12

Cyber

From Bleeding Talent to Bleeding Edge

Vishaal “V8” Hariprasad and Casey “Waldo” Miller

Introduction

Russia has perpetrated software supply chain and ransomware attacks disrupting thousands of US businesses.[1] China has sponsored targeted attacks on research and academic organizations to steal intellectual property beneficial to its economy.[2] Cyber is a critical element of national power.[3] Yet, amid a rapid rise in digital crime and conflict over the last five years, the United States faces a critical shortfall of over seven hundred thousand cyber workers.[4]

Due in part to industrial-age thinking within hardware-centric services, the military is acutely affected by this technical cyber talent gap in areas that include (1) cyber roles and responsibilities; (2) technical talent management; and (3) acquisition risk avoidance.[5]

Companies across the nation are paying top dollar for cybersecurity and development talent. Near-peer and adversarial nations continuously demonstrate their maturation and are conducting cyberattacks of increased sophistication. The United States must field and rely upon a highly skilled and technical cadre of cyber talent to compete. How can the future US military force attract, train, and retain high-quality cyber talent?

This paper examines the various cyber roles with the Department of Defense (DoD), how leading companies manage equivalent talent, and how the current DoD budgeting and acquisition mentality detracts from retaining high-quality cyber talent. Ultimately, the DoD can improve the retention of critical cyber talent by empowering military workforce management at the unit level, getting compensation right, investing in and empowering continuity of expertise, and inverting the military cyber acquisition calculus.

The views expressed in this chapter are solely those of the individual authors and do not necessarily reflect the views of any organization with which they are, or have been, affiliated.

Military Cyber Roles

The DoD employs military, civilian, and contractor personnel in various cyber-related roles. Every role is vital in the cyber ecosystem, but cyber talent cannot be managed with a singular approach. Understanding how the DoD approaches cyberspace is essential to identifying and categorizing cyber talent management categories. Recommendations for talent management should be tailored to each category.

Military services today organize, train, and equip their respective cyber career fields. US Cyber Command is tasked with executing cyber operations.[6] Each service has occupational specialty codes for cyber operation career fields. When considering relevant cyber talent management, there are four general categories of focus for cyber talent in the military services:

1. *Information Technology Operations*. Corporate enterprises rely on information technology (IT) and communication networks. The Department of Defense Information Network (DODIN) is the world’s largest enterprise data network, connecting all aspects of the DoD over cyber transport systems. The Defense Information Systems Agency is responsible for maintaining the DODIN. These tasks include the design, implementation, and upkeep of communications and information networks and infrastructure. These are traditional IT services that have the highest overlap with civilian equivalents.
2. *Defense*. Defending the DODIN requires teams that monitor, hunt, assess, and analyze adversary activity on or against the DODIN. This is known as defensive cyber operations (DCO) and is traditionally seen in the civilian sector as blue team, threat intel, and cybersecurity analysts.
3. *Offense*. Utilizing cyber capabilities to disrupt, degrade, or deny adversaries is known as offensive cyber operations (OCO).[7] Legally, offensive operations are not allowed by civilians. However, the skill sets required to conduct offensive operations share similarities with proactive cybersecurity services, such as penetration testing and red teaming, where companies hire security teams to simulate cyberattacks and find vulnerabilities.
4. *Development*. The tools utilized for IT, DCO, and OCO are acquired from civilian companies and defense contractors or are developed organically by government and military members. This organic cyber capability development (CCD), which is similar to the

> development work of senior software engineers and exploitation and vulnerability analysts in the commercial sector, is critical to providing the adaptability required to meet the challenges inherent in cyberspace. The pace of daily operations requires new and updated capabilities, which must keep pace with commercial patching—and move much faster than government contracting. The DoD is adopting modern coding practices and improving delivery speeds via software factories. Like manufacturing factories, software factories are assembly plants for development and integration, which contain multiple pipelines equipped with tools, process workflows, scripts, and environments, to produce software deployable artifacts with minimal human intervention.[8]

Table 12.1 compares each service's relevant career field and cyber skill category. Regardless of the service title for the roles, these cyber functional areas

Table 12.1. Summary of US Military Cyber Career Categories

Service	Officer Career Fields
Army*	17A Cyber Warfare (DCO / OCO) 170D Cyber Tool Developer (CCD) 25A Signals (IT)
Navy[†]	1800 Cryptologic Warfare (DCO / OCO)[‡] 1820 Information Professional (IT) 1840 Cyber Warfare Engineer (CCD)
Marines[§]	0602 Communications (IT) 1702 Cyberspace Warfare (DCO / OCO) 1705 Cyberspace Warfare Development (CCD)
Air Force & Space Force[‖]	17D Warfighter Communications Operations (IT) 17S Cyber Effects Operations (DCO / OCO / CCD)

*See US Department of the Army, "CY Branch DA PAM 600-3," January 17, 2018.

[†] See US Department of the Navy, "Special Duty Officer—Cyber Warfare Engineer Information Sheet," US Naval Academy, February 2020.

[‡] See House Committee on Armed Services Bill, James M. Inhofe National Defense Authorization Act for Fiscal Year 2023. H.R. 7776 (2022).

[§] See US Department of the Navy, "Update to FY22 MOS Manual for the 17XX Occupational Field," US Marine Corps, MARADMINS 399/21, August 2021.

[‖] See US Department of the Air Force, "Air Force Officer Classification Directory," Air Force Personnel Command, October 31, 2021.

have the same general job descriptions for both military and civilian industries. The 2023 National Defense Authorization Act (NDAA), Section 1533 A.2.N, directs the study of "Whether the Department of Defense should create a separate service to perform the functions and missions currently performed by Cyber Mission Force units generated by multiple military services."[9]

Given the identical core technologies that underpin the cyber domain, nearly all work roles and missions can be filled and executed by civilians.[10] An additional RAND study went so far as to state: "There are tens of thousands of 'citizen soldiers' . . . who have the potential to support the Army's cyber mission needs or the propensity to learn cyber skills."[11] So why do we need military cyber talent?

Figure 12.1 displays the United States Cyber Command (USCYBERCOM) Force concept. On the right, routine (IT) uses for business operations are depicted in blue. In red, at the opposite end of the spectrum, are offensive (OCO) operations, with defensive (DCO) operations between them. The aspect of building the tools necessary to support the entire range is known as capability development (CCD). The offensive use case for cyber operations is unique to the military, while IT and defensive use cases are the same in the

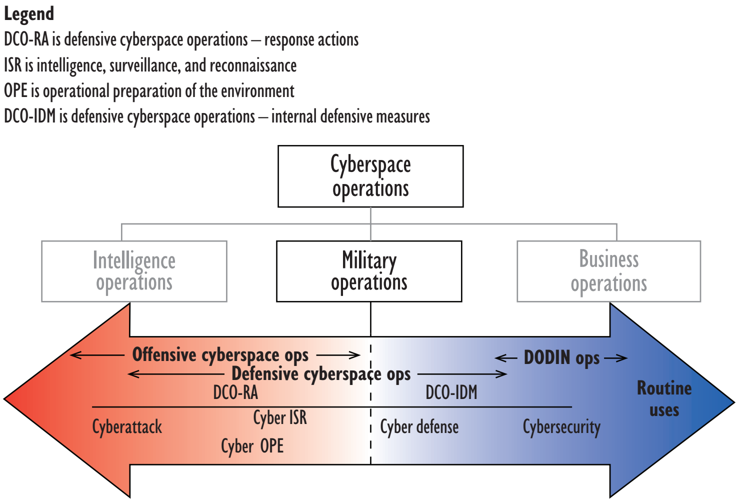
Legend
DCO-RA is defensive cyberspace operations – response actions
ISR is intelligence, surveillance, and reconnaissance
OPE is operational preparation of the environment
DCO-IDM is defensive cyberspace operations – internal defensive measures
Cyberspace operations
Intelligence operations
Military operations
Business operations
Offensive cyberspace ops
Defensive cyberspace ops
DCO-RA
DCO-IDM
DODIN ops
Routine uses
Cyberattack
Cyber ISR
Cyber OPE
Cyber defense
Cybersecurity

Figure 12.1 Cyber Force Concept

Source: Redrawn from Department of Defense Office of Inspector General, "DODIG-2016-026: (U) Combat Mission Teams and Cyber Protection Teams Lacked Adequate Capabilities and Facilities to Perform Missions (Redacted)," FOIA document, November 24, 2015, 33.

civilian sector. Therefore, when it comes to cyber talent retention, the military should focus its efforts on OCO and CCD in support of OCO.

Recruiting and retaining high-quality technical talent is not a new problem. Silicon Valley and large tech companies like Meta (Facebook), Microsoft, Amazon, Apple, and Google have dealt with technical talent management for three decades.[12] A common theme among large tech companies and successful start-ups is identifying and retaining employees who provide outsize returns. In his book *Game Changer: How to Be 10x in the Talent Economy*, serial entrepreneur Michael Solomon studied the highest-impact employees and coined the term "10x talent" to describe those who produced outsize returns to their organizations compared to the average worker.[13] Solomon's examination of high-performing and high-return technical talent identified three standard cultural norms. First, high performers enjoy solving complex problems. Second, they enjoy learning new skills while improving and mastering their current skills. Third, high performers appreciate feedback and results. They want to know that their work has had an impact, whether delivering revenue, executing on a mission, or providing personal fulfillment.[14]

Military cyber problem sets are challenging, require training and continuous improvement, and have outsize mission impacts. Moreover, the civilian sector cannot engage in offensive operations legally.[15] Therefore, individuals who find fulfillment and excitement in offensive and national defense missions will naturally gravitate toward a career in military cyber operations. The challenge, however, has been in how the department approaches managing, incentivizing, and retaining technical talent.[16] A RAND study focused on US Air Force cyber officer retention identified the desire to remain in technical roles for longer durations and frequencies throughout the officers' careers.[17] Assignments to nontechnical positions or away from the cyber mission led many midlevel technical officers to separate.

Cyber talent that separates does not have to wait long to find a job. Given the skill set overlap with the civilian sector, military cyber talent can find significantly higher salaries and equivalent or better benefits in the civilian sector. The civilian sector recruits and retains sought-after talent through competitive salaries. Jobs that require creativity, solving complex problems, and dealing with ambiguity tend to be higher paying than jobs that require adherence to checklists.[18] To the maximum extent possible, successful technology companies find ways to automate simple and repetitive tasks while freeing up talent to focus on hard-to-solve complex problems.[19]

The army has succeeded in early efforts to utilize Assignment Incentive Pay and the Selective Retention Bonus to compensate highly skilled cyber soldiers.[20] In addition, the 2016 NDAA established the Cyber Excepted Service (CES) program for Defense Department civilians. The CES system provides various tools to compensate civilian members based on technical skills and capabilities, allowing the department to be competitive with civilian compensation.[21] However, the focus of the CES program is only to enable flexibility within the current government service pay and promotion system. The maximum annual compensation for any member of the CES program is limited to $176,300.[22] By comparison, senior engineers at companies like Google, Facebook, Microsoft, and Apple earn $225,000 to $350,000 in total annual cash compensation.[23] Including stock options, senior engineers can earn $650,000 a year or more in total compensation.

Prioritizing high-quality talent who focus on the cutting edge of military cyber operations will require an appreciation for the work environment and values these individuals seek. Additionally, to remain competitive with the civilian sector, the military must ensure that top-tier talent continuously have compelling and challenging problems to solve, a growth path that incentivizes technological development, and pay and benefits commensurate with their skills.

Acquisition and Budgeting for Cyber Relevance

Speed is everything in cyber operations. To keep the best technical talent engaged, incentivized, and armed with the tools for success, acquisition and budgeting processes must evolve. With cyber operations, the operator is truly the defining factor. Whether an airman in an aircraft, a soldier in a tank, or a sailor on a ship, the expertise, training, and decision making of the individual matter as much as the platform they utilize. In cyber, the same is true. However, the platform can and will change based on the adversary, the timing, and the technologies involved.[24]

A recent congressional blue-ribbon panel, Section 809, identified that the Department of Defense acquisition process needs to evolve from “an outdated, industrial-era bureaucracy to a more streamlined, agile system able to evolve in sync with the speed of technology innovation.”[25] With a focus on hardware, industrial-era weapons, and large-scale systems over individuals, the current acquisition and budgeting process cannot react to cutting-edge cyber technology evolution.

In addition to a systems-level approach, acquisitions lack clarity in the cyber operations domain.[26] With the traditional domains of war, success metrics were easier to visualize, understand, and implement. When it comes to cyber development, however, there can be ambiguity in what is needed to solve a pressing problem. The modern, agile approach to software and cyber problems requires the iterative flexibility to fail and learn fast.[27] Iterative problem solving requires comfort with a continuum of risk versus black-or-white metrics. Traditional acquisitions are de-risked through an exhaustive and time-consuming requirement-gathering and validation process to minimize the chance of program failure. This distorted focus on a perfect acquisition process over operational speed is a crucial concern for cyber operators.[28]

A study on navy cyber acquisitions recommended that acquisition governance for cyber be done at the lowest levels possible with appropriate accountability mechanisms.[29] Doing so allows for rapid integration and iteration in an agile manner. Agility and speed in the acquisition process for cyber-related systems and operations are just the starting point. There must also be a culture of risk-adjusted decision making that allows for failing fast while increasing the chances of success. One of the Air Force's best-known test pilots, General Chuck Yeager, said it best: "You don't concentrate on risks. You concentrate on results."[30]

Acquisitions and budgeting fall into two key categories for cyber: personnel and systems. Regarding personnel, there needs to be flexibility in payment and benefits tied to appropriate skills. Additionally, an investment must be made in continued technical educational growth and the retention of expertise through a thoughtful blend of active, reserve, and civilian force management. At the same time, systems acquisitions must adopt a fail-fast mentality where experimentation is part of the calculus, and fear is for lack of speed and innovation versus not attaining the perfect metrics.[31]

Recommendations

Empower Military Manpower Management at the Unit Level

Today, commanders are extremely limited in authority and time when hiring personnel. Except for highly classified (i.e., "green door") or specially coded units, air force squadrons receive the manpower assigned to them via the Air Force Personnel Center (AFPC). Commanders can advertise open, major command-approved positions through a "talent marketplace" web application for most officer career fields and a few enlisted fields. Subsequently, military members slated to move to a new assignment can review open positions and place bids for the positions that interest them. This is a great start to increasing transparency and awareness, but ultimately the decision is left to AFPC—meaning there are instances where a commander and applicant can confirm a perfect match, and AFPC can (and does) overrule.

Unfortunately, hiring is not much easier or faster on the civilian side. On average, a new hire already working in the government should expect to wait two to four months after being selected to begin a position. That time balloons for hires outside of government—often taking well over a year. Furthermore, because commanders are not the final authority, it is not uncommon for an individual to have satisfactorily completed a technical interview by a board of their peers only to be informed much later by headquarters that they are, in fact, not qualified for a position.

Removing individuals provides similar challenges and outcomes—requiring commanders and leadership teams to devote a significant amount of time and energy to rehabilitate underperforming or toxic individuals before being allowed to remove them.

Improve Compensation

Although other services have already transitioned many of their civilian cyber billets to the DoD's CES, the air force is woefully behind. CES is an enterprise-wide approach for managing civilian cyber professionals across the department. The CES is aligned with Title 10 and Title 5 provisions, offering flexibilities for recruiting, retaining, and developing cyber professionals across departments. In addition to receiving increased pay, thanks to the targeted local market supplement, civilian employees can also be promoted based on qualification instead of time—encouraging employees to continue improving. However, until the compensation cap is removed, the most promising senior talent will always have enticing options in the civilian sector.

Congress authorized temporary promotions for military officers in Section 503 of the FY2019 NDAA to account for those who "have a skill in which the armed force concerned has a critical shortage of personnel (as determined by the secretary of the military department concerned)." The army is the only service to have leveraged this authority, yet even it only used a fraction of the nearly eight hundred authorized. This authority could be better leveraged to ensure the right folks are eligible for the right positions, regardless of rank—and tied to time in service.

However, more than pay and rank, what typically brings people to work for the government is the mission and purpose—and this is certainly true in cyberspace. Controlled tours and assignments that do not have a time limit are important for military members working in cyber because they allow for a structured and organized approach to the growth and development of technical expertise. This is particularly important in the field of cybersecurity, where the nature of the work can be complex and constantly evolving. By implementing controlled tours, military leaders can ensure that personnel are appropriately educated, have time and experience in threat-representative environments, and are ultimately prepared for operations. Additionally, controlled tours allow for more stability and effective resource management, as personnel can be scheduled and tasked in a way that maximizes their impact and minimizes disruptions to ongoing operations. Overall, controlled tours help ensure the safety and success of military members working in cyber jobs and are vital to effective military operations in the digital age.

Invest in and Empower Continuity of Expertise

The cyber domain is constantly evolving and advancing, and the military needs to keep pace with our adversaries to counter cyber threats effectively. By investing in and empowering continuity of expertise, the military can ensure it has a knowledgeable and skilled workforce that can adapt to new technologies and tactics.

For our active-duty military, this is only possible by defining, building, and investing in a technical track. To remain relevant in cyber, the military requires a strong foundation of technical knowledge and experience, which is crucial for the long-term success of cyber operations. By investing in training and development programs and committing to growing and promoting technical talent, the military can cultivate a competent and capable cyber workforce able to meet the challenges of the future.

There are few work roles in cyber today that only military members can fill. This fact provides an opportunity to consider more holistic courses of action regarding structuring and blending operations squadron manning—especially when taking into account the additional compensation tools available for the civilian workforce.

Finally, cyber is the ideal domain to fully exploit the resources available through the reserve total force initiative. Cyber operations require diverse skills, including information technology, communication, and intelligence, making it easy to integrate and utilize the expertise of National Guard and reserve members already working in these fields in their civilian lives. Operations are often conducted by small, highly skilled teams, allowing members with specialized cyber skills to significantly contribute to operations.

From nearly every angle, the military is trailing industry in cyber expertise. It should consider new, improved, and innovative ways to maximize its experience.

Invert Acquisition Calculus

It is possible that the fastest and most effective way for the military to recruit and retain incredible cyber talent is to change how it is structured and what it values. The military could start by automating and contracting out basic functions and tasks. This would help improve efficiency and reduce costs. Automation allows for the performance of repetitive tasks with a high degree of accuracy and speed—eliminating the need for a highly qualified and motivated force to complete them. Additionally, automating and contracting basic functions and roles can help to free up resources and allow the military's cyber experts to focus on more complex and value-added tasks. By outsourcing certain functions, the military can focus its time, money, and personnel on activities more directly aligned with its mission and goals. Overall, automating and contracting basic functions and roles would allow the military to operate more efficiently and effectively and better achieve its strategic objectives.

With the easy stuff automated, the military can focus on recruiting, hiring, and retaining the highest-quality ("10x talent") military and civilian force to focus on the most wicked problems. An added benefit of this approach is that a workforce with an increased talent density often requires less personnel overall. A decrease in the size of the force, so long as the talent density remains high, would ensure plenty of worthy work to keep the workforce challenged and feeling valued.

The last step is removing distractions or barriers to accountability, and modifying how the military is organized is a big part of that. Acquisitions and operations are two critical functions to the success of the military. Unfortunately, these two functions are deliberately siloed and operate independently, leading to inefficiencies and conflicts. Today, the military often chooses not to execute cyber operations at all rather than risk a mistake in acquisitions or contracting. To overcome these challenges and maximize the effectiveness of these functions, it is essential that acquisitions and operations work for the same operational commander.

One of the main benefits of having acquisitions and operations in the same chain of command is that it helps to align these two functions around a common set of goals and mission objectives. When acquisitions and operations work toward the same outcomes, it is easier for them to coordinate their efforts and collaborate to achieve their objectives. This helps to eliminate unnecessary duplication of effort and ensures that resources are used in the most effective way possible. And when things do go wrong, the team can quickly and effectively conduct a root-cause analysis to determine the issue and immediately implement a fix.

With acquisitions and operations under the same commander, the organization can begin fostering a culture of accountability and transparency. With these two functions combined, managers can more easily drive performance and ensure they meet operational needs. Additionally, having a single point of contact for acquisitions and operations makes it easier for combatant commanders to seek guidance and support when needed, which can help to improve operational outcomes while improving morale and fostering a sense of teamwork and collaboration within the organization. By aligning these functions around common operational goals and objectives, fostering a culture of accountability, and improving communication and collaboration, organizations can respond more quickly to better serve the needs of their stakeholders.

Notes

1. The White House, "Fact Sheet: Imposing Costs for Harmful Foreign Activities by the Russian Government," April 15, 2021.

2. US Department of Justice, "Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, including Infectious Disease Research," Office of Public Affairs, July 19, 2021.

3. US Cyberspace Solarium Commission, Report, March 2020, https://www.solarium.gov/report.

4. The White House, "Requests Your Insight and Expertise on Cyber Workforce, Training, and Education," Office of the National Cyber Director, October 3, 2022.

5. Catherine A. Theohary, "Defense Primer: Cyberspace Operations," Congressional Research Service Report IF10537, updated December 9, 2022; Chaitra M. Hardison, Leslie Adrienne Payne, John A. Hamm, Angela Clague, Jacqueline Torres, David Schulker, and John S. Crown, "Attracting, Recruiting, and Retaining Successful Cyberspace Operations Officers," RAND Corporation, 2019; Department of Defense Office of Inspector General, "DODIG-2016-026: (U) Combat Mission Teams and Cyber Protection Teams Lacked Adequate Capabilities and Facilities to Perform Missions (Redacted)," FOIA document, November 24, 2015.

6. Theohary, "Defense Primer."

7. Theohary, "Defense Primer."

8. US Department of Defense (DoD), "Memorandum: Department of Defense Software Modernization," Office of the Deputy Secretary, February 2, 2022.

9. James M. Inhofe National Defense Authorization Act for Fiscal Year 2023. H.R. 7776, 117th Congress (2022).

10. Albert A. Robbert, James H. Bigelow, John E. Boon Jr., Lisa M. Harrington, Michael McGee, Craig Moore, Daniel M. Norton, and William W. Taylor, "Suitability of Missions for the Air Force Reserve Components," RAND Corporation, 2014.

11. Jennie W. Wenger, Caolionn O'Connell, and Maria C. Lytell, "Retaining the Army's Cyber Expertise," RAND Corporation, 2017.

12. Marcel Schwantes, "What Smart Companies Like Facebook and Amazon Are Doing to Attract, Retain, and Manage Top Talent," *Inc.*, October 9, 2020.

13. Michael Solomon, Rishon Blumberg, and Daniel Weizmann, *Game Changer: How to Be 10x in the Talent Economy* (New York: HarperCollins Leadership, 2020).

14. Solomon, Blumberg, and Weizmann, *Game Changer*.

15. Catherine A. Theohary and Anne I. Harrington, "Cyber Operations in DOD Policy and Plans: Issues for Congress," Congressional Research Service Report R43848, January 5, 2015.

16. Hardison et al., "Attracting, Recruiting, and Retaining."

17. Hardison et al., "Attracting, Recruiting, and Retaining."

18. "Cybersecurity Supply/Demand Heat Map," *Cyber Seek* (accessed December 20, 2022).

19. Michael Chui, James Manyika, and Mehdi Miremadi, "Four Fundamentals of Workplace Automation," *McKinsey Quarterly* 29, no. 3 (November 2015): 1–9.

20. Wenger, O'Connell, and Lytell, "Retaining the Army's Cyber Expertise."

21. DoD, "Cyber Excepted Service: Frequently Asked Questions," *DoD Cyber Exchange*, Defense Civilian Personnel Advisory Service, January 2018, https://dl.dod.cyber.mil/wp-content/uploads/dces/pdf/GeneralCESFAQs.pdf.

22. DoD, "2022 Department of Defense Cyber Excepted Service Pay Rates," *DoD Cyber Exchange*, Defense Civilian Personnel Advisory Service, March 2022, https://dl.dod.cyber.mil/wp-content/uploads/dces/pdf/2022_CES_Pay_Rates.pdf.

23. "Big Tech Salaries Revealed: How Much Engineers, Developers, and Product Managers Make at Companies including Apple, Amazon, Facebook, Google, Microsoft, Intel, Uber, IBM, and Salesforce," *Business Insider*, April 28, 2022.

24. Vasu Jakkal, "Cybersecurity Threats Are Always Changing—Staying on Top of Them Is Vital, Getting Ahead of Them Is Paramount," *Microsoft Security Blog*, February 9, 2022.

25. US Congress Section 809 Panel, *Report of the Advisory Panel on Streamlining and Codifying Acquisition Regulations, Volume 3 of 3*, January 2019.

26. US Government Accountability Office, "Defense Acquisitions: Cyber Command Needs to Develop Metrics to Assess Warfighting Capabilities," GAO-22-104695, March 2022.

27. Bryan Casey, "Failing Fast, Traditional Strategy, and How They Work Together," *IBM Cloud*, October 4, 2019.

28. Thomas Klemas, Rebecca K. Lively, and Nazli Choucri, “Cyber Acquisition: Policy Changes to Drive Innovation in Response to Accelerating Threats in Cyberspace,” *Cyber Defense Review* Special Edition: International Conference on Cyber Conflict (CYCON US) (2019): 103–20.

29. Isaac R. Porche III, Shawn McKay, Megan McKernan, Robert W. Button, Bob Murphy, Katheryn Giglio, and Elliot Axelband, “Rapid Acquisition and Fielding for Information Assurance and Cyber Security in the Navy,” RAND Corporation, 2012.

30. Tim Stelloh and The Associated Press, “Chuck Yeager, Air Force Officer Who Broke Speed of Sound, Dies at 97,” *NBC News*, December 7, 2020.

31. Charles W. Mahoney, “Corporate Hackers: Outsourcing US Cyber Capabilities,” *Strategic Studies Quarterly* 15, no. 1 (Spring 2021): 61–89.