cyberseek.org/heatmap.html

Costs to take the tests necessary to obtain these certifications vary widely; CompTIA's Security+ is $330,[96] whereas attempting the GIAC test runs $1,899.[97] Additionally, many providers offer study guides or classroom trainings designed to prepare prospective test-takers for the exam. For example, CompTIA offers a study book for the Security+ exam for $149, or a bundle of resources—including the exam fee and a retake fee—for $1,049.[98] Given this, potential test-takers must consider the expected return on investment for pursuing the certifications, but data on this is limited.

Statistics from the organizations that operate these tests present a compelling case for the return on investment of certification. (ISC)2's 2015 Global Information Security Workforce Study compares average salaries of security professionals who hold an (ISC)2 certification[99] with those who do not: $103,117 for certification holders and $76,363 for the non-certified,[100] which makes the test an easy sell for those candidates that are qualified to take it. (That data

correlating earnings and certification almost certainly reflects additional factors. For example, professionals further along in their careers are both more likely to earn a higher salary and to have had an opportunity to take the test.)

The cybersecurity community would benefit from more in-depth, third-party research on the economics and expected outcomes of certifications in cybersecurity. (ISC)2's numbers do generally track with non-industry-specific expectations for the returns on industry certifications. The Bureau of Labor Statistics collects data on the impacts of certifications on salary via the Current Population Survey, and has found that the median earnings of a worker are $793 per week without a certification, and $1,145 per week with a certification.[101] Furthermore, research into certifications in other industries shows that they can enable career transitions across industries. Because certifications can demonstrate competence in core or transferrable skills, if an employer or section of the market becomes obsolete or unprofitable, workers with certain certifications may be more able to parlay their experience into a career transition.[102] All other things being equal, there are good economic reasons for an individual to pursue industry certification.

While earning a certification does not guarantee a job or higher earning potential —especially in cybersecurity where the impact depends heavily on *which* certification one pursues—it does offer a way for jobseekers to distinguish themselves and demonstrate their workplace-relevant capabilities. Unfortunately, patterns in hiring limit the extent to which these certifications are useful as a means for offering a clear entry point to jobseekers trying to enter the cybersecurity industry. The most in-demand certifications often require years of work experience, whereas the more commonly held early-career certifications see much less demand. Analytics company Burning Glass breaks certifications into two broad categories: "Door Openers, which help new labor market entrants enter a field; and Career Escalators, which pave the path for experienced workers' upward mobility."[103]

There are more open positions seeking CISSP holders than there are CISSP holders in total.

Using this framework, cybersecurity's most in-demand certifications are Career Escalators, rather than Door Openers, which limits their utility as an alternative means for breaking into the industry. For example, the Certified Information Systems Security Professional (CISSP) is the most frequently requested

certification,[104] and the certification is only granted to applicants who pass a test and can demonstrate five years of work experience. There are variations on the CISSP certification for applicants who can pass the test but do not have the required work experience, and a year of experience can be waived based on education or prior certifications,[105] but these adaptations are only useful if employers are willing to hire applicants who have taken these routes.[106] Not all certifications have the same requirements for work experience, but applicants with more easily obtained certifications are generally much more common.

While industry certifications could offer an alternative point of entry into a cybersecurity career, and Door Opener-type certifications do exist in cybersecurity, it does not appear that they are often being used for this purpose. As long as employers are predominantly relying on the Career Escalator-type certifications that come with years of work experience, these certification regimes will not creating an alternative entry point into the industry on a meaningful scale. Having a means of demonstrating a sound grasp of the fundamentals does very little good if employers are only willing to hire employees with advanced knowledge and experience.

Other Ways to Demonstrate Cybersecurity Competence

Forums like online platforms and cybersecurity competitions could add to the number and variety of mechanisms for demonstrating competence, but they are not yet to the point of being effectively scalable. Carefully designed hiring policies and funding mechanisms could incentivize growth and best utility of these mechanisms.

Certifications are not the only means of demonstrating competence. Another promising means for communicating this follows the model of the TechHire initiative that began with the support of the White House in 2015.[107] The program is a combination of training, evaluation, and community outreach designed to provide a means for candidates to demonstrate their skills, to supplement their knowledge as needed and to connect them with employers.[108] Programs like this generally require external support, which limits their growth. Moreover, while the information technology sector more generally has some successful examples of this approach, cybersecurity does not. A valuable proof of concept would be the creation of a low- or no-cost indicator of competence, ideally coupled with a teaching platform, that carried the credibility of a well-respected organization. Carefully crafted funding mechanisms could incentivize the development and operation of such an indicator. More generally, with appropriate support, organizers and developers could provide meaningful pathways into the cybersecurity workforce.

Hiring models that reward self-taught talent offer particular promise in cybersecurity, a field with a culture that prizes hackers and curiosity. Information security is a community known for its particularly individualistic ethos, and there is already a legacy of hiring based on demonstration of individual skill, rather than formal education. Capture the flag competitions (CTFs) are a cornerstone of many major information security conferences, and, anecdotally speaking, many organizations use these competitions to identify potential future hires.[109]

Similarly gamified cybersecurity exercises are increasingly popular as clubs for students. The CyberPatriot National Youth Cyber Education Program, for example, is a nonprofit program that runs the annual National Youth Cyber Defense Competition. Teams are organized around schools, girl scout and boy scout troops, and other youth organizations. These teams compete remotely at intervals throughout the school year to practice and demonstrate students' ability to secure computer systems.[110] Having just completed its tenth year, the program boasted 5,584 teams registered to compete in the 2017-2018 competition.[111] Similarly, the National Collegiate Cyber Defense Competition offers college students an opportunity to put theory to practice by competing with other schools to defend a simulated company network.[112] Programs like these reinforce the ethos that cybersecurity skill is something to be demonstrated in practice while also giving students hands-on experience to inform their education.

Because there is a strong tradition of demonstrating competence through competitions rather than through degrees or certifications, this community could be particularly accepting of hiring practices that use competitions to identify qualified candidates. However, data is scarce on just how widespread such hiring is. Gaining a more thorough sense of this hiring dynamic would be an excellent area for future research.

One of the challenges to using cybersecurity competitions as a hiring mechanism is that such hiring pathways are only useful to employers that specialize in cybersecurity itself. There are a wide range of jobs that require cybersecurity skill, but that cross over into other sectors like healthcare, finance, or transportation. Employers in these hybrid jobs are not likely to have the contextual knowledge of the cybersecurity community to know how or where to recruit competition winners. Recognition from a capture the flag event is not likely to mean much to a hospital administrator or port authority manager who may not understand which specific technical skills that particular competition demonstrates. While some employers may be able to use competitions as a hiring tool, the benefit is limited to those employers already familiar with the CTF scene.

A second challenge with using competitions to address the cybersecurity workforce shortage is identifying how it could be scaled beyond its present capacity. If this kind of hiring is already occurring, what can be done to widen this

onramp into a cybersecurity career? Increasing the number of competitions does not necessarily increase the number of qualified participants. What can be done to encourage potential participants to pursue the skills that would distinguish them as a competitor? Such demonstrations of skill provide an alternative way for jobseekers to communicate competence, but in order to have a meaningful impact on the workforce shortage, they must be scalable.

Section Four: What is the Role of Government in Cyber Workforce Development?

This section explores three aspects of governments' role in cybersecurity workforce development:

1. The extent to which addressing the workforce shortage is the responsibility of the U.S. government,

2. The policy options available to the U.S. government, and

3. The lessons that the U.S. can take from cybersecurity workforce development abroad.

Finally, it will look at the responsibility of the larger cybersecurity ecosystem to consider how other stakeholders can and should engage with government efforts.

Is the U.S. Government Responsible for Growing the Nation's Cybersecurity Workforce?

> *The U.S. government has a unique responsibility for enabling and incentivizing growth in the cybersecurity workforce because an inadequate workforce exposes the nation to serious consequences for economic and national security.*

There are policy tools available to the U.S. government that could help drive the development of the cybersecurity workforce, but how these tools are implementable on a practical level depends heavily on how stakeholders in the U.S. cybersecurity community interpret the government's role—and obligation—to invest in the cybersecurity workforce. On one end of the spectrum of opinions are proponents for a heavily market-driven solution.

Researchers at the RAND Corporation determined in a 2014 report that "the difficulty in finding qualified cybersecurity candidates is likely to solve itself, as the supply of cyber professionals currently in the educational pipeline increases, and the market reaches a stable, long-run equilibrium... It is unlikely that major new initiatives are needed to help the market stabilize in the long run."[113] This perspective assumes that the financial incentives to provide strong cybersecurity are sufficient to drive improvement in the hiring market over time.

The challenge with this fundamentally laissez faire approach to cybersecurity workforce development is that the costs of flawed or inadequate cybersecurity practices—failures indirectly driven by unfilled cybersecurity positions—continue to stack up while the market meanders towards presumably more efficient workforce development systems. Estimations of global losses to cybercrime range from $600 billion[114] per year to some $6 trillion per year by 2021.[115]

The costs of bad cybersecurity extend beyond dollar figures. The U.S. government is obligated to protect the nation, but government is not solely responsible for providing for national cybersecurity. The discussion below also describes the role that other stakeholders play. Nonetheless, the expectations for government in cybersecurity are different because of its fundamental mandate to protect critical national interests. To give a prominent example, providing for secure and fair elections is largely dependent on ensuring that all actors across companies, state and local governments, and other institutions have the resources and capacity needed to protect their own networks, which is predicated on having knowledgeable experts on staff (or at least on call). To borrow a quote from former Homeland Security Secretary Jeh Johnson, "the American people have a right to know from our leaders: What are you doing about it?"[116] Because the U.S. government holds an outsized responsibility for driving better cybersecurity, it also owns a large share of the responsibility (and practical necessity) to build the workforce that will provide that cybersecurity.

The costs of flawed or inadequate cybersecurity practices continue to stack up while the market meanders towards presumably more efficient workforce development systems.

Unsurprisingly in the face of rising costs of cybersecurity failures—financial and otherwise—many stakeholders argue that a more proactive stance in cybersecurity workforce development is warranted. But even here, there is a diversity of opinion on where the onus for intervention sits within the cybersecurity ecosystem. For example, the Business-Higher Education Forum makes a business case for investments from across the community that incentivize collaborative efforts of businesses and academic institutions.[117] Others—this author included—have argued that an inadequate cybersecurity workforce is a national security liability,[118] and therefore the U.S. government is

obligated more than other stakeholders to support community-wide workforce development efforts as part of its responsibility to provide for the national defense. While experts can debate where the U.S. government's responsibility falls on the spectrum from market-driven solutions to extensive federal investment, current and growing threats to U.S. interests clearly warrant some degree of involvement.

What Is the Range of Policy Options Available for Building a Stronger Cybersecurity Workforce in the United States?

Policymakers—at a variety of levels of government—can fund the development of research and programs, set their own spending priorities to support particular pathways, facilitate and incentivize opportunities for collaboration among stakeholders, and lead by their own example. This is not an exhaustive list; many more options exist.

While the U.S. government holds a share of the responsibility for building a more robust national cybersecurity workforce, public policy is only one of the drivers of change in the workforce. Government cannot simply will (or legislate, regulate, or fund) a stronger workforce into existence. Government can, however, can set spending priorities, support development of certain pathways through their own workforce, and incentivize collaboration between stakeholders, all of which have the potential to contribute to overall progress.

In practice, these sorts of policy options can take several forms. To take one category of potential policy levers—setting spending priorities—federal, state, and local governments have a number of tools at their disposal. One would be to fund research. This could take place on several levels.

Government cannot simply will (or legislate, regulate, or fund) a stronger workforce into existence.

The first potential level of research would be to better understand the current state of the workforce and its drivers, including compiling better data and statistics for a baseline to evaluate future progress. Some examples of

government funding for cybersecurity workforce development exist, but these funding opportunities more frequently tend to focus on launching specific programs,[119] developing new teaching methodologies or curriculums,[120] or providing scholarships for individual students[121] rather than developing foundational research. The CyberSeek website is a good beginning, but there is much more work to be done (and funded) in order to get an adequate picture of the current workforce.

As the community learns which pathways and tools provide the best return on investment, government at all levels can drive growth in those areas. State governments in particular have room to shape these options. For example, the California Apprenticeship Initiative,[122] offered through the California Community College Chancellor's Office, gave local educators the opportunity to start development on cybersecurity apprenticeship programs.[123] At the federal level, a recent Department of Labor notice of funding opportunity for apprenticeship expansion is in the same spirit, albeit with significantly different requirements for program scale.[124] When crafted carefully to align with industry and education requirements and capabilities, strategic efforts to drive program development go a long way to creating alternative pathways into cybersecurity jobs.

Beyond grant writing and other forms of direct support, governments can also drive change by being strategic about spending on their own efforts. For example, when evaluating proposals for work on government contracts, agencies could give a degree of preference to proposals that hire staff trained through apprenticeships or to firms that utilize the NICE Workforce Framework. Similarly, future contracts might relax requirements for specific degrees to allow greater flexibility for innovative education and hiring pathways.

Because change in the cybersecurity ecosystem is so dependent on a wide network of stakeholders, some of policymakers' influential options come from more indirect forms of support. Given their position and authority, government actors are often ideally placed to facilitate opportunities for collaboration among other stakeholder. For example, the National Initiative on Cybersecurity Education (NICE) supports two annual conferences[125] designed to bring stakeholders together to discuss workforce development and educational efforts. This government support creates a rich environment for industry, academia, and the public sector to compare requirements and capabilities, and to engage a diverse community in generating and evaluating strategies for workforce growth. Similarly, platforms like the NICE Working Group[126] that enable community-based resource sharing and ongoing dialogue between stakeholders are a low-cost way to indirectly support workforce growth by facilitating opportunities for collaboration. However, they are limited by the degree of engagement and support they receive from the wider community. Facilitating dialogue among stakeholders is a tool best used in conjunction with a suite of other efforts.

When crafted carefully to align with industry and education requirements and capabilities, strategic efforts to drive program development go a long way to creating alternative pathways into cybersecurity jobs.

An easily-overlooked—but remarkably powerful—tool for governments seeking to support cybersecurity workforce development is simply to lead by example. The state government of North Carolina, for example, places disabled veterans as apprentices in cybersecurity roles in their Department of Information Technology and other state agencies[127] through a collaboration with the Innovative Systems Group, a contractor and apprenticeship program sponsor, and local educational institutions.[128] As private sector employers evaluate the business case for implementing unconventional hiring practices, this model sets a valuable precedent. However, not all good ideas are completely novel. Government can continue to build and support offices like the National Initiative on Cybersecurity Education that have a proven track record of good work in establishing standards and building collaboration for the community of stakeholders in the field.

What Can the United States Learn from Cybersecurity Workforce Development Abroad?

Policymakers can look to other governments for examples of varying solutions to the cybersecurity workforce challenge, but they must recognize that many of these solutions cannot function properly in a U.S. context without significant adaptations.

The cybersecurity workforce shortage is by no means a uniquely American phenomenon. There are some differences in the perceived causes of the shortage, but the shortage itself remains essentially the same. For example, survey respondents in Latin America and the Middle East and North Africa are more inclined to cite business conditions that do not support additional personnel as the reason for the shortage, whereas in North America and Europe,

respondents were more inclined to say that qualified personnel were difficult to find. Globally, 66 percent of respondents still felt that too few information security professionals worked in their department.[129]

National governments have many strategies for developing their cybersecurity workforce, but a common thread is recognition that private sector engagement will play a key role bringing about future success. One difference of note, particularly in the United Kingdom and Europe, is that this public-private collaboration is often the basis for apprenticeship programs. For example, the United Kingdom's Department of Digital, Culture, Media, and Sport (DCMS) sponsored a program that placed apprentices in cybersecurity roles across a range of employers responsible for critical national infrastructure,[130] a promising program for employers who need the skills and talent pipeline, and for government policymakers looking to improve security in critical infrastructure. Especially in Germany, Austria, and Switzerland, apprenticeships across all industries are a key feature of strong national traditions in career and technical education.[131] Companies based in those countries that maintain a workforce in the United States have been eager to encourage the United States to adopt similar practices.[132]

Globally, 66 percent of respondents still felt that too few information security professionals worked in their department.

Given cybersecurity's inclination towards on-the-job learning, importing apprenticeship models for cybersecurity in the United States is an interesting proposition, but the difference in context between the United States and Europe means that many aspects of these programs would need to be adjusted for a U.S. environment. Implementation would require major adaptations in funding sources and shifts in philosophies about how such programs might work.[133] However, workforce development experts are willing to take on the challenge. For example, 3aaa—a U.K-based apprenticeship development company—is working with TranZed Apprenticeship Services in Baltimore, Md. to implement cybersecurity (and other) apprenticeships in the area.[134] But not all efforts in this vein originate from abroad. Similar homegrown efforts have taken shape in Illinois,[135] Virginia,[136] and New Mexico[137]. Further research could help illuminate how this workforce development solution, so successful internationally, can be adapted to help fill the U.S. workforce shortage in cybersecurity.

The United Kingdom and Europe are certainly not alone in presenting useful workforce development lessons in cybersecurity; other case studies have much to offer. Israel, for example, is home to a remarkably robust cybersecurity community.[138] Israel benefits from a combination of mandatory conscription and military expertise in cybersecurity.[139] The result is a steady supply of practitioners emerging from cybersecurity units that go on to establish and staff private-sector technology firms.[140] While this model may not be especially viable in other contexts (particularly in countries without such high levels of military participation), Israel's focus on the military as a tool to shape its cybersecurity workforce warrants closer study. The cybersecurity workforce development systems in states like Russia, China, and North Korea are somewhat more opaque, but further open-source (and unclassified) research into these workforce training systems would very likely add significantly to the cybersecurity workforce conversation in the United States.

Whether from the private sector, higher education, the military, or any one of dozens of categories of stakeholders, there are plenty of opportunities to collaborate and invest. However, cybersecurity has particularly significant implications for national security and economic stability, which means that the U.S. government has particular incentive to initiate and coordinate such community-wide collaborations and investments. Significant workforce development efforts are not likely to succeed without buy-in from this all stakeholders; but the market alone is not likely to *start* these efforts before the costs of inadequate cybersecurity become intolerably high. Therein lies the central challenge—and opportunity—for policymakers in cybersecurity workforce development: initiating collaborative solutions that engage the wide array of stakeholders in cybersecurity workforce development.

The Role of Other Stakeholders

> *Businesses and other actors across the cybersecurity community can and should recognize the benefits for their own long-term success in improving the overall state of the workforce, though it is unreasonable to expect them to act out of altruism alone to improve the alignment between cybersecurity education and jobs. Here too, policymakers can incentivize and educate to reduce friction in implementation of novel solutions.*

U.S. government decision-makers have the responsibility and many of the the tools to shoulder outsized responsibility for investment in U.S. cybersecurity workforce development, but they are not alone. The cybersecurity workforce is an ecosystem with many inputs, influencers, and interlocking parts. There is no central authority, and for all its ability to influence that ecosystem, U.S. federal,

state, and local governments can only incentivize, facilitate, and model improvement in cybersecurity development. The federal government cannot create that improvement on its own but must work with outside partners in the private sector, higher education, nonprofits, state and local government. That can include C-suite officers in industry, hiring managers at firms, faculty and administrators at colleges and universities, state and local workforce development agencies, parents and students, subject matter experts employed in the field and in adjacent areas of study, and many, many others. All these stakeholders have a role in driving improvements in the workforce.

Government policymakers cannot and should not expect any of these stakeholders to act outside of their perception of their own best interests. The opportunity, then, is to align incentives, lower the costs of collaboration and innovation, and educate stakeholders on the long-term collective and individual benefits of investment in the workforce. It is still incumbent on stakeholders outside of government to critically assessing their policies and ensuring they fit with cybersecurity's relatively unique realities. The rapid growth of the field and the limited existing infrastructure and resources to adapt mean that doing business in cybersecurity is different than in other industries, and prudent employers will benefit from regularly evaluating the need for agility and innovation in their cybersecurity workforce development strategy.

The scale of the challenge in cybersecurity workforce development is large enough to provide plenty of room for stakeholders to develop solutions. Regardless of who carries the responsibility of investing funding and attention into the problem, the entire cybersecurity community has an interest in improvement. Apart from the "rising tide lifts all boats" nature of investment in workforce development, the interconnectedness of the inputs and influencers in the workforce—from schools to startups to government intelligence agencies—creates an ideal (and unavoidable) opportunity for cooperation between public and private sectors.[141]

A stronger cybersecurity workforce offers outsized benefits all stakeholders (and, conversely, outsized costs of an inadequate workforce), therefore supporting that development warrants greater-than-normal investment from all stakeholders. Employers that, in other sectors, might be able to wait for trained talent to come knocking must implement more robust training programs.[142] Educators who have relied on conventional systems for teaching technology fundamentals must consider means for exposing their students to more applied learning opportunities. Policymakers, for their part, can help stakeholders reach these ends by shining a light on the compelling economic benefits of collaboration and innovation and by carefully aligning stakeholder incentives wherever possible.

Conclusions

This report is not intended to solve the cybersecurity workforce development problem, but rather to unpack the topics and questions embedded in that larger conversation and provide options for the path forward. It is intended to help frame the community's future conversations on cybersecurity workforce development. Widening the pipeline of cybersecurity talent and creating alternative entry points into that pipeline leads to complex questions about the role of higher education, the future of work-based learning, and alignment between industry and education. In many ways, cybersecurity is a test case for a number of evolving questions in the relationship between work and education.

Cybersecurity workforce development happens to be both very urgent and very politically salient at the present moment. Both the Obama and Trump administrations have singled out the importance cybersecurity workforce development in official policies,[143] and Congressional hearings demonstrate growing interest from lawmakers.[144] The appetite for cybersecurity policy coupled with overlap with larger questions on the future of work and higher education has created an environment that is particularly conducive to innovative solutions that deliver wide-reaching impact.

Cybersecurity is a test case for a number of evolving questions in the relationship between work and education.

There is ample opportunity for further research from the cybersecurity community. This report underscores a number of questions not well understood due to a lack of data. From the percentage of the workforce trained in military and intelligence organizations to the number of jobs in other sectors that cross into cybersecurity, the empirics around pathways and dynamics through the cybersecurity workforce are extremely limited. For employers—in public and private sectors alike—who wish to make a meaningful investment in cybersecurity workforce development, research in these areas would inform future policy decisions, leading to better workforce development mechanisms across the cybersecurity community.

There are two basic principles that will certainly need to be a part of any solutions. First, broad stakeholder engagement will be critical to making any lasting change. Cybersecurity workforce development is characterized by its interconnectedness and the interdependencies between different mechanisms for change. The impact of the cybersecurity workforce on national security and economic stability make a very clear case for policy intervention to strengthen that workforce; however, effective policies will require input, acceptance, and ongoing coordination from different actors and sectors in the cybersecurity community.

Second, no single approach or solution will fill the all the open jobs in cybersecurity. The scale of the problem is too big—and its causes are too multifaceted—for there to be any silver bullets. Policymakers have a key role to play in initiating changes and aligning incentives among different actors, but policy interventions must be supported by other efforts. Nothing short of community-wide engagement across the full range of stakeholders will create lasting change to cybersecurity workforce development.

Appendix: Unanswered Questions in Cybersecurity Workforce Empirics

The body of this paper has highlighted a number of areas in which additional empirical information could help improve understandings in cybersecurity workforce development. Those questions are gathered and presented here. These are not intended to be rhetorical or conceptual questions about policy, but rather areas where statistical data and measurable observations could enable better decision-making. Because these questions have been removed from their original context, in some cases the questions have been rephrased or expanded to make meanings clear.

Workforce Sources

- How many U.S. cybersecurity professionals got their initial training in the intelligence community or military? What are the costs of this training to the federal government? What are the economic benefits to the rest of the cybersecurity community? What would comparable education cost if conducted outside of government?

- How many U.S. cybersecurity professionals came directly out of a higher education degree program?

- How many U.S. cybersecurity professionals learn in informal settings—on-the-job or through self-teaching—and, without a degree, how do they market themselves to employers?

- What degrees, certifications, experiences do jobseekers possess when they are hired into cybersecurity jobs? Note that this is a different question than asking what job postings require of applicants.

- How many employers are sourcing employees from capture-the-flag or similar competitions? Which types of employers find this method of screening candidates to be useful?

State of the Workforce

- How many cybersecurity workers are in the federal government? (This research is underway.)

- How many jobs in sectors or functions outside of cybersecurity require significant cybersecurity expertise?

- For what percentage of cybersecurity jobs is a bachelor's (or master's or PhD) critical to success?

- How many private sector employers offer significant training for entry-level employees? What do these programs look like? What percentage of internally-trained employees stay with the company?

- What is the return on investment of industry certifications for an individual job seeker (or employee), controlling for other variables like years of work experience, current employment, and prior certifications?

Individual Outcomes

- What percentage of baccalaureate graduates (with a degree applicable to cybersecurity) that intend to go into cybersecurity get a job in the field? Are they more likely to be hired into the private or public sector?

- Do certifications (and/or which certifications) correlate with success on the job?

- What percentage of computer science (or similar) graduates go into cybersecurity?

- What are the long-term career paths for cybersecurity professionals trained in the military or intelligence community? How many go back to school to pursue additional degrees? How many pursue other forms of training or credentialing?

- What are the employment outcomes for students that pass through cybersecurity bootcamps?

- How does education via massive open online courseware impact a cybersecurity professional's long-term career? At what point in their career do professionals use these resources (e.g. for upskilling, career transitions, or as an alternative to a bachelor's degree)?

Notes

1 "Experts Urge Rapid Patching of 'Struts' Bug," Krebs on Security, August 23, 2018, https://krebsonsecurity.com/2018/08/experts-urge-rapid-patching-of-struts-bug/.

2 Dan Goodin, "Failure to patch two-month-old bug led to massive Equifax breach," Ars Technica, September 13, 2017, https://arstechnica.com/information-technology/2017/09/massive-equifax-breach-caused-by-failure-to-patch-two-month-old-bug/.

3 Prepared Testimony of Richard F. Smith before the Committee on Energy and CommerceSubcommittee on Digital Commerce and Consumer Protection, House of Representatives, 115th Cong. (2017), https://docs.house.gov/meetings/IF/IF17/20171003/106455/HHRG-115-IF17-Wstate-SmithR-20171003.pdf.

4 Alfred Ng, "Equifax CEO steps down in wake of massive data breach," CNET, September 26, 2017, https://www.cnet.com/news/equifax-ceo-steps-down-in-wake-of-massive-data-breach/.

5 Ken Kam, "After Falling 33%, Equifax Is Still Overvalued,"Forbes, September 21, 2017, https://www.forbes.com/sites/kenkam/2017/09/21/after-falling-33-equifax-is-still-overvalued/#71c9da132b88.

6 Alfred Ng, "Equifax CEO steps down in wake of massive data breach," CNET, September 26, 2017, https://www.cnet.com/news/equifax-ceo-steps-down-in-wake-of-massive-data-breach/.

7 CyberCorps is a Scholarship for Service program. Students receive government grants to fund bachelor's or postgraduate studies in cybersecurity, and then are expected to fill a government cybersecurity job for a defined period of time. For more information, see https://www.sfs.opm.gov/.

8 (ISC)2 Cybersecurity Workforce Study, 2018: Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens, (ISC)2, 2018, https://www.isc2.org/-/media/7CC1598DE430469195F81017658B15D0.ashx.

9 (ISC)2 Cybersecurity Workforce Study, 2018: Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens, (ISC)2, 2018, https://www.isc2.org/-/media/7CC1598DE430469195F81017658B15D0.ashx.

10 Jason Reed and Jonathan Acosta-Rubio, Innovatio n Through Inclusion: The Multicultural Cybersecurity Workforce, Center for Cyber Safety and Education, (ISC)2, International Consortium of Minority Cybersecurity Professionals, and Frost and Sullivan, March 2018, 7, https://www.isc2.org/-/media/Files/Research/Innovation-Through-Inclusion-Report.ashx.

11 U.S. Const., art. 1 § 8. https://www.archives.gov/founding-docs/constitution-transcript.

12 Though work on this is underway. See: Mark D. Reinhold, "Requirements of the Federal Cybersecurity Workforce Assessment Act," (official memorandum, Washington, D.C.: United States Office of Personnel Management), https://chcoc.gov/content/requirements-federal-cybersecurity-workforce-assessment-act. https://www.chcoc.gov/content/requirements-federal-cybersecurity-workforce-assessment-act

13 Risk Nexus: Overcome by Cyber Risk? Economic benefits and costs of alternate cyber futures, Atlantic Council, Zurich Insurance Group, and the Pardee Center on International Futures, September 10, 2015, 4, http://www.atlanticcouncil.org/images/publications/risk-nexus-september-2015-overcome-by-cyber-risks.pdf#page=4.

14 For the purposes of this discussion, "information security" and "cybersecurity" are used interchangeably, with the acknowledgement that different discourse communities within the field often understand them to imply differences. This report endeavors to reflect the studies and reference material cited herein, and so generally has opted to use the same terminology used those materials, despite the

variance in language that it has created throughout this document. For example, the study that informs this count of professionals uses the term "information security," which is reflected here.

15 Robert Ayoub, The 2011 (ISC)2 Global Information Security Workforce Study, (ISC)2 and Frost and Sullivan. 2011, 7, https://iamcybersafe.org/wp-content/uploads/2017/01/2011_global_wf_study.pdf.

16 Michael Suby and Frank Dickson, The 2015 (ISC)2 Global Information Security Workforce Study, (ISC)2, Booz Allen Hamilton, NRI Secure, Cyber 360, and Frost and Sullivan, 2015, 3, https://www.iamcybersafe.org/wp-content/uploads/2017/01/FrostSullivan-ISC%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf.

17 2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk, Center for Cyber Safety and Education, (ISC)2, Booz Allen Hamilton, Alta Associates, and Frost and Sullivan, 2017, https://iamcybersafe.org/wp-content/uploads/2017/07/N-America-GISWS-Report.pdf.

18 (ISC)2 Cybersecurity Workforce Study, 2018: Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens, (ISC)2, 2018, https://www.isc2.org/-/media/7CC1598DE430469195F81017658B15D0.ashx.

19 William Newhouse, Stephanie Keith, Benjamin Scribner, and Greg Witte, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, National Institute of Standards and Technology, U.S. Department of Commerce, August 2017, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf.

20 Ibid. 25, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf.

21 Job Market Intelligence: Cybersecurity Jobs, 2015, Burning Glass Technologies Research, 2015, 3, https://www.burningglass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf.

22 For a closer look at issues unique to cybersecurity in the financial sector, see: William A. Carter and Denise E. Zheng, The Evolution of Cybersecurity Requirements for the U.S. Financial Industry, Center for Strategic and International Studies, July 2015, https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/150717_Carter_CybersecurityRequirements_Web.pdf.

23 Katrina Brooker, "Goldman in Ventureland," Bloomberg, July 28, 2015, https://www.bloomberg.com/news/features/2015-07-28/how-goldman-sachs-became-a-tech-investing-powerhouse.

24 Portia Crowe and Matt Turner, "JPMORGAN: 'We are a technology company,'" Business Insider, February 23, 2016, https://www.businessinsider.com/marianne-lake-says-jpmorgan-is-a-tech-company-2016-2.

25 (ISC)2 "Global Cybersecurity Workforce Shortage to Reach 1.8 Million as Threats Loom Larger and Stakes Rise Higher," news release, June 7, 2017, (ISC)2, accessed September 12, 2018, https://www.isc2.org/News-and-Events/Press-Room/Posts/2017/06/07/2017-06-07-Workforce-Shortage.

26 "Cybersecurity Supply and Demand Heat Map," Cyberseek, http://cyberseek.org/heatmap.html.

27 A style of competition common at conferences and in training programs that encourages participants to demonstrate skills in a simulated environment.

28 Job Market Intelligence: Cybersecurity Jobs, 2015, Burning Glass Technologies Research, 2015, 3, http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf.

29 For a particularly colorful demonstration of such criticism, see Ming Chow's Hall of Shame. The Senior Lecturer in Computer Science at Tufts University has compiled some of the more egregious examples of

impractical requirements in cybersecurity job postings, viewable at http://mchow01.github.io/career/2017/08/16/hall-of-shame-job-postings-recruiting.html. Ming Y. Chow, "Hall of Shame Job Postings and Recruiting," August 16, 2017.

30 Robert Walker, "There Is No Cyber Talent Crunch; You're Just Hiring Wrong," Tripwire, June 5, 2017, https://www.tripwire.com/state-of-security/risk-based-security-for-executives/connecting-security-to-the-business/there-is-no-cyber-talent-crunch-youre-just-hiring-wrong/.

31 (ISC)2 Cybersecurity Workforce Study, 2018: Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens, (ISC)2, 2018, https://www.isc2.org/-/media/7CC1598DE430469195F81017658B15D0.ashx.

32 "Table 318.10. Degrees conferred by postsecondary institutions, by level of degree and sex of student: Selected years, 1869-70 through 2025-26," The National Center for Education Statistics, March 2016, https://nces.ed.gov/programs/digest/d15/tables/dt15_318.10.asp?referrer=report.

33 2015-2016 is the most recent year available through the National Center for Education Statistics as of writing.

34 "Table 325.35. Degrees in computer and information sciences conferred by postsecondary institutions, by level of degree and sex of student: 1970-71 through 2015-16," The National Center for Education Statistics, November, 2017, https://nces.ed.gov/programs/digest/d17/tables/dt17_325.35.asp?current=yes.

35 2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk, Center for Cyber Safety and Education, (ISC)2, Booz Allen Hamilton, Alta Associates, and Frost and Sullivan, 2017, 5, https://iamcybersafe.org/wp-content/uploads/2017/07/N-America-GISWS-Report.pdf#page=5.

36 Joseph B. Fuller and Manjari Raman, Dismissed by Degrees: How Degree Inflation is Undermining U.S. Competitiveness and Hurting America's Middle Class, Accenture, Grads of Life, Harvard Business School, October 2017, 4, http://www.hbs.edu/managing-the-future-of-work/Documents/dismissed-by-degrees.pdf.

37 Byron Auguste, "Skills And Tomorrow's Jobs Report: The Usual Suspects," Forbes, July 5, 2018, https://www.forbes.com/sites/byronauguste/2018/07/05/skills-and-tomorrows-jobs-report-the-usual-suspects-warning-spoilers.

38 Steve Lohr, "A New Kind of Tech Job Emphasizes Skills, Not a College Degree," The New York Times, June 28, 2017, https://www.nytimes.com/2017/06/28/technology/tech-jobs-skills-college-degree.html.

39 Jennifer Burrowes, Alexis Young, Dan Restuccia, Joseph Fuller, and Manjari Raman, Bridge the Gap: Rebuilding America's Middle Skills, Accenture, Burning Glass, and Harvard Business School, November November 2014, 4, http://www.hbs.edu/competitiveness/Documents/bridge-the-gap.pdf.

40 Carlson, Jennifer. "Critical Success Factors for a Cybersecurity Apprenticeship Program." Presentation, Pre-Conference Seminar at National Institute for Cybersecurity Education Annual Conference and Expo, Dayton, Ohio, 2017.

41 Marc van Zadelhoff, "Cybersecurity Has a Serious Talent Shortage. Here's How to Fix it," May 04, 2017, https://hbr.org/2017/05/cybersecurity-has-a-serious-talent-shortage-heres-how-to-fix-it.

42 Clive Belfield and Thomas Bailey, The Labor Market Returns to Sub-Baccalaureate College: A Review, Center for Analysis of Postsecondary Education and Employment, March 2017, https://capseecenter.org/wp-content/uploads/2017/04/labor-market-returns-sub-baccalaureate-college-review.pdf.

43 Douglas Webber, "Is College Worth It? Going Beyond Averages," Third Way, September 18, 2018,

https://www.thirdway.org/report/is-college-worth-it-going-beyond-averages.

44 Hacking the Skills Shortage: A Study of the international shortage in cybersecurity skills, McAfee and Center for Strategic and International Studies, July 27, 2016, 13, https://www.mcafee.com/us/resources/reports/rp-hacking-skills-shortage.pdf#page=13.

45 Ibid. 13.

46 Job Market Intelligence: Cybersecurity Jobs, 2015, Burning Glass Technologies Research, 2015, 3, https://www.burningglass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf.

47 Aaron Gregg, "Delays in federal background checks leave more than 700,000 people in limbo," The Washington Post, August 27, 2017, https://www.washingtonpost.com/business/economy/delays-in-federal-background-checks-leave-more-than-700000-people-in-limboas-backlog-grows-trump-administration-stops-reporting-numbers/2017/08/25/8a1bbab6-8921-11e7-a94f-3139abce39f5_story.html?utm_term=.5e508744728d.

48 Security Clearance Reform: Testimony before the Senate Select Committee on Intelligence, 115th Congress (2018), (statement of David J. Berteau, President and CEO of the Professional Services Council), https://www.intelligence.senate.gov/sites/default/files/documents/os-dberteau-030718.pdf.

49 Mark Warner, "We Need Revolution, Not Just Evolution in Security Clearances," The Cipher Brief, February 2, 2018, https://www.thecipherbrief.com/column/agenda-setter/need-revolution-not-just-evolution-security-clearances.

50 Judy Woodruff, "White House security clearance process 'broken,' says top Trump intelligence official," PBS Newshour, February 13, 2018, https://www.pbs.org/newshour/show/white-house-security-clearance-process-broken-says-top-trump-intelligence-official.

51 Personnel Security Clearances: Additional Actions Needed to Ensure Quality, Address Timelines, and Reduce Investigation Backlog, U.S. Government Accountability Office (GAO), December 12, 2017, https://www.gao.gov/assets/690/688918.pdf.

52 Personnel Security Clearances: Plans Needed to Fully Implement and Oversee Continuous Evaluation of Clearance Holders, U.S. Government Accountability Office, November 21, 2017, 2, https://www.gao.gov/products/GAO-18-117.

53 Jason Miller, "DoD to bring more employees with 'critical positions' under continuous evaluation," The Federal News Radio, September 21, 2017, https://federalnewsradio.com/other-dod-agencies/2017/09/dod-to-bring-more-employees-with-critical-positions-under-continuous-evaluation/.; Nicole Ogrysko, "ODNI developing comprehensive continuous evaluation capabilities for agencies in 2018," Federal News Radio, November 17, 2017, https://federalnewsradio.com/other-dod-agencies/2017/11/odni-developing-comprehensive-continuous-evaluation-capabilities-for-agencies-in-2018/.

54 Martin Giles, "Cybersecurity's insidious new threat: workforce stress," MIT Technology Review, August 7, 2018, https://www.technologyreview.com/s/611727/cybersecuritys-insidious-new-threat-workforce-stress/.

55 Roman V. Yampolskiy, "AI is the future of Cybersecurity, for Better and for Worse," Harvard Business Review, May 8, 2017, https://hbr.org/2017/05/ai-is-the-future-of-cybersecurity-for-better-and-for-worse.

56 "Staffing the IT Security Function in the Age of Automation," The Ponemon Institute sponsored by DomainTools, May 2018, https://www.domaintools.com/content/Ponemon_Report_Staffing_IT_Age_of_Automation.pdf.

57 Matthew Goldstein, "Private Sector Pay Lures F.B.I.'s Hacking Experts," New York Times, July 21, 2015, https://www.nytimes.com/2015/07/22/business/dealbook/fbi-scrambles-as-private-sector-lures-online-crime-investigators.html.; Rachel King, "MasterCard Sues Nike and Its Former CISO Over Poaching," The Wall Street Journal, January 12, 2015, https://blogs.wsj.com/cio/2015/01/12/mastercard-sues-nike-and-its-former-ciso-over-poaching/.; Simone Petrella, "NIST Cybersecurity Workforce RFI," CyberVista, August 1, 2017. 3, https://www.nist.gov/sites/default/files/documents/2017/08/02/cybervista.pdf#page=3.

58 "The Case for Early Education about STEM Careers," ASPIRES, King's College London, https://www.kcl.ac.uk/sspp/departments/education/research/aspires/10FactsandFictionsfinalversion.pdf.

59 "Trends in the State of Computer Science in U.S. K-12 Schools," Gallup in partnership with Google, 2016, http://services.google.com/fh/files/misc/trends-in-the-state-of-computer-science-report.pdf.

60 Interdisciplinary Pathways towards a More Secure Internet, National Science Foundation, Report on the Cybersecurity Ideas Lab, Arlington, Virginia, February 10-12, 2014, 9, https://www.nsf.gov/cise/news/CybersecurityIdeasLab_July2014.pdf#page=9

61 RK Raj and A Parrish, "Toward Standards in Undergraduate Cybersecurity Education in 2018," Com puter 51, issue 2 (February 2018): pp 72-75, https://ieeexplore.ieee.org/abstract/document/8301119/.

62 The computing societies are: Association for Computing Machinery (ACM), IEEE Computer Society (IEEE CS), Association for Information Systems Special Interest Group on Security (AIS SIGSEC), and International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8). For more, see https://www.csec2017.org/

63 Cybersecurity Curricula 2017 Version 0.95 Report, Joint Task Force on Cybersecurity Education, November 13, 2017, 14, https://docs.wixstatic.com/ugd/895bd2_331dd0a4e2cf41a1b17f394e3e62a955.pdf#page=14.

64 And, indeed, others across higher education have also emphasized and developed mechanisms for incorporating other disciplines in a computer science-based cybersecurity curriculum. For example, see the University of Nevada Reno and Truckee Meadows Community College's Interdisciplinary Cybersecurity Modules: http://capacity.unr.edu/.

65 For more on this, particularly with an eye to incorporating cybersecurity into policy education, see Jessica Beyer and Sara Curran, Cybersecurity Workforce Preparedness: The Need for More Policy-Focused Education, Wilson Center Digital Futures Project, November 22, 2017, https://www.wilsoncenter.org/publication/cybersecurity-workforce-preparedness-the-need-for-more-policy-focused-education.

66 Peter Swire, "A Pedagogic Cybersecurity Framework," Communications of the ACM 61 [October 2018]: 23-26, https://cacm.acm.org/magazines/2018/10/231364-a-pedagogic-cybersecurity-framework/abstract.

67 Allen Parrish, John Impagliazzo, Rajendra K. Raj, Henrique Santos, Muhammad Rizwan Asghar, Audun Jøsang, Teresa Pereira, and Eliana Stavrou, "Global Perspectives on Cybersecurity Education for 2030: A Case for a Meta-Discipline," Proceedings of 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education (ITiCSE'18), July 2-4, 2018, https://dl.acm.org/citation.cfm?doid=3197091.3205840.

68 Kirk Carapezza, "With more than 200,000 unfilled jobs, colleges push cybersecurity," PBS Newshour, January 22, 2015, https://www.pbs.org/newshour/education/college-struggle-keep-pace-need-cyber-soliders.

69 Arati Prabhakar, "Cybersecurity Summit," (panel discussion, Washington Post Live, October 01, 2014),

https://www.c-span.org/video/?321807-1/discussion-government-cybersecurity&start=189.

70 RK Raj and A Parrish, "Toward Standards in Undergraduate Cybersecurity Education in 2018," Com puter 51, issue 2 (February 2018): pp 72-75, https://ieeexplore.ieee.org/abstract/document/8301119/.

71 Michael M. Crow and William B. Dabars, The New American University, Baltimore: Johns Hopkins University Press, 2015, 7-8.

72 "Table 348. Average graduate and first-professional tuition and required fees in degree-granting institutions, by first-professional field of study and control of institution: 1988-89 through 2009-10," National Center for Education Statistics, October 2010, https://nces.ed.gov/programs/digest/d10/tables/dt10_348.asp.

73 Jon Marcus, "Graduate programs have become a cash cow for struggling colleges. What does that mean for students?," PBS Newshour, September 18, 2017, https://www.pbs.org/newshour/education/graduate-programs-become-cash-cow-struggling-colleges-mean-students.

74 Kevin Carey, "Those Master's-Degree Programs at Elite U.? They're For-Profit," The Chronicle of Higher Education, April 21, 2014, https://www.chronicle.com/article/Those-Master-s-Degree/146105.

75 2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk, Center for Cyber Safety and Education, (ISC)2, Booz Allen Hamilton, Alta Associates, and Frost and Sullivan, 2017, https://iamcybersafe.org/wp-content/uploads/2017/07/N-America-GISWS-Report.pdf.

76 Jessie Brown and Martin Kurzweil, The Complex Universe of Alternative Postsecondary Credentials and Pathways (Cambridge, Mass.: American Academy of Arts & Sciences, 2017), https://www.amacad.org/multimedia/pdfs/publications/researchpapersmonographs/CFUE_Alternative-Pathways/CFUE_Alternative-Pathways.pdf.

77 Elizabeth Catte, "In Appalachia, Coding Bootcamps That Aim To Retrain Coal Miners Increasingly Show Themselves To Be 'New Collar' Grifters," BELT Magazine, January 11, 2018, http://beltmag.com/appalachia-coding-bootcamps/.

78 Jaikumar Vijayan, "Can cybersecurity boot camps fill the workforce gap?," The Christian Science Monitor Passcode, January 20, 2017, https://www.csmonitor.com/World/Passcode/Security-culture/2017/0120/Can-cybersecurity-boot-camps-fill-the-workforce-gap.

79 Liz Eggleston, 2016 Coding Bootcamp Outcomes and Demographics Study, Course Report, September 14, 2016, https://www.coursereport.com/reports/2016-coding-bootcamp-job-placement-demographics-report.

80 Ibid.

81 Liz Eggleston, 2015 Coding Bootcamp Alumni & Demographics Study, Course Report, October 25, 2015, https://www.coursereport.com/reports/2015-coding-bootcamp-job-placement-demographics-report.

82 CompTIA, "CompTIA Pledges to Get the UK Cyber Ready," news release, June 27, 2018, CompTIA, accessed September 12, 2018, 2016.https://www.comptia.org/about-us/newsroom/press-releases/2018/06/27/comptia-pledges-to-get-the-uk-cyber-ready.

83 Kevin Carey, "Here's What Will Truly Change Higher Education: Online Degrees That Are Seen as Official," New York Times, March 5, 2015, https://www.nytimes.com/2015/03/08/upshot/true-reform-in-higher-education-when-online-degrees-are-seen-as-official.html.

84 Michael Bernick, "Coursera's Bet On The Upskilling of American Workers," Forbes, February 21,

2018, https://www.forbes.com/sites/michaelbernick/2018/02/21/courseras-bet-on-the-upskilling-of-american-workers/#38ebb3b5eb24.

85 Tajha Chappellet-Lanier, "Cybersecurity MOOC Cybrary hits 1 million registered users," Technical.ly/DC, May 11, 2017, https://technical.ly/dc/2017/05/11/cybersecurity-mooc-cybrary-one-million-registered-users/

86 "Hacking the Skills Shortage: A Study of the international shortage in cybersecurity skills," McAfee and Center for Strategic and International Studies, July 27, 2016, 13. https://www.mcafee.com/us/resources/reports/rp-hacking-skills-shortage.pdf#page=13.

87 For a sampling, see responses to NIST/NICE Executive Order on Cybersecurity Workforce Request for Information. For an example, see ISACA's response at https://www.nist.gov/sites/default/files/documents/2017/08/01/nice_rfi_final_isaca.pdf#page=6.

88 Definition and Principles for Expanding Quality Apprenticeship in the U.S., Apprenticeship Forward Collaborative, Forthcoming, https://www.apprenticeshipforward.org/.

89 Marian Merritt, "Cybersecurity Apprenticeships Enhance Cybersecurity Infrastructure," United States Department of Commerce, January 31, 2018, https://www.commerce.gov/news/blog/2018/01/cybersecurity-apprenticeships-enhance-cybersecurity-infrastructure.

90 Michael Prebil, "Teach Cybersecurity with Apprenticeship Instead," New America, April 14, 2017, https://www.newamerica.org/education-policy/edcentral/teach-cyber-apprenticeship-instead/.

91 Mary Alice McCarthy, Iris Palmer, and Michael Prebil, Connecting Apprenticeship and Higher Education Eight Recommendations, Washington D.C., New America, December 06, 2017, https://na-production.s3.amazonaws.com/documents/Connecting-Apprenticeship-HigherEd.pdf.

92 Mary Alice McCarthy (McCarthyEdWork), "Apprenticeships or College? How About Both?," December 8, 2017, 3:06pm, https://twitter.com/McCarthyEdWork/status/939269991416975360.

93 Job Market Intelligence: Cybersecurity Jobs, 2015, Burning Glass Technologies Research, 2015, 3, http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf.

94 "Cybersecurity Supply and Demand Heat Map," Cyberseek, accessed September 12, 2018, http://cyberseek.org/heatmap.html.

95 Ibid. http://cyberseek.org/heatmap.html. In a slight discrepancy, the certifying authority, (ISC)2 identifies 79,617 holders. (ISC)2, "(ISC)2 Member Counts," accessed March 07, 2018 https://www.isc2.org/About/Member-Counts.

96 "CompTIA Security+," CompTIA, accessed September 12, 2018, https://certification.comptia.org/certifications/security.

97 "Certifications: Pricing," GIAC Certifications, accessed September 12, 2018, https://www.giac.org/certifications/pricing.

98 "The Official CompTIA Security+ Study Guide (Exam SY0-501) eBook," CompTIA, accessed October 16, 2018, https://store.comptia.org/product/978-1-64274-009-7. "CompTIA Security+ Premier Bundle," accessed October 16, 2018, https://store.comptia.org/product/S-CMLBDL-PRM.

99 Referred to as "members" and "non-members" in the report. One becomes a member by obtaining a (ISC)2 certification.

100 Michael Suby and Frank Dickson, The 2015 (ISC)2 Global Information Security Workforce Study, (ISC)2, Booz Allen Hamilton, NRI Secure, Cyber 360, and Frost and Sullivan, 2015, 18, https://iamcybersafe.org/

wp-content/uploads/2017/01/FrostSullivan-ISC%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf#page=18.

101 "Median weekly earning of full-time wage and salary workers by certification and licensing status and selected characteristics, 2017 annual averages," United States Department of Labor Bureau of Labor Statistics, last modified February 08, 2018, https://www.bls.gov/cps/cpsaat54.htm.

102 Michael Prebil, "Come What May: Embedding Tech Skills for the Future of Work," New America, November 20, 2017, https://www.newamerica.org/education-policy/edcentral/come-what-may-embedding-tech-skills-future-work/.

103 "The Narrow Ladder: The Value of Industry Certifications in the Job Market," Burning Glass Technologies, October 2017, 3, https://www.burningglass.com/wp-content/uploads/BurningGlass_certifications_2017.pdf.

104 "Cybersecurity Supply/Demand Heat Map" Cyberseek, http://cyberseek.org/heatmap.html.

105 "CISSP – The World's Premier Cybersecurity Certification," (ISC)2, accessed September 12, 2018, https://www.isc2.org/Certifications/CISSP.

106 This, like so many other questions in the cybersecurity job market, would be an excellent area for further research.

107 "TechHire Initiative," The White House President Barack Obama, accessed September 12, 2018, https://obamawhitehouse.archives.gov/issues/technology/techhire.

108 "TechHire," accessed September 12, 2018, https://techhire.org/.; TechHire is operated by Opportunity@Work, an independent 501(c)3 that was originally incubated at New America.

109 Tal Kopan, "Hacking contests ID cyber talent for government, industry," Politico, July 29, 2014, https://www.politico.com/story/2014/07/hacking-contests-id-cyber-talent-for-government-industry-109494.

110 "Competition Overview What does a School Need to Participate?," CyberPatriot, accessed September 12, 2018, https://www.uscyberpatriot.org/Pages/Competition/Competition-Overview.aspx.

111 "CyberPatriot X National Finalists Announced," GlobeNewswire, March 06, 2018, http://www.globenewswire.com/news-release/2018/03/06/1416123/0/en/CyberPatriot-X-National-Finalists-Announced.html.

112 "About: National Collegiate Cyber Defense Competition," National Collegiate Cyber Defense Competition, accessed September 12, 2018, http://www.nationalccdc.org/index.php/competition/about-ccdc.

113 Martin C. Libicki, David Senty, and Julia Pollak, Hackers Wanted: An Examination of the Cybersecurity Labor Market, The Rand Corporation, Santa Monica, CA: RAND Corporation, 2014, 73, https://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR430/RAND_RR430.pdf#page=98.

114 James Lewis, Economic Impact of Cybercrime: No Slowing Down, Center for Strategic and International Studies and McAfee, February 2018, 4, https://www.mcafee.com/us/resources/reports/restricted/economic-impact-cybercrime.pdf.

115 Steven Morgan, 2017 Cybercrime Report, Cybersecurity Ventures, October 16, 2017, https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf.

116 Jeh Johnson, "Cyberspace is the New Battlespace," Lawfare, March 07, 2018, https://www.lawfareblog.com/cyberspace-new-battlespace.

117 Invest to Improve: The Cybersecurity Talent Deficit, The Business-Higher Education Forum, 2017,

http://www.bhef.com/sites/default/files/bhef_2017_invest_to_improve.pdf.

118 Laura K. Bate, "The Cyber Workforce Gap: A National Security Liability?" War on the Rocks, May 17, 2017, https://warontherocks.com/2017/05/the-cyber-workforce-gap-a-national-security-liability/.

119 "NSF investments aim to address growing cybersecurity challenge," National Science Foundation, October 31, 2017, https://www.nsf.gov/news/news_summ.jsp?cntn_id=243566.

120 "Call for Cybersecurity Curriculum Development Grant Proposal," National Initiative for Cybersecurity and Career Studies, April 3, 2017, https://niccs.us-cert.gov/featured-stories/call-cybersecurity-curriculum-development-grant-proposal.

121 "CyberCorps (R) Scholarship for Service (SFS)," National Science Foundation, accessed September 12, 2018, https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=504991.

122 "California Apprenticeship Initiative," Foundation for California community Colleges, accessed September 12, 2018, https://foundationccc.org/What-We-Do/Workforce-Development/Workforce-Services/California-Apprenticeship-Initiative.

123 Steve Linthicum, "Driving an effective cybersecurity apprentice program (Part 1)," Certificati on Magazine, February 13, 2017, http://certmag.com/driving-effective-cybersecurity-apprentice-program-part-1/.

124 Department of Labor "U.S. Department of Labor Announces Funding Opportunity for Apprenticeship Expansion in Key Industry Sectors," news release, July 18, 2018, Department of Labor, accessed September 12, 2018, https://www.dol.gov/newsroom/releases/eta/eta20180718.

125 The NICE Conference and Expo (https://niceconference.org/) and the NICE K12 Cybersecurity Education Conference (https://www.k12cybersecurityconference.org/).; Editor's Note: In partnership with Florida International University, New America has been awarded the five-year grant to host the NICE Conference and Expo.

126 "NICE Working Group," NIST, last modified August 28, 2018, https://www.nist.gov/itl/applied-cybersecurity/nice/about/working-group.

127 "Cyber warriors: Disabled veterans begin new cybersecurity careers with DIT's help," North Carolina Department of Information Technology, January 10, 2018, it.nc.gov/blog/newsletter/01-09-2018/cyber-warriors-disabled-veterans-begin-new-cybersecurity-careers-dit's.

128 "Cybersecurity Apprenticeship Program (CAP)," ISG, accessed September 12, 2018, http://isglink.com/apprenticeship-program/.

129 2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk, Center for Cyber Safety and Education, (ISC)2, Booz Allen Hamilton, Alta Associates, and Frost and Sullivan, 2017, 3, https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf#page=3.

130 "Cyber security CNI apprenticeships," Department of Digital, Culture, Media, and Sport, updated January 26, 2017, https://www.gov.uk/guidance/cyber-security-cni-apprenticeships#benefits-for-industry.

131 A Skills Beyond School Brief on Austria, Germany, and Switzerland, The Organization for Economic Co-operation and Development (OECD), November 2014, http://www.oecd.org/education/skills-beyond-school/skills-beyond-school-Austria-Gemany-Switzerland.pdf.

132 Elizabeth Redden, "Importing Apprenticeships," I nside Higher Ed, August 08, 2017, https://www.insidehighered.com/news/2017/08/08/interest-grows-us-germanswiss-model-apprenticeships.

133 Ryan Craig and Tom Bewick, "Making Apprenticeships Work Five Policy Recommendations," University Ventures, February 04, 2018, http://universityventures.com/images/Making_Apprenticeships_Work_-_UV_Whitepaper.pdf.

134 Stephen Babcock, "TranZed is introducing a new way to train tech workers: Apprenticeships," Technical.ly, December 06, 2016. https://technical.ly/baltimore/2016/12/06/tranzed-tech-apprenticeships-utx/

135 "Central Illinois Center of Excellence for Secure Software," ISHPI, accessed September 12, 2018, https://www.ishpi.net/about-us/community-initiatives/cicess/.

136 "Cyber Apprenticeship," Peregrine News Updates, September 29, 2016, http://www.gbpts.com/blog/cyber-apprenticeship.

137 "Bridging the gap between training opportunities and workforce needs," New Mexico Information Technology Apprenticeship Program, accessed September 12, 2018, https://nmitap.org/.

138 Keith Breene, "Who are the cyberwar superpowers?" World Economic Forum, May 04, 2016, https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/.

139 Natasha Cohen, Rachel Hulvey, Jittip Mongkolnchaiarunya, and Anne Novak , Robert Morgus and Adam Segal, Cybersecurity as an Engine for Growth, Washington D.C., New America, September 21, 2017, 13, https://na-production.s3.amazonaws.com/documents/FINAL_Clusters.pdf#page=13.

140 Richard Behar, "Inside Israel's Secret Startup Machine," Forbes, May 11, 2016, https://www.forbes.com/sites/richardbehar/2016/05/11/inside-israels-secret-startup-machine/#7db503c91a51.; Tim Johnson, "How Israel became a leader in cyber security and surveillance," McClatchy DC Bureau, February 21, 2017, http://www.mcclatchydc.com/news/nation-world/national/national-security/article134016454.html.

141 For more on such partnerships, see Adam Segal, Rebuilding Trust Between Silicon Valley and Washington, Council on Foreign Relations, January 2017, https://cfrd8-files.cfr.org/sites/default/files/pdf/2017/01/CSR78_Segal_Silicon_Valley.pdf.

142 Simone Petrella, "Cybersecurity's Disastrous Game of Chicken,"Humans of Cybersecurity, New America, July 13, 2017, https://www.newamerica.org/cybersecurity-initiative/humans-of-cybersecurity/blog/cybersecuritys-disastrous-game-chicken/.

143 Shaun Donovan, Beth Cobert, Michael Daniel, and Tony Scott, "Strengthening the Federal Cybersecurity Workforce," The White House President Back Obama, July 12, 2016, https://obamawhitehouse.archives.gov/blog/2016/07/12/strengthening-federal-cybersecurity-workforce.; Exec. Order No. 13800, C.F.R. 3 # (2017), https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.

144 Reviewing Federal IT Workforce Challenges and Possible Solutions: Hearing before the Subcommittee on Information Technology, House of Representatives, 115th Congress (2017), https://oversight.house.gov/hearing/reviewing-federal-workforce-challenges-possible-solutions/.; Challenges of Recruiting and Retaining a Cybersecurity Workforce: Hearing before the Cybersecurity and Infrastructure Protection Subcommittee of the Homeland Security Committee, House of Representatives, 115th Congress (2017), https://homeland.house.gov/hearing/challenges-recruiting-retaining-cybersecurity-workforce/.; U.S. House of Representatives, "House Subcommittees Discuss Development of Cybersecurity Apprenticeships to Meet Growing National Security Needs," news release, October 24, 2017, Committee on Education and the Workforce, accessed September

12, 2018, https://edworkforce.house.gov/news/documentsingle.aspx?DocumentID=402064.

NEW AMERICA