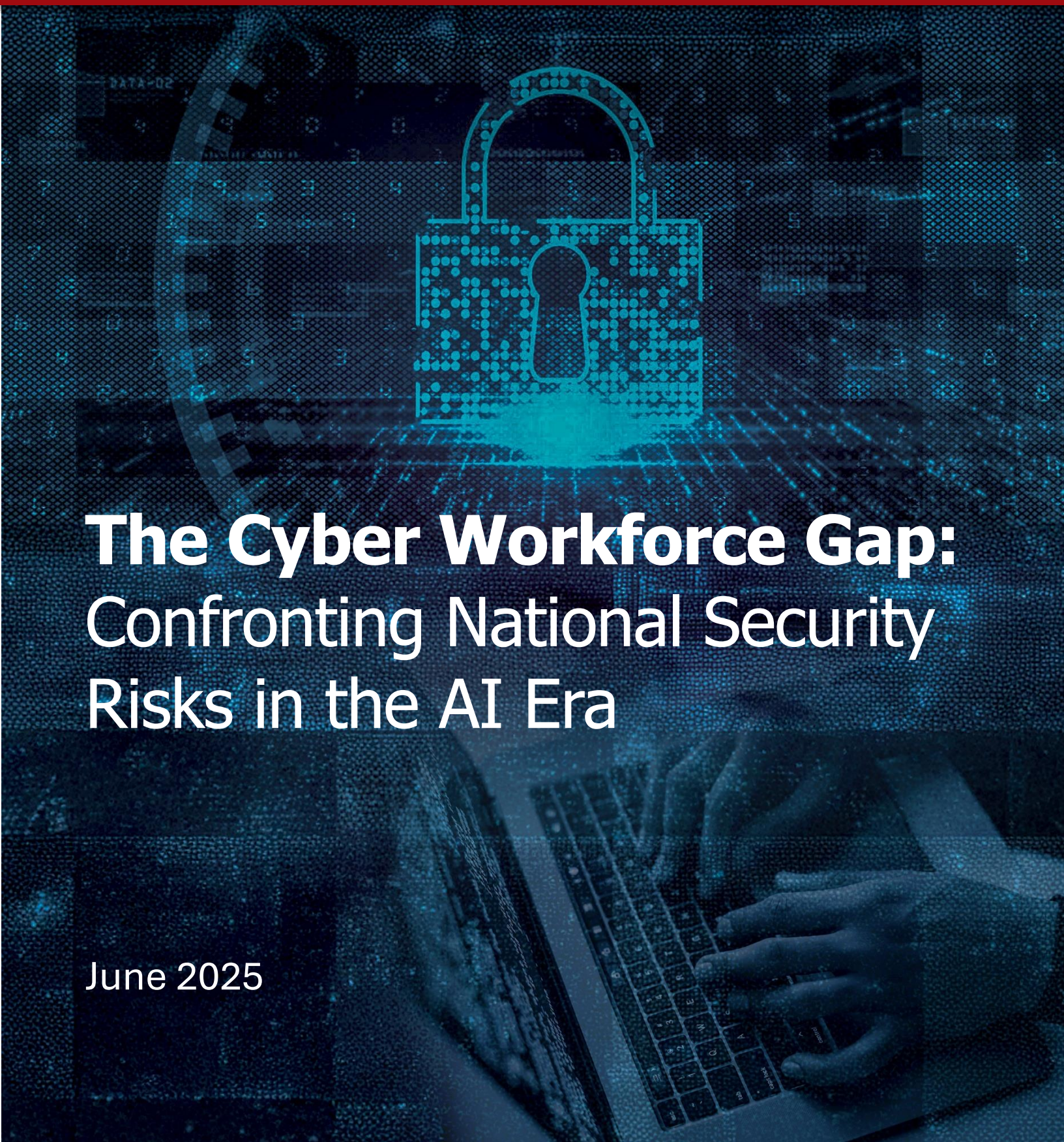
BENS INSIGHTS:
Elevating Thought Leadership in National Security

BUSINESS EXECUTIVES FOR NATIONAL SECURITY
SECURING AMERICA'S FUTURE



The Cyber Workforce Gap: Confronting National Security Risks in the AI Era

June 2025

The Cyber Workforce Gap

U.S. defensive capabilities in cyberspace will be unable to mitigate evolving information warfare and its accompanying doctrine implemented by state and non-state advanced persistent threat (APT) groups. Private sector estimates highlight a massive deficit in filled U.S. (and North American) cybersecurity roles, with some ranging as high as 522,000. While the People's Republic of China (PRC) faces the largest workforce shortage—potentially increasing its talent gap to 3.27 million individuals by 2027—the state's intensive investment in developing a competitive cyber headcount places it as the pacing threat. Furthermore, with the growing usage of artificial intelligence (AI) to distribute ransomware-laced emails, a workforce that can detect and respond to any number of threats is paramount. To determine how public-private partnerships can effectively enhance the U.S. homeland's virtual security, we must assess different approaches to addressing human capital concerns as this critical sector and the role private stakeholders play in broader national interests rapidly evolve.

Nicholas Andersen
President and COO
Invictus International Consulting LLC

Gregg Azcuy
President and CEO
Storage Engine Incorporated

Elizabeth Wharton
Founder
Silver Key Strategies

Note: Interviews have been edited for length and clarity. The views expressed are their own and may not reflect those of their employers or BENS

Why is it important to have a healthy and skilled cybersecurity talent pool within the U.S. national security enterprise? What role do you see AI, large language learning models, and other agents play in maximizing cybersecurity frameworks' potential?

Nicholas Andersen: Cyber warfare and digital attacks drastically lowered the cost threshold for malicious actors to operate, which is a huge shift. Kinetic operations traditionally had a high barrier to entry—you needed resources, recognition, and capabilities—and that kept a lot of players out. But with cyber, that playing field is leveling fast. Since the attack surface keeps expanding, every single industry needs to take cybersecurity seriously. It doesn't matter if it's a traditional defense contractor like Boeing, Lockheed, Huntington Ingalls, or something more abstract. You can have an attack on a content delivery network, and suddenly a streaming service is offline. That might seem trivial, but if that's how people get their information there are real national security implications. Even social platforms like Facebook contribute to national resilience by enabling people to check in and reassure loved ones after natural disasters, especially when traditional communication networks fail. As the world becomes more interconnected, the demand for cybersecurity talent is outpacing traditional pipelines, putting us at a significant disadvantage.

When you add in the impact of AI and large language models, you're looking at both a massive opportunity and a significant risk. On the one hand, automation helps defenders because we can hand off repetitive, grunt work to machines and let humans focus on what we're uniquely good at. We can build solid, reliable models to defend ourselves more efficiently. But on the other hand, this tech also lowers the bar for attackers. It means people need less knowledge and expertise can cause harm. We will need a whole new skillset from our cybersecurity workforce, since this isn't just about tools. It's about how we vet and evaluate models, as well as how we evaluate and understand the data, weighting, and logic behind outputs.

Gregg Azcuy: As threats evolve at an unprecedented pace, a deep bench of cybersecurity professionals ensures that the U.S. cannot only defend against attacks but anticipate and outmaneuver adversaries. Investing in a healthy talent ecosystem is a fundamental element of resilience and strategic advantage. Artificial intelligence, large language models, and emerging autonomous systems offer tremendous potential to strengthen cybersecurity defenses. These technologies can and do accelerate threat identification, enhance pattern recognition, and automate incident response. Yet, current guardrails around AI models are often insufficient; motivated adversaries are already finding ways to bypass protections. To maximize their positive impact while minimizing risk, AI tools must be deployed thoughtfully, some are already built into storage arrays—with rigorous governance, continual testing, and human oversight at their core.

One other important area to highlight is the growing need to preemptively prepare for the post-quantum era in cybersecurity. As quantum computing progresses steadily, the risk they pose to existing encryption is immediate despite full-scale systems still being years away. Adversaries are already working to steal encrypted data today with the expectation that it can be broken once quantum capabilities mature. The U.S. Department of Defense (DOD) has two national security directives addressing this, but compliance is very low. Post-Quantum Encryption (PQE/PQC/QSE) must be integrated into national security planning now, not deferred until quantum technology is fully realized. Transitioning critical systems and communications to quantum-resilient encryption standards requires focus, coordinated strategy, and

sustained investment. By proactively embracing PQE now, we can mitigate future vulnerabilities, protect sensitive information across its full lifecycle, and ensure the resilience of U.S. national security systems well into the future. Furthermore, talent in quantum computing is more acute than that of AI engineering and is becoming ever more concerning as this is unaddressed in a meaningful, coordinated way.

Elizabeth Wharton: Beginning with the healthy and skilled cybersecurity talent pool in national security, when you hear about attacks –whether they're from nation-state sponsored groups or not—the level of sophistication, training, resources, and knowledge are essentially identical to a nation-state's capabilities. And they aren't just targeting government systems; they're going after companies embedded in everyday life—travel, personal data, financial systems, even casinos like Caesars Palace and MGM. These threats impact every layer of daily life for U.S. citizens. When responding, we need people who are not only defending our systems but actively hunting threats—some of which have been sitting inside our critical infrastructure for extended periods of time. If we expect to keep the lights on, elevators running, and our data protected, we need defenders who can act immediately. These defenders can't do that if they're burned out or undertrained, which is unsustainable.

In terms of AI, large language models (LLMs), and other systems, we're asking both people and machines to process exponentially more data and make sense of it quickly. The only way to scale that is through automation. But automation must be guided by humans who know how to use it—people who understand the data, who can prompt effectively, who know how to interpret what these models are spitting out. If you don't know what to ask, or what the data means, the AI won't help you. It's like asking a doctor to diagnose a patient without telling them all the symptoms.

What does the cybersecurity talent pipeline look like, and are there any glaring deficiencies in the current process? Overall, what is the ideal course of action to take in addressing these problems?

Nicholas Andersen: The traditional talent pipeline has always been going to college, getting a degree, landing an entry-level job, and then receiving specialized training. But when it comes to the cybersecurity space, that model just can't keep up. You see job postings asking for 10 years of experience with technologies that haven't even existed for a decade. Or you see roles requiring a college degree when a degree doesn't really make someone any better or worse at doing that job. The capacity we're going to need in this field is immense, and there is no way we can meet that demand through traditional paths alone. In my view, we should be looking at more apprenticeship-style programs and other ways to bring in non-traditional workforce entrants. That includes children coming straight out of high school. For example, in Fairfax County, Virginia, there are some phenomenal programs that allow students to graduate high school with certifications and technical training.

At my company, we also focus heavily on hiring military veterans, particularly those with four to twelve years of service—experienced enough to contribute immediately, but not so senior that their background is primarily in oversight. They often arrive with security clearances, which are essential for our national security work, and signals trustworthiness and reliability even when not required. Due to clearance timelines, we usually engage students by the summer between their sophomore and junior years. We bring

them into our company's internship program, start the clearance process, and by the summer before their senior year, have them work as full-time paid interns. Ideally, they're already cleared and trained enough that we can bring them on full-time after graduation. But that's a multi-year investment. This is the reality when you work in national security. Overall, there are a ton of gaps in the pipeline, but it's not always a resource issue. There are multiple programs that help cover the cost of certifications or offer scholarships for cybersecurity training. To me, the biggest challenge is messaging. Are we telling people that this is a space they can enter, where they don't have to be coders or computer scientists to be successful? We need people who can solve hard problems, think critically, and can look at something and say, "this doesn't look right." Getting that message out and making it stick will be key to long-term success.

Gregg Azcuy: The cybersecurity talent pipeline remains a critical and growing area of concern. While there have been commendable efforts across government, academia, and industry, the overall supply of highly skilled cybersecurity professionals remains insufficient to meet the scale, speed, and sophistication of today's evolving threats. Specialized areas such as threat intelligence, AI-enabled cybersecurity, and quantum-resilient security face particularly acute shortages at the time when adversarial capabilities are accelerating. Many cyber defense functions that once relied on human intervention must now be fully automated, further shifting the demand toward highly technical, AI-proficient expertise. Additionally, the current ecosystem lacks unified standards for cybersecurity education, clear career pathways, and sufficient incentives to attract and retain top-tier talent. The lengthy and complex security clearance process remains a significant barrier to quickly onboarding new cybersecurity staff, especially those who are technically qualified but lack immediate eligibility.

Addressing these deficiencies requires a comprehensive and coordinated strategy. Building an enduring cybersecurity workforce must be treated as a national strategic investment, beginning with early STEM engagement, expanding public-private training partnerships, accelerating clearance processes for qualified candidates, and creating rewarding career trajectories that span government, industry, and academia. Just as important, the cybersecurity workforce must be agile and prepared for continuous innovation, as AI and emerging technologies reshape the very definition of cybersecurity expertise daily. We must also face the reality that a large portion of U.S.-trained science and engineering doctorates are awarded to non-U.S. citizens. We need to construct a policy to provide a path to citizenship to retain this talent pool in the U.S.

Elizabeth Wharton: Right now, you have college graduates, or people transitioning from other roles, all trying to land new opportunities. If you check LinkedIn, one of the most popular careers was AI prompt engineering. A couple of years ago, that was *the* job, and everyone was rushing to learn how to ask the right questions. But now many people know how to complete this task, meaning people pursuing that specific career track must pivot. The need to pivot is one of the bigger challenges because people get locked into rigid definitions of what constitutes a "job" instead of stepping back and asking about the underlying skills. Essentially, if the tech shifts—and it will—the workforce needs to shift as well. Another thing that the cybersecurity sector realized is that if people don't understand how the code works, there are no ways to improve it. This leads us to question whether everything from fundamental skills to other expertise that will still matter six months or a year from now is still being taught.

The cybersecurity talent cycle must be rethought in a way that particularly emphasizes the fundamentals, since those core skills can transfer across jobs. One path I've seen is a return to more vocational-style training. Not everyone needs a PhD or a master's degree to work with code in cyberspace, which makes us

wonder what happened to apprenticeship models. In those processes, candidates needed just the basics. This leads me to question whether we can teach people just enough to get started before building their skills from there. Look at hands-on industries—HVAC, electrical, plumbing. You start with the fundamentals, and once you have that, you can specialize. And if things change, you can go back, retrain, learn more. But you've got a foundation. It's faster because you're not waiting seven years and completing a dissertation in a field that might look completely different in a year.

Where does the private sector face the biggest challenges when working with the U.S. Government on cybersecurity issues? What are some examples of successful cybersecurity coordination, and why were they successful?

Nicholas Andersen: I think the largest challenge right now is getting real value out of government programs. There are countless initiatives you can engage—threat intel exchange program, DHS' indicators of compromise (IOC) system, Information Sharing and Analysis Centers (ISACs), InfraGard—the list goes on. These programs do have value, especially when it comes to building relationships. But outside relationship-building, many of these programs place a heavy burden on the private sector without delivering an equivalent benefit. This is especially true when talking about threat intelligence sharing. Too often, the information that is shared is already available through open-source channels. On top of that, the government's internal review process slows everything down. The result is that by the time something gets released, it's no longer actionable or timely. Concerns around classification, sources, and methods are legitimate. But unless we find a way to reduce those barriers—to share high-quality, useful information quickly—we're not going to see the private sector continue to invest time and resources into these programs. I think we really need to focus our efforts on improving those information-sharing pipelines, making them more effective and valuable. At the same time, we also need to keep supporting the longer-term investments, like university programs or DHS/NSA Centers of Academic Excellence. Going further, we need to similarly start engaging students earlier to give them a real, visible pathway into the national security workforce and cyberspace.

Gregg Azcuy: The private sector encounters several critical challenges when partnering with the U.S. Government on cybersecurity efforts. Chief among them is the instability caused by recurring continuing resolutions, which introduce funding uncertainty and inhibit companies' ability to invest in long-term, innovative cybersecurity solutions. Without clear visibility into sustained funding commitments, the private sector remains reluctant to dedicate significant resources and talent to national security initiatives. Adding to this instability is the standard "Termination for Convenience (T4C)" clause embedded in government contracts. While a longstanding feature of federal procurement, the recent increase in T4C actions has further eroded confidence in long-term public-private collaboration, especially in fields demanding continuous innovation and investment. Procurement processes present an additional challenge. The heavy reliance on generalized requests for quotations and lowest-price-award models, or having to work through existing contractors, often prioritizes short-term cost savings over long-term mission effectiveness. As a result, moving toward value-based contracting and performance-driven partnerships would more effectively align public and private sector efforts against sophisticated adversaries.

There are strong examples of successful collaboration between public and private sectors. NSA's Cybersecurity Collaboration Center and CISA's Joint Cyber Defense Collaborative (JCDC) demonstrate that early engagement, shared threat intelligence, and aligned objectives can drive highly effective public-private partnerships. Recently, new initiatives in quantum, like DARPA and the State of Maryland, the Cleveland Clinic and Miami University (OH) have been established. Microsoft President Brad Smith, also recently appealed for the USA and allies to strengthen investment, workforce development, and supply chain security for quantum and technology in general. But much more is still needed.

Elizabeth Wharton: One of the biggest challenges right now is that people don't know what to do when they see a problem. They get an alert or notice something's off—like someone accessing protected data. Maybe it's on a critical infrastructure system and it *looks* like a threat actor is poking around. The reaction is usually, *Okay… I should probably tell someone about this*. But then companies don't know what to do next, wondering who they need to speak with, how to communicate what's happening, and how to deescalate the situation. That whole "now what?" moment is a huge gap. It's not just about seeing the issue—it's about understanding how to share that information productively. The challenge becomes: how do we filter out the noise and bring forward what matters? We talk a lot about spotting vulnerabilities, but are we equipping people to raise the right flags, to the right people, in the right way? That's where collaboration and tuning—whether it's human processes or machine models—really comes into play.

I've seen examples where collaboration has worked, like when the FBI worked with private-sector partners at Lumen and Microsoft to collectively go after the threat actors behind Salt Typhoon or various crypto-related scams. These efforts worked because each party didn't try to compete for credit. It was about rising above the noise, bringing what was being witnessed to the table, and collaborating jointly. Partnerships like this example are successful because of the communication, sharing, and working past legal and organizational barriers. It's not about embarrassing anyone—it's about protecting systems and moving the ball forward together.

1030 15th St. NW · Suite 200 East
Washington, DC 20005
www.BENS.org | X: @BENS_org | 202.296.2125