THE CYBER DEFENSE REVIEW
In press, 8 pages
https://doi.org/10.55682/cdr/s46q-kxsv

SENIOR LEADER PERSPECTIVE

Wrong Players, Wrong Game: Rethinking Who Belongs in Cyber

Lt. Gen. (Ret.) Mary O'Brien*

Former Joint Staff Director of Command, Control, Communication, & Computers/Cyber (J6), USA

The term 'cyber' no longer maps cleanly onto the domain it once described. Today, 'cyber' encompasses everything from data governance, autonomous systems, and artificial intelligence, to the cascading interdependencies of critical infrastructure — yet the workforce structure and team compositions have not kept pace with these changes. This article argues that the mismatch is not primarily a technology problem, but a talent and framing issue. By continuing to recruit and organize cyber teams as though 'cyber' remains a narrow technical discipline, the United States risks fielding the wrong players for a global competition that has fundamentally changed. Drawing from direct leadership experience navigating these gaps in the Air Force, Joint Force, and across industry, the author identifies five non-technical disciplines that belong inside the cyber tent. She outlines the justification for including behavioral science, political science and international relations, economics and game theory, organizational behavior, and public health. She then proposes a corrective strategic approach to workforce development, hiring, and institutional culture that would begin to close the gap.

Keywords: cyber workforce; interdisciplinary teams; cyber domain expansion; talent pipeline; non-STEM; workforce development; strategic competition; organizational behavior; critical infrastructure

* Corresponding author: mobrien@mobrienstrategies.com

Lieutenant General (Ret.) Mary O'Brien's final assignment was as Joint Staff Director of Command, Control, Communications and Computer/Cyber and Chief Information Officer, J6. Over a 34-year Air Force career, her senior assignments included: Deputy Chief of Staff for Intelligence, Surveillance, Reconnaissance and Cyber Effects Operations at Headquarters Air Force; Commander, Twenty-Fifth Air Force; and Director of Intelligence, J2, at U.S. Cyber Command. She retired in 2023. Now in private industry, she serves on the Strategic Advisory Council of Ondas, Inc (NASDAQ:ONDS), the Advisory Council of Cyabra (NASDAQ:CYAB), the Advisory Board of Markon, and The Cyber Guild Advisory Council. She also serves the military veteran community as an independent director for Operation Homefront on the cyber technology and development committees. Gen. O'Brien holds a B.S. in Chemistry from the U.S. Air Force Academy, a M.A. from The George Washington University, and a M.S.S. from Air War College.

Close your eyes and picture someone you know who works in cybersecurity. Is the person a man in his 30s, with a computer science or other STEM degree, sitting in a dimly-lit room at a desk with multiple monitors, perhaps wearing a hoodie? Now, imagine a conversation with this person. Did he speak in acronyms about his preferred operating system and programming language, and become slightly impatient with anyone who didn't understand? I'll bet if you ask him about organizational dynamics or human psychology, he would tell you those topics are for people with soft skills, and he wouldn't mean it as a compliment.

That image, while a stereotype, is not uncommon. For a long time, both public and private cyber professionals were required to have extensive technical backgrounds and experience, documented by credentials that demonstrate technical breadth and depth, along with years of experience in key roles (Romanosky, Schwindt, and Johnson 2023). These were reasonable expectations for operating in a past version of the cyber domain — a much narrower one focused on network intrusion, malware analysis, and penetration testing. The stereotype of who belongs in 'cyber' is a problem today because the outdated stereotype has outlived its usefulness, now that the domain has greatly expanded. In most cases, our mental model of who belongs in this critical workforce has not caught up.

My hypothesis is that **we are fielding the wrong players for a global competition when the game has fundamentally changed**. The consequences of that mismatch are severe. They show up in operations, in policy failures, and in missed warning signals. Our adversaries are adroit at exploiting dimensions of a new environment that our STEM-oriented teams are less equipped to detect or defend against.

A DOMAIN THAT HAS OUTGROWN ITS DEFINITION

When the U.S. Department of Defense (DoD) published its first Strategy for Operating in Cyberspace in July 2011, formally designating cyberspace as the fifth operational domain alongside land, air, maritime, and space, the framing made sense for that moment in time (U.S. Department of Defense 2011). Depending on who you asked, 'cyber' meant Information Technology (IT) network management tasks performed by network administrators and help desk personnel triaging trouble tickets, with their success measured in network uptime and internet connectivity. It was an infrastructure management problem, not a strategic one.

On the other hand, security researchers, defense journalists, and policy wonks were discussing the implications of the sophisticated Stuxnet worm targeting Iranian centrifuges, although it barely registered with the general public. U.S. Cyber Command became partially operational in 2010, under the authority of the U.S. Strategic Command. The 2011 strategy was itself framed almost entirely around protecting networks, defending DoD systems, and developing offensive cyber capabilities for warfighting. Whether referring to IT or national security, the language describing cyber was domain-specific and infrastructure-focused. 'Cyber' meant the networks, and it seemed logical to look for the workforce to perform that work in existing technical fields related to the networks.

That framing is now insufficient. 'Cyber' in 2026 encompasses data as a strategic asset and as a weapon. It encompasses autonomous systems that make consequential decisions with, or without, human intervention. It encompasses the artificial intelligence layers that now sit beneath nearly every sensitive national security system (Ribeiro 2026). Perhaps most consequentially, it encompasses the cascading interdependencies of critical infrastructure, such as power grids linked to water systems linked to food distribution linked to financial markets, where a targeted disruption in one sector can rapidly propagate into crises that look nothing like a cyber attack to the people experiencing them in other sectors (World Economic Forum 2025).

In early 2024, I had an opportunity to talk privately about emerging technology to a congressional representative who also operates a family farm. He mentioned that the farm uses drones for a variety of functions, from monitoring crop health to making decisions about fertilizers and pesticides to detecting moisture levels for irrigation efficiency. It won't be a surprise to people following the major drone commercial suppliers that a well-known Chinese drone company manufactured his drones, now operating in the heart of "America's breadbasket."

I respectfully walked him through a hypothetical scenario in which his foreign agricultural drones are used as delivery vectors for cyberattacks. As a farmer and Member of Congress, he already fully understands the vital role of the Agriculture and Food Sector in U.S. critical infrastructure, with its complex system of networks necessary for the production, processing, and distribution of food and agricultural products, contributing to nearly 20% of the U.S. economy. He also appreciates the importance of digital and cyber infrastructure as modern agriculture relies heavily on GPS, automation, robotics, and data management systems. It was not, repeat not, clear to me if he understood that cyber attacks on the food and agriculture sector, especially targeting small and mid-sized (family) farms, are rising rapidly, with a 101% global increase in 2025.

Who owns the policy response to that conversation? Which experts belong at the table to mitigate the cyber risks to agriculture, just one of the 16 Critical Sectors designated by Presidential Policy Directive 21 in 2013 (Executive Office of the President 2013)? Are these responsibilities reserved for our traditional 'cyber' workforce? I offer my discussion with the congressman as one of many potential examples of how work that needs to be performed in the 'cyber' domain expanded, but the updated workforce and organizational structures we need were left behind.

We are still relying on a 2011 'cyber' workforce model to address our 2026 'CYBER' challenges.

AN ATTEMPT AT WORKFORCE EVOLUTION

During my tenure as the Headquarters Air Force Director of Intelligence, Surveillance, Reconnaissance and Cyber Effects Operations (A2/6), I decided to reclassify all of our cyber enlisted Airmen from 'enabling' Air Force Specialty Code (AFSC) designations to 'operations' designations. The personnelists resisted my decision because the change would disrupt long-established classification structures, and, probably more concerning to them, implementing the new AFSC designations would require programming updates in their fragile legacy databases. Other Air Force senior leaders pushed back because the enlisted Airmen were not performing tasks clearly associated with airplanes and airpower–their definition of 'operations.' Most surprising to me, some of the enlisted cyber Airmen argued against including the entire community and wanted to make distinctions between Internet Protocol (IP)-based functions and Radio Frequency (RF) functions, which I considered inconsequential, but were important in their community.

We pressed forward with the change and reclassified everyone into the new 'operations' AFSC. We achieved the results I intended. There was better alignment with the cyber officers, who were already included in the 'operations' designations, and a more explicit acknowledgment throughout the force of the critical role these Airmen perform in order for the Air Force to deliver airpower, any time, anywhere.

Several years and a transition to private industry later, I'm still reflecting on lessons from my experience broadening the view of the Air Force enlisted cyber Airmen. The way we label and categorize the 'cyber' workforce powerfully shapes who we believe belongs in it. If we define cyber primarily as a technical function requiring credentials versus demonstrated skills, we will hire primarily for technical credentials (Romanosky, Schwindt, and Johnson 2023). We will build teams organized around technical specialties, and we will evaluate performance against technical metrics. We will systematically exclude or undervalue people who don't fit into that mental model, regardless of what skills they could contribute.

A DIFFERENT MENTAL MODEL

The stereotypical cybersecurity professional, technically brilliant, domain-narrow, and skeptical of 'soft' disciplines, is not an exaggeration. When that mental model dominates how cyber teams are built, evaluated, and promoted, it creates a self-reinforcing cycle. We hire people who match the model, and as a result, they design and implement partial solutions limited to the technical aspects of more complex problems. Understandably, they frequently miss detecting and identifying all dimensions of the problems.

The hardest problems in cyber do not fit into one mental model, and neither should the majority of the workforce. For example, deterrence is not a purely technical problem, although there are technological aspects to it. It has links to perception, signaling, and strategic psychology. An insider threat is not a network security problem. It is an organizational behavior and human factors problem. The exponential growth of disinformation and influence operation campaigns on social media platforms is a social science problem that exploits technical vectors to deliver their narratives to the targeted audience. Some of the critical infrastructure under attack, such as the previously-mentioned agriculture,

as well as medical, water, and energy, could ultimately be viewed as a public health-adjacent problem about cascading system failure and the significant impact on population centers.

Are we trying to engineer our way out of complex 'cyber' problems that require a different kind of expertise? In some studies and publications, there are recommendations to add requirements for additional competencies (dare I say 'soft-skills') on top of the already lengthy list of technical credentials demanded from the cyber workforce (Dawson and Thomson 2018). This is an unfortunate trend that results in frustrating searches for "unicorns" and leads to burnout among technical cyber experts trying to be all things to everybody. The type of experts we need to add to the 'cyber' team is out there, but we have built mental models and institutions with structural barriers to recruit the right people.

FIVE DISCIPLINES THAT BELONG IN THE GAME

In my experience, vague calls for 'interdisciplinary teams' have a way of generating agreement without generating action. Therefore, I offer the following five disciplines as specific, but not exclusive, examples of the types of required experts as a challenge to an incomplete mental model of the traditional cyber workforce, given what the domain now encompasses.

Psychology and behavioral science. The attack surfaces in most significant cyber operations are the human beings with access to the network. Social engineering, phishing, insider exploitation, and influence operations all rely on behavioral vulnerabilities (Muhly et al. 2025). Understanding why people make the decisions they make under uncertainty, stress, and incomplete information is not a soft-skills add-on. It is a core competency for anyone defending systems that humans use.

Political science and international relations. Cyber operations occur in a geopolitical context. Geopolitical considerations shape what is possible, what is permissible, and what is strategically wise. Attribution, escalation management, alliance coordination, and norm-setting are political science constructs (Lewis 2022). A cyber team executing technical operations against a state, or non-state, actor in the absence of a full understanding of the potential strategic and diplomatic consequences of those operations is operating in the dark. Operational planning should include experts who understand alliance equities, escalation dynamics, and adversary decision-making before the first packet is sent.

Economics and game theory. Adversary actors in cyberspace are making strategic cost-benefit calculations, managing risk, and responding to incentives (Morgan 2024). Deterrence theory, sanctions design and enforcement, and the economics of vulnerability markets all require economic reasoning. Game theory offers frameworks for reasoning about adversary decision-making under uncertain conditions that are directly applicable to cyber competition. These frameworks are rarely taught in technical programs.

Sociology and organizational behavior. Cyber resilience is an organizational property as well as a technical property. How organizations respond to incidents, how quickly information flows (or doesn't flow) across bureaucratic or hierarchical boundaries, how workforce culture shapes whether certain people get exceptions to best security practices are all sociological and organizational questions (Huang and Pearlson 2020). Persistent failure to implement basic security hygiene across a large organization is not primarily a technical failure. It is a culture and behavior problem. Organizational behaviorists

and sociologists understand how nudges, defaults, and social norms drive compliance far more reliably than policy mandates alone.

Public health. Even prior to the COVID-19 pandemic, the public health field has spent decades developing frameworks for understanding how threats propagate through populations, how to model cascade effects in complex interdependent systems, and how to design interventions that work at scale under uncertainty (Trump et al. 2017). These efforts offer transferable frameworks to questions about critical infrastructure resilience, cyber epidemic modeling, and the management of large-scale cyber incidents. The intellectual cross-pollination between cyber and public health remains essentially unexplored.

OUR ADVERSARIES ARE NOT MAKING THIS MISTAKE

China's cyber operations are not executed by technical teams working in isolation from strategic and behavioral context. The integration of linguists, psychologists, and influence specialists into cyber operations is widely documented and reflects a different mental model of the domain (Beauchamp-Mustafaga 2023). Russia's information operations similarly blend technical capability with social science expertise in ways that have proven effective precisely because they target human systems, in addition to targeting technical systems and networks (Hoffman 2025).

While we debate, we are already competing against adversaries who have already internalized that the most exploitable vulnerabilities in the modern 'cyber' operating environment are human and institutional. The gap between their conception of cyber operations and ours is a talent and skills gap, as well as a doctrine and operational planning gap (Beauchamp-Mustafaga 2023).

WHAT CORRECTIVE ACTION LOOKS LIKE

Candidly, I am more confident in the diagnosis than in my prescription. Institutional change of this kind is slow and contested. I have observed dozens of well-intentioned reform efforts lose momentum to be appropriately circumspect about whether my recommendations will result in changes. That said, there are concrete starting points.

Rewrite the credential filters. Cyber workforce hiring, in both government and the private sector, relies heavily on STEM credentials and technical certification as screening mechanisms. Those filters should be supplemented with explicit pathways for candidates whose expertise lies in the five disciplines described above. This is a recognition that the existing standards respond to a narrower version of the problem than the problems we actually face today.

Invest in mid-career transition pathways. The talent we need might already be available. Mid-career political scientists, psychologists, economists, public health professionals, and other experts could significantly contribute to cyber work…with targeted bridging. Programs designed to facilitate that transition already exist, although at a modest scale. From my vantage point as an advisory council member of The Cyber Guild, a nonprofit focused on building inclusive pathways into the cyber workforce, I am participating in expanding a working model for connecting transitioning government and military professionals to cyber employers through mentorship, structured networking, and most importantly, explicit skills translation. They have expanded the pipeline by broadening the entry

criteria. Scaling programs, particularly those explicitly welcoming non-STEM professionals, would grow the workforce pipeline in ways that technical training programs alone cannot.

Change how we organize teams. Technical expertise should anchor cyber teams, not monopolize them. Embedding behavioral scientists, political analysts, and organizational specialists into operational planning at the working level would change the character of the analytical products those teams produce. This requires hiring different people and restructuring team charters and evaluation criteria to value interdisciplinary contributions.

Measure differently. Organizations produce what they measure. If cyber effectiveness is measured primarily in technical metrics, such as intrusion detection rates, patch compliance, or network availability, then that is what teams will prioritize. Incorporating measures of organizational resilience, evaluating the availability of decision quality information under adverse conditions, and assessing the effectiveness of human behavior-centered defenses would create incentive structures to make interdisciplinary contributions visible and valued.

THE NEXT 10 YEARS

The ongoing discussions about artificial intelligence today lead me to predict that the 'cyber' domain ten years from now will be shaped more by the breadth and quality of the human judgment we bring to bear, and less by the technical tools we build. We need to incorporate expert human judgment on how, when, and why to use those tools. The current 'cyber' workforce model will not get us there.

I cannot say with certainty what the optimal team composition should be for every future cyber task, but I am confident it differs from what we are currently fielding. Building the future workforce means conceding that the mental model we started with has reached its limit, and it's long overdue to expand beyond it.

We have talented players now. Let's put some new players in the game.

REFERENCES

Beauchamp-Mustafaga, Nathan. 2023. *Chinese Next-Generation Psychological Warfare: The Military Applications of Emerging Technologies and Implications for the United States.* RAND Corporation, June 1, 2023. https://www.rand.org/content/dam/rand/pubs/research_reports/RRA800/RRA853-1/RAND_RRA853-1.pdf.

Dawson, Jessica, and Robert Thomson. 2018. "The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance." *Frontiers in Psychology* 9 (June 12, 2018): 744. https://doi.org/10.3389/fpsyg.2018.00744. https://pmc.ncbi.nlm.nih.gov/articles/PMC6005833/.

Executive Office of the President. 2013. *Presidential Policy Directive 21: Critical Infrastructure Security and Resilience,* February 12, 2013. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

Hoffman, Frank. 2025. "Assessing Cognitive Warfare," November 14, 2025. https://smallwarsjournal.com/2025/11/14/assessing-cognitive-warfare/.

Huang, Kelman, and Keri Pearlson. 2020. *Building a Model of Organizational Cybersecurity Culture: Identifying Factors Contributing to a Cyber-secure Workplace.* MIT Sloan School of Management. https://mitsloan.mit.edu/shared/ods/documents?PublicationDocumentID=7507.

Lewis, James Andrew. 2022. *Creating Accountability for Global Cyber Norms.* Center for Strategic and International Studies, February 23, 2022. https://www.csis.org/analysis/creating-accountability-global-cyber-norms.

Morgan, Evan. 2024. "Eroding Global Stability: The Cybersecurity Strategies Of China, Russia, North Korea, And Iran," August 1, 2024. https://irregularwarfare.org/articles/eroding-global-stability-the-cybersecurity-strategies-of-china-russia-north-korea-and-iran.

Muhly, Fabian, Jennifer Jordan, Robert B. Cialdini, and Gregory P.M. Neidert. 2025. "Create a Company Culture That Takes Cybersecurity Seriously," June 24, 2025. https://hbr.org/2025/06/create-a-company-culture-that-takes-cybersecurity-seriously.

Ribeiro, Anna. 2026. "2026 and beyond: Urgent need for integrated cybersecurity strategies in evolving industrial landscape," December 14, 2026. https://industrialcyber.co/features/2026-and-beyond-urgent-need-for-integrated-cybersecurity-strategies-in-evolving-industrial-landscape.

Romanosky, Sasha, Karen Schwindt, and Ryan Johnson. 2023. *Comparison of Public and Private Sector Cybersecurity and IT Workforces.* RAND Corporation, February 7, 2023. https://www.rand.org/pubs/research_reports/RRA660-7.html.

Trump, Benjamin D., Kelsey Poinsatte-Jones, Meir Elran, Craig Allen, Bojan Srdjevic, Myriam Merad, Dejan M. Vasovic, and José Manuel Palma-Oliveira. 2017. "Social Resilience and Critical Infrastructure Systems." In *Resilience and Risk,* 289–299. Springer, April 25, 2017. https://doi.org/10.1007/978-94-024-1123-2_9.

U.S. Department of Defense. 2011. *Department of Defense Strategy for Operating in Cyberspace.* Washington, DC: U.S. Department of Defense. https://csrc.nist.gov/csrc/media/projects/ispab/documents/dod-strategy-for-operating-in-cyberspace.pdf.

World Economic Forum. 2025. "How to secure the digital future: Resilience, trust and leadership," October 16, 2025. https://www.weforum.org/stories/2025/10/securing-digital-future-cyber-resilience-trust-ai-age-gfc-amgfcc.