



WHAT IS A CYBER WARRIOR? THE EMERGENCE OF U.S. MILITARY CYBER EXPERTISE, 1967–2018

Rebecca Slayton



How have military cyber operations, a diverse set of activities that often differ little from civilian cyber security work, achieved the status of "warfighting"? What activities have the greatest warfighting status, what activities have the least, and why? This paper examines the establishment and growth of expertise associated with cyber operations in the individual services and at the joint level since the late 1960s. Threat-oriented activities, such as attacking adversaries or responding to adversaries that have breached U.S. networks, have more readily achieved warfighting status than have vulnerability-oriented activities, such as patching software, training users in good security practices, and other actions that aim to prevent intrusions. Ultimately, the lower status of work and expertise associated with vulnerability mitigation remains a significant problem for military cyber operations.

On May 4, 2018, U.S. Cyber Command was elevated from a sub-unified command under U.S. Strategic Command, making it America's 10th unified combatant command. At a ceremony marking this change, Deputy Secretary of Defense Patrick Shanahan described the command's challenge as strengthening "our arsenal of cyber weapons, cyber shields and cyber warriors."

Shanahan's words evoke the image of a traditional warrior, fighting with weapons and a shield. And yet, cyber "warfare" differs dramatically from traditional combat.² In fact, many cyber warriors spend less time using virtual "weapons" than they do inventing or maintaining them. While joint doctrine treats use, invention, and maintenance as important components of cyber "operations," i.e.,

warfighting, this paper shows that, in practice, the individuals who perform these activities do not all have equal "warrior" status.

Of course, it may seem strange that *any* cyber experts would have warrior status. After all, they typically work at desks, and without substantial physical risk. Furthermore, while missiles, drones, combat aircraft, and other high technology have all changed how militaries fight and what it means to be a warrior, the technologies with which cyber warriors work are not unique to the military.³ Every major civilian organization today also relies on complex computer networks and experts who defend them. While some cyber warriors attack adversary computer networks, many spend their time focused on defensive work that differs very little, if at all, from that of civilian computer security

1 Jim Garamone, "Cybercom Now a Combatant Command, Nakasone Replaces Rogers," *DOD News*, May 4, 2018, <https://www.defense.gov/Explore/News/Article/Article/1512994/cybercom-now-a-combatant-command-nakasone-replaces-rogers/>.

2 I am using terms such as "cyber warfare" and "cyber warrior" colloquially. I do not mean to imply that what they do qualifies as "war" as war is understood in international law. The term "cyber warrior" has been used broadly to refer to a wide range of career specializations within the military.

3 For discussion of the warfighting identity of missileers, see George L. Chapman, "Missile: The Dawn, Decline, and Reinvigoration of America's Intercontinental Ballistic Missile Operators," Master's Thesis, Air University, 2017, <https://apps.dtic.mil/dtic/tr/fulltext/u2/1045804.pdf>. On drones and warfighting, see P. W. Singer, *Wired for War: The Robotics Revolution and Conflict in the 21st Century* (New York: Penguin Press, 2009) and Hugh Gusterson, *Drone: Remote Control Warfare* (Cambridge, MA: MIT Press, 2016). Air Force pilots continue to be the butt of jokes implying that they are not tough enough, as compared to marines. For example, see Mark Thompson, "Petraeus Zinger Wounds Air Force Egos," *Time*, Aug. 21 2009, <http://content.time.com/time/nation/article/0,8599,1917841,00.html>.

experts. Indeed, the U.S. Defense Department has leveraged the civilian U.S. National Initiative on Cybersecurity Education workforce framework to build its own cyber workforce.⁴ For that matter, the Department of Defense uses civilian contractors for both offensive and defensive cyber operations.

So, why are some kinds of cyber experts who work for the Defense Department considered “warfighters” but others are not? This paper examines the historical process by which some of these kinds of experts gained warfighter status while others did not. It shows how, throughout the 1990s and early 2000s, key leaders in intelligence, communications, and warfighting communities made the case that computer network operations should be treated as a kind of warfighting. While specific approaches varied across different services and professional specializations, all of these leaders struggled against a culture that has historically treated information-related work such as intelligence, computing, and communications as a warfighting *support* function, something lower in status than warfighting itself.

Elevating the status of cyber expertise entailed challenging organizational hierarchies that made cyber experts subordinate to traditional warfighters. For example, it meant empowering cyber experts and organizations to effectively issue commands to warfighting units, directing them to remediate vulnerabilities in their computer networks. It also involved reorganizing well-established military specializations, such as signals intelligence, electronic warfare, and communications, around cyber infrastructure and operations. Perhaps most importantly, it meant establishing new career paths through which cyber experts might advance to the highest levels of command.

Military leaders made their case for elevating cyber expertise in a variety of ways. For example, they developed concepts of cyber operations that were analogous to well-established concepts of kinetic operations. They also conducted exercises that revealed the potential impact of cyber operations on military warfighting and gathered data that highlighted a steady increase in intrusions that might have gone completely unnoticed if not for the work of cyber experts.

I argue that these and related activities succeeded in establishing cyber operations as a type of warfighting, but that some kinds of skills, knowl-

edge, and ability were more readily seen as warfighting than others. In particular, threat-focused activities like offensive operations, intrusion detection, and incident response, which were first developed within signals intelligence units, were most easily viewed as warfighting. By contrast, vulnerability-focused activities such as password management, software patching, and other forms of technology maintenance, which were primarily the responsibility of communications units, were slow to be seen as a kind of warfighting.

Today, the distinction between threat-focused and vulnerability-focused activities can be found in joint doctrine, which outlines three primary missions for cyberspace operations. The first mission, offensive cyber operations, is unique to the military. U.S. law prohibits civilian organizations from conducting offensive cyber operations unless they are operating under military authority. The second mission, defensive cyber operations, responds to threats that have already breached Defense Department networks. Some of these activities, including incident response, intrusion detection, and network monitoring, are very similar to defensive work within major corporations, civilian government, and other non-military organizations.

The third mission, Department of Defense Information Network (DODIN) operations, focuses on mitigating vulnerabilities. It includes “actions taken to secure, configure, operate, extend, maintain, and sustain [Defense Department] cyberspace and to create and preserve the confidentiality, availability, and integrity of the DODIN.” Like defensive cyber operations, these activities are commonplace in non-military organizations. Furthermore, by virtue of their focus on mitigating vulnerabilities rather than attacking adversaries, they have struggled to gain the status of warfighting. In an effort to cast its work as warfighting, Joint Force Headquarters-DODIN describes its mission with the phrase “Fight the DODIN,” not “secure,” “maintain,” or “sustain” the DODIN.⁵ And joint doctrine seems to recognize the lower regard in which such operations might be held, noting that “although many DODIN operations activities are regularly scheduled events, they cannot be considered routine, since their aggregate effect establishes the framework on which most DOD [Department of Defense] missions ulti-

4 William Newhouse et al., *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*, National Institute of Standards and Technology, Publication 800-181, August 2017, <https://doi.org/10.6028/NIST.SP.800-181>. The framework consists of seven broad functions, 33 areas of work, and 52 work roles. Each of the work roles consists of specific tasks and requires specialized knowledge, skills, and abilities. Altogether, the framework lists 1,007 tasks, 630 kinds of knowledge, 374 kinds of skills, and 176 abilities.

5 Jeffrey R. Jones, “Defense Department Cyber Requires Speed, Precision and Agility,” *Signal*, May 1, 2019, <https://www.afcea.org/content/defense-department-cyber-requires-speed-precision-and-agility>.

mately depend.”⁶

Joint doctrine does not formally prioritize any one of these three missions over the others. Yet, as this paper shows, the personnel assigned to offensive or defensive cyber operations tend to have greater warfighting status, and thus greater prestige and opportunities, than do personnel assigned to DODIN operations. Offensive and defensive cyber operations, by virtue of their focus on confronting intelligent and changeable adversaries, tend to be less routine than DODIN operations and are therefore more readily construed as warfighting. By contrast, DODIN operations are focused on maintaining and sustaining technology. Such work can be carried out in innovative ways. However, it is also very often routine and mundane. Furthermore, although effective DODIN operations require an understanding of how threats operate, their focus is ultimately on infrastructure rather than adversaries, further reducing any claim to warfighting.

The history of military cyber operations is thus not just about innovation, but also about the importance of mundane maintenance work, such as training users, patching software, and strengthening passwords.

And yet, DODIN operations are also the first line of defense, without which defensive cyber operations would become impossible. Without a defense of computer networks, the modern military simply

could not function with any level of confidence. While I do not take a position on whether DODIN operations and other forms of security maintenance should be considered “warfighting,” I do argue that such work has tended to be undervalued and that its lower status continues to impact military cybersecurity.

By analyzing historical efforts to make computer network attack and defense a kind of warfighting, this paper builds upon and extends existing histories of cyber operations. The earliest books and papers to describe the rise of military cyber operations treated them as the necessary response to a series of “wake-up calls” that came in the form of computer network intrusions, by both real adversaries and penetration testers, in the 1990s and 2000s.⁷ This narrative first emerged in the 1990s among Defense Department insiders who advocated putting greater emphasis on cyber operations.⁸ More recently, scholars have analyzed the rise of military cyber operations as a response to a broad set of technological changes that took place in the 1990s and early 2000s.⁹ In the most thorough account to date, Sarah White argues that the unique cultures and professional subcultures of the military services — including intelligence, signals intelligence, cryptology, communications, and electronic warfare — led to considerable variation in their cyber doctrines.¹⁰ White describes a two-stage process of innovation, wherein the services experimented with many different forms of cyber doctrine in the 1990s, but these doctrines became more similar after cyber operations became a major activity at the joint level.

This paper draws on the work of White and others, but its theoretical assumptions and contributions differ in three significant ways. First, I focus not only on innovation, but on what comes after innovation: maintenance and repair.¹¹ To be

6 “Joint Publication 3-12: Cyberspace Operations,” Joint Chiefs of Staff, June 8, 2018, II-2–II-3. The definition does exclude “actions taken under statutory authority of a chief information officer (CIO) to provision cyberspace for operations, including IT architecture development; establishing standards; or designing, building, or otherwise operationalizing DODIN IT for use by a commander.” See page II-2.

7 Jason Healey, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, Kindle ed. (Vienna, VA: Cyber Conflict Studies Association, 2013) and Gregory J. Rattray, *Strategic Warfare in Cyberspace* (Cambridge, MA: MIT Press, 2001).

8 See, for example, “Security in Cyberspace,” Hearings Before the Committee on Governmental Affairs, U.S. Senate, 104th Congress, 2nd Session, 1996 and “Department of Defense Authorization for Appropriations for Fiscal Year 2001 and the Future Years Defense Program, Part 5: Emerging Threats and Capabilities,” Senate Armed Services Committee, 106th Congress, 2nd Session, 2000.

9 Fred Kaplan, *Dark Territory: The Secret History of Cyberwar* (New York: Simon & Schuster, 2016); Thomas Rid, *Rise of the Machines: A Cybernetic History* (New York: W.W. Norton & Company, 2016); Myriam Dunn Cavelty, *Cyber-security and Threat Politics: US Efforts to Secure the Information Age* (New York: Routledge, 2007); Michael Warner, “Cybersecurity: A Pre-history,” *Intelligence and National Security* 27, no. 5 (2012), <https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1136012/notes-on-military-doctrine-for-cyberspace-operations-in-the-united-states-1992/>; and “Notes on Military Doctrine for Cyberspace Operations in the United States, 1992–2014,” updated Aug. 27, 2015.

10 Sarah P. White, “Subcultural Influence on Military Innovation: The Development of U.S. Military Cyber Doctrine,” Harvard University, 2019, <http://nrs.harvard.edu/urn-3:HUL.InstRepos:42013038>. White defines doctrine broadly to include “personnel management processes, organizational reform, and conceptual development.” See page 5.

11 David Edgerton, *The Shock of the Old: Technology and Global History Since 1900* (London: Profile Books, 2007); Andrew L. Russell and Lee Vinsel, “After Innovation, Turn to Maintenance,” *Technology and Culture* 59, no. 1 (January 2018): 1–25, <https://doi.org/10.1353/tech.2018.0004>; and Rebecca Slayton and Brian Clarke, “Trusting Infrastructure: The Emergence of Computer Security Incident Response, 1989–2005,” *Technology and Culture* 61, no. 1 (January 2020): 173–206, <https://doi.org/10.1353/tech.2020.0036>.

sure, this is partly a story of innovation, as the establishment of military cyber capabilities entailed transforming the relationships between many distinctive professional communities and the computer networks that they continually created, operated, and maintained. These innovations were simultaneously organizational and technological — that is, they were sociotechnical. But, contrary to a substantial body of scholarship on the sources of military innovation, I argue that innovation is not always an unmitigated good.¹² As discussed further below, as the Defense Department incorporated innovations in microcomputers and networking into its information systems in the 1980s, its vulnerability to computer network attack grew substantially.¹³ This vulnerability dramatically increased the need for new kinds of sociotechnical repair and maintenance that constitute the majority of cyber operations today. The history of military cyber operations is thus not just about innovation, but also about the importance of mundane maintenance work, such as training users, patching software, and strengthening passwords.

Second, whereas most historical accounts treat the rise of military cyber operations as a response to technological changes that were taking place external to the military, I examine these technological changes as internal to the military. The U.S. military did not simply respond to the rise of

computer networking. It also actively drove the development of new technological capabilities as it pursued various functional advantages, such as increased efficiency in logistics systems or operational advantages in network-centric warfighting.¹⁴ The vulnerabilities associated with military computer networking were not simply a product of flawed commercial technology. They were also produced by practices internal to the Department of Defense. These include the decentralized pursuit of new networking technologies, a lack of strong security standards, and a lack of security training and a security culture among the communications and computing personnel charged with deploying computer systems.¹⁵

Third, I analyze cyber expertise as more than a set of knowledge, skills, and abilities that people and organizations possess. Rather, I draw on work that examines expertise as a set of dynamic relationships between people or groups claiming to possess specialized knowledge and skills and people or groups lacking such knowledge and skills.¹⁶ Experts must do more than simply possess knowledge, skills, and abilities. They must also persuade others of the veracity of their claims and the effectiveness of their actions.¹⁷ This process of persuasion may include, for example, gaining professional certification, demonstrating mastery over technologies, and other cultural practices that establish

12 The literature on military innovation is vast. Some key works include the following: Barry R. Posen, *The Sources of Military Doctrine: France, Britain, and Germany Between the World Wars* (Ithaca, NY: Cornell University Press, 1984); Stephen Peter Rosen, *Winning the Next War: Innovation and the Modern Military* (Ithaca, NY: Cornell University Press, 1991); Kimberly Martin Zisk, *Engaging the Enemy: Organization Theory and Soviet Military Innovation, 1955–1991* (Princeton, NJ: Princeton University Press, 1993); Carl H. Builder, *The Masks of War: American Military Styles in Strategy and Analysis* (Baltimore, MD: Johns Hopkins University Press, 1989); Dima Adamsky, *The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel* (Stanford, CA: Stanford University Press, 2010); Williamson Murray and Allan R. Millett, eds., *Military Innovation in the Interwar Period* (New York: Cambridge University Press, 1998); and Terry C. Pierce, *Warfighting and Disruptive Technologies: Disguising Innovation* (New York: Frank Cass, 2004).

13 For example, the number of Defense Department microcomputers expanded from roughly 500 in 1980 to more than 36,000 in 1985. Terminals to use those computers expanded from roughly 9,000 to nearly 68,000. *Federal Government Information Technology: Management, Security, and Congressional Oversight*, Office of Technology Assessment, 1986. Most of these computers did not have security features built into them. Additionally, the rise of microcomputers and networking expanded the number of users radically and further decentralized control over networks, which itself increased the problems of security management and contributed to vulnerability.

14 The development of the internet through the Defense Advanced Research Projects Agency is the most obvious example of military-driven innovation, but it is by no means an isolated example. The U.S. military's influence on the computer industry waned in the 1980s as other significant market segments emerged, but it remained the largest U.S. government computer consumer.

15 This conclusion has been reiterated in numerous reports on military cybersecurity. See, for example, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat*, Department of Defense Science Board, 2013, 65, <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-081.pdf>; *Department of Defense Cybersecurity Culture and Compliance Initiative*, Department of Defense, (September 2015), 1, <https://dod.defense.gov/Portals/1/Documents/pubs/OSD011517-15-RES-Final.pdf>; and *A Review and Assessment of the Department of Defense Budget, Strategy, Policy, and Programs for Cyber Operations and U.S. Cyber Command for Fiscal Year 2019*, Committee on Armed Services, House of Representatives, 115th Congress, 2nd Session, (2018), 7.

16 See, for example, E. Summerson Carr, "Enactments of Expertise," *Annual Review of Anthropology* 39 (October 2010): 17–32, <https://doi.org/10.1146/annurev.anthro.012809.104948>; Trine Villumsen Berling and Christian Bueger, eds., *Security Expertise: Practice, Power, Responsibility* (New York: Routledge, 2015); Brian Wynne, "Sheep Farming After Chernobyl: A Case Study in Communicating Scientific Information," *Environment Magazine* 31, no. 2 (1989): 10–39, <https://doi.org/10.1080/00139157.1989.9928930>; and Steven Epstein, "The Construction of Lay Expertise: AIDS Activism and the Forging of Credibility in the Reform of Clinical Trials," *Science, Technology, & Human Values* 20, no. 4 (Autumn 1995): 408–37, <http://www.jstor.org/stable/689868>.

17 Stephen Hilgartner, *Science on Stage: Expert Advice as Public Drama* (Stanford, CA: Stanford University Press, 2000); Epstein, "The Construction of Lay Expertise"; Sheila Jasanoff, *Science at the Bar: Law, Science, and Technology in America* (Cambridge, MA: Harvard University Press, 1995); Gwen Ottinger, *Refining Expertise: How Responsible Engineers Subvert Environmental Justice Challenges* (New York: New York University Press, 2013); and Rebecca Slayton, *Arguments that Count: Physics, Computing, and Missile Defense, 1949–2012* (Cambridge, MA: MIT Press, 2013).

trust between experts and non-experts.¹⁸

This relational understanding of expertise is critical to understanding how organizations create and compete with cyber forces. Organizations must do much more than train, recruit, or contract for talented personnel: They must also establish effective relationships between cyber warriors and the many other military professionals with whom they work. A relational conception of expertise is also crucial for explaining how some skilled and knowledgeable individuals and groups are able to raise their status within an organization while others are not. Finally, international competition in cyberspace depends not only on acquiring and organizing skilled personnel, but also on persuading adversaries of the capability of a nation's cyber warriors, that is, on establishing a relationship of superiority.

Expertise provides a unique basis for authority — not the formal authority of command structures or legal statutes, but the authority that comes from being able to effectively persuade. However, what counts as a persuasive argument, and therefore what counts as an authoritative expert, differs from one culture to the next. For example, while Ayurvedic doctors are respected as highly effective throughout much of India, they are likely to be considered quacks in Western cultures. Culture also shapes what counts as relevant and important knowledge and skills and what counts as a persuasive and effective expert.

The U.S. military is by no means a monolithic culture,¹⁹ but its primary mission is warfighting. Expertise generally gains in status the more essential it is to warfighting. All of the services' career fields explicitly distinguish between warfighting and warfighting support. Moreover, traditional warfighting experience has often been a prerequisite for professional promotion. The most senior commanders lead warfighting rather than warfighting support units, and organizational hierarchies empower warfighting commands over warfighting support. In this context, raising the status of cyber expertise entails reframing it as a form of warfighting

rather than warfighting support.

The remainder of this paper is organized in three parts. First, I briefly outline the origins of computer network operations in the Defense Department, highlighting both vulnerability-oriented and threat-oriented approaches. Second, I discuss the rise of "information warfare," which provided a conceptual and organizational context for further developing computer network operations during the 1990s. Third, I discuss the growing challenge of defending networks and the associated rise of joint computer network operations in the mid and late 1990s. Defending military operations from computer network intrusions demanded a level of coordination that no single service could provide. Fourth, I discuss how the services began to elevate computer network operations in the new millennium, partly in response to the growing prominence of joint cyber operations. I conclude with a discussion of current cyber operations, in particular the challenge of raising the status of work focused on mitigating vulnerabilities.

The Origins of U.S. Computer Network Operations

Technological, Organizational, and Professional Vulnerability

The origins of what came to be called computer network operations can be found in U.S. intelligence organizations, which tested the security of several state-of-the-art computer systems in the late 1960s and early 1970s by attempting to break in and take control of them.²⁰ These "tiger teams" were always successful, demonstrating pervasive vulnerabilities in even the best-designed systems.²¹ It is reasonable to assume that intelligence agencies were also exploring ways of compromising adversaries' computer systems, although the existence of any such operations remains highly classified.²²

By contrast, the need for computer network de-

18 Carr, "Enactments of Expertise."

19 Several scholars have argued that the cultures of the individual services shape their development and implementation of doctrine. A few key works include Builder, *The Masks of War*; Jeffrey W. Donnithorne, *Four Guardians: A Principled Agent View of American Civil-Military Relations* (Baltimore, MD: Johns Hopkins University Press, 2019); and White, "Subcultural Influence on Military Innovation."

20 James P. Anderson, *Computer Security Technology Planning Study, Vol 1*, Electronic Systems Division of the Air Force Systems Command, October 1972, <https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/ande72a.pdf>; James P. Anderson, *Computer Security Technology Planning Study, Vol 2*, Electronic Systems Division of the Air Force Systems Command, October 1972, <https://apps.dtic.mil/dtic/tr/fulltext/u2/772806.pdf>.

21 For examples of early tests, see discussion in Jeffrey Yost, "Oral History Interview with Roger R. Schell," Charles Babbage Institute, May 1, 2012, <http://hdl.handle.net/11299/133439> and Warner, "Cybersecurity: A Pre-history," 786.

22 Asked in 2012 whether penetration tests of U.S. systems led to offensive work within the intelligence community, Roger Schell, an Air Force officer who played a leading role in developing more secure computer systems, responded that "we recognize that it would not be unexpected if an adversary were to take an offensive thing, and we didn't consider ourselves stupider than the adversary, you know, you can pretty well connect those dots." Yost, "Oral History Interview with Roger R. Schell."

fense became a subject for public discussion after a panel of computer scientists addressed it at a 1967 conference and, for the first time, publicly acknowledged the existence of the National Security Agency, previously described as “No Such Agency.”²³ For computer scientists, the ease with which computers could be penetrated by outsiders was partly a technological problem: Hardware-software systems were so complex that they inevitably contained errors that could be exploited. With the sponsorship of the National Security Agency and the Air Force, computer scientists worked on developing techniques for reducing such errors and proving that computer systems actually enforced the security policies that they were programmed to enforce. These efforts failed to produce a provably secure computer, but succeeded in growing a community of government, industry, and academic computer security experts.²⁴

This community recognized that security was also a market problem: Companies had no incentive to design secure systems in the 1970s and 1980s because there was little consumer demand for security. Although the 1974 Privacy Act mandated that federal agencies undertake information security measures, and although the U.S. federal government had substantial market power as a major consumer of computing hardware and services, the personnel responsible for buying systems usually lacked the understanding needed to specify the security requirements for new purchases.²⁵ Similarly, computing managers got “mostly ‘arm

waving’ from the vendor,” rather than an objective evaluation of the “secure-worthiness” of computer systems.²⁶ Accordingly, computer scientists convened by the National Bureau of Standards in 1978 proposed to develop “a process for evaluating the security of computer systems, and for accrediting particular systems for particular applications.”²⁷

These recommendations led to the creation of the Trusted Computer System Evaluation Criteria and the associated National Computer Security Center at the National Security Agency.²⁸ The center helped coordinate the development of these criteria and then used them to evaluate the security of commercial computer systems. But rapid innovation and the rise of computer networking threatened to make the criteria obsolete and led to a long series of “interpretations” to guide evaluations of new kinds of products.²⁹ Meanwhile, the slow process and high expense of evaluation deterred many organizations, including those in the Defense Department, from demanding high security ratings.³⁰ That changed somewhat after 1987, when the National Telecommunications and Information Systems Security Committee directed that, by 1992, all federal agencies must use only operating systems evaluated at level “C2” or higher to process national security information.³¹ Evidence suggests that this mandate was indeed successful in improving security standards in the computer market.³²

Nevertheless, C2 was still not a particularly high level of security, and communications and computing personnel did not typically demand more se-

23 For the introductory talk in this session, see Willis H. Ware, “Security and Privacy in Computer Systems,” paper presented at the spring Joint Computer Conference, New York, April 18–20, 1967.

24 For an excellent summary of the research agendas begun to solve this problem, see Donald MacKenzie, *Mechanizing Proof: Computing, Risk, and Trust* (Cambridge, MA: MIT Press, 2001).

25 For more on the Privacy Act and associated requirements, see Rebecca Slayton, “Measuring Risk: Computer Security Metrics, Automation, and Learning,” *IEEE Annals of the History of Computing* 37, no. 2 (April–June 2015): 32–45, <https://doi.org/10.1109/MAHC.2015.30>.

26 Clark Weissman, “Access Controls Working Group Report,” in Susan K. Reed and Dennis K. Branstad, “Controlled Accessibility Workshop Report: A Report of the NBS/ACM Workshop on Controlled Accessibility,” Dec. 10–13, 1972, Santa Fe, CA, 19.

27 Theodore M.P. Lee, “Processors, Operating Systems and Nearby Peripherals: A Consensus Report,” in Ruthberg, “Audit and Evaluation of Computer Security II: System Vulnerabilities and Controls,” Proceedings of the National Bureau of Standards Invitational Workshop Held at Miami Beach, FL, Nov. 28–30, 1978, 8–13.

28 Slayton, “Measuring Risk.”

29 These became known as the “rainbow series.” See discussion in M. Schaefer, “If A1 Is the Answer, What Was the Question? An Edgy Naïf’s Retrospective on Promulgating the Trusted Computer Systems Evaluation Criteria,” paper presented at the Annual Computer Security Applications Conference, Tucson, AZ, December 6–10, 1984.

30 Schaefer, “If A1 Is the Answer”; Steven B. Lipner, “The Birth and Death of the Orange Book,” *IEEE Annals of the History of Computing* 37, no. 2 (April–June 2015): 19–31, <https://doi.org/10.1109/MAHC.2015.27>.

31 The National Security Telecommunications and Information Systems Security Committee (NTISSC) was first established as the U.S. Communications Security Board in 1953 by NSC-168. “CNSS History,” Committee on National Security Systems, accessed Dec. 20, 2020, <https://www.cnss.gov/CNSS/about/history.cfm>. In 1984, President Ronald Reagan’s national security decision directive (NSDD-145) gave the Committee responsibility for safeguarding “national security information” — something that could include sensitive, but non-classified, information. The directive also appointed the director of the National Security Agency as the national manager for telecommunications and information systems security, a role that made the director of the agency the executive secretary for a steering group that oversaw the NTISSC. The NTISSC was chaired by the assistant secretary of defense for command, control, communications, and intelligence and included representatives from the military services and intelligence agencies. *National Security Decision Directive Number 145*, The White House, Sept. 17, 1984, <https://fas.org/irp/offdocs/nsdd145.htm>.

32 Lipner, “The Birth and Death of the Orange Book.”

curity than was required by the federal mandate.³³ Furthermore, these personnel did not know how to use “trusted” systems to build secure networks.³⁴ Computer network vulnerabilities were thus also a result of training and management problems, in addition to being technological and market problems. In 1990, the assistant secretary of defense for com-

[T]he need for computer network defense became a subject for public discussion after a panel of computer scientists addressed it at a 1967 conference and, for the first time, publicly acknowledged the existence of the National Security Agency, previously described as “No Such Agency.”

mand, control, communications, and intelligence tasked the National Security Agency and Defense Communications Agency (soon to become the Defense Information Systems Agency) with developing means of better managing information security. This led to the creation of the Defense Information Systems Security Program, whose aim was to develop a comprehensive and integrated security architecture and policy for the Defense Department.³⁵

However, the purchase, deployment, and man-

agement of computer networks remained highly decentralized across the military, and networks proliferated in the 1980s and early 1990s.³⁶ This left the problem of configuring and maintaining such networks to disparate personnel in communications and computing fields throughout the services.³⁷ As outlined briefly below, each of the services structured its computer and communications career fields a bit differently, but the personnel charged with deploying and managing computer networks generally received little or no training in computer security.³⁸

In the late 1980s and early 1990s, the U.S. Army Information Systems Command was responsible for the Army’s global networking and communications.³⁹ However, in late 1996, the Information Systems Command was made subordinate to the Army Forces Command, where it became Army Signal Command, reducing its independence and underscoring its support role.⁴⁰ The community responsible for computer networking and communications, the Signal Corps, was a support field focused on making networks available to commanders, not securing networks from adversaries.⁴¹ Additionally, the Army’s cultural preference for officers who were generalists rather than technical specialists did not reward deep investment in technical skills in the early 1990s.⁴² None of this encouraged the development of technically deep, security-savvy computer network managers.

By contrast, the Air Force has historically reward-

33 The Trusted Computer System Evaluation Criteria outlined seven levels of security (D, C1, C2, B1, B2, A1, A2), which were defined by the extent to which they fulfilled four kinds of criteria: security policy, accountability mechanisms, assurance mechanisms, and documentation. The levels were ordered hierarchically, with increasingly stringent security requirements. For example, the second lowest level (C1) enforced a discretionary security policy while C2 added better accountability to level C1.

34 John C. Nagengast, “Defining a Security Architecture for the Next Century,” *Journal of Electronic Defense* 15, no. 1 (January 1992): 51–53.

35 Nagengast, “Defining a Security Architecture for the Next Century.” The Defense Information Systems Security Program would be managed by a new Center for Information Systems Security and jointly staffed by personnel from the Defense Information Systems Agency and the National Security Agency. It is not clear from published records whether the Defense Information Systems Security Program ever produced the unified security architecture and policy. “Budget Plan Leaves Military Computers Vulnerable to Intrusion,” *Defense Daily* 184, no. 54 (1994).

36 In the early 1990s, efforts to give the Defense Information Systems Agency centralized control over the services’ information technology purchasing and management largely failed. See, e.g., “Services Retain Information Technology Design, Acquisition powers,” *Defense Daily* 180, no. 57, Sept. 21, 1993. On the proliferation of networks, see Allen Li, “DOD’s Information Assurance Efforts,” Letter to the Chairman of the House Subcommittee on Military Research and Development, June 11, 1998, 4, <https://www.gao.gov/assets/90/87860.pdf>.

37 Although National Telecommunications and Information Systems Security Directive No. 500, “Telecommunications and Automated Information Systems Security Education, Training, and Awareness,” issued in June 1987, officially required agencies to implement security education and training programs, its effectiveness seems to have been limited. This directive is mentioned in the one that superseded it: “NSTISS Directive 500: Information Systems Security (INFOSEC) Education, Training, and Awareness,” National Security Telecommunications and Information Systems Security Committee, Feb 25, 1993, <https://apps.dtic.mil/sti/pdfs/ADA362604.pdf>.

38 The lack of skills and training among systems administrators throughout the military was repeatedly identified as a principal reason for breaches in Defense Department networks. See, for example, *Virus Highlights Need for Improved Internet Management*, General Accounting Office, June 12, 1989, 20–21, <https://www.gao.gov/products/IMTEC-89-57>; Jack L. Brock, “Hackers Penetrate DOD Computer Systems,” Testimony Before the Subcommittee on Government Information and Regulation, Committee on Governmental Affairs, U.S. Senate, (November 1991), 1, <https://www.gao.gov/assets/110/104234.pdf>; and *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*, Government Accountability Office, May 22, 1996, 6.

39 See, e.g., Maura Harrington, “Army’s IS Ready for the Worst,” *Computerworld* XXV, no. 2 (1991).

40 “Army Streamlines Information Services for Force XXI,” *Army Logistician*, no. Jan/Feb (1997). This change was ostensibly made in support of efforts to create a digitized force for the 21st century, Force XXI.

41 White, “Subcultural Influence on Military Innovation,” 108–09.

42 See White, “Subcultural Influence on Military Innovation,” chap. 3.

ed technical depth, expecting its officers to develop substantial technical expertise prior to taking command.⁴³ The Air Force was also an early leader in networked computing and communications. By December 1989, Air Force Communications Command was the most globally dispersed command in the Air Force, including more than 54,000 personnel working in 430 U.S. locations and 27 foreign locations.⁴⁴ Yet, in the early 1990s, as part of post-Cold War streamlining and downsizing, the Air Force reduced the independence and strength of its communications command and associated personnel. In October 1990, communications personnel were put under the command of the operational units that they served, shrinking the command to fewer than 8,000 personnel. In July 1991, the Communications Command was further demoted from major command to field operating agency.⁴⁵ Over the next several years, the number of distinct Air Force Specialty Codes for computing and communications officers were substantially reduced as very different areas of work were merged together and officers were explicitly encouraged to be generalists rather than specialists.⁴⁶ Taken together, these changes eroded any possibility of centralized control of computer network security in the Air Force, while discouraging communications officers from pursuing technical depth that would be needed to ensure security.

The Navy's communications and computing management was even more decentralized than the Air Force's in the 1980s and 1990s. Throughout the 1990s, the Naval Computer and Telecommunications Command was responsible for ensuring interoperability of legacy and new communications-computing systems and for providing, operating, and maintaining shore-based and non-tactical communications systems.⁴⁷ However, this left myriad other systems to be developed by other commands. By

the turn of the millennium, the Navy had 28 different commands independently developing, operating, and maintaining their own computer systems.⁴⁸ The Navy also lacked a centralized communications command or career field in the 1990s, despite having enlisted ratings such as "radioman" and "data processing technician."⁴⁹ Afloat, responsibilities for communications were often assigned to officers for a limited period, without any formal training.⁵⁰ Ashore, much of the communications and computing work was performed by general unrestricted line officers, a non-combat, shore-based community that was 93 percent female in 1990.⁵¹ It became the fleet support officer community after laws barring women from combat roles were lifted in 1995, and continued to perform many of the same functions both ashore and afloat. Yet, there was no formal training required for performing these roles. People typically had to learn on the job.⁵²

To summarize, vulnerabilities in Defense Department networks were not just a matter of external technological changes or insecurities in commercial products that the department could not control. The Department of Defense actively drove many innovations in computer networking and security but failed to ensure that its networks would be securely deployed or maintained. Although communications and computing personnel in the services comprised the first line of computer network defense — responsible for configuring networks, managing passwords, and much more — most lacked an understanding of how to secure networks. It was ultimately the Defense Department's inability to centrally manage the security of computer networks, combined with a lack of security skills and knowledge among its disparate communications-computing personnel, that made its networks so vulnerable.

43 Sarah White discusses this cultural preference in "Subcultural Influence on Military Innovation," chap. 4.

44 Thomas S. Snyder, ed., *Air Force Communications Command, 1938-1991: An Illustrated History* (Scott Air Force Base, Illinois: Air Force Communications Command Office of History, 1991), 259. For more about the Air Force's early contributions to computing, see discussions of air defense in Slayton, *Arguments that Count* and in Paul N. Edwards, *The Closed World: Computers and the Politics of Discourse in Cold War America* (Cambridge, MA: MIT Press, 1996).

45 Snyder, *Air Force Communications Command, 1938-1991*, 261.

46 A much more detailed account of these changes can be found in Joseph R. Golembiewski, "From Signals to Cyber: The Rise, Fall, and Resurrection of the Air Force Communications Officer," Master's Thesis, School of Advanced Air and Space Studies, Air University, 2010.

47 Michael R. "Mo" Morris, "History of NAVNETWARCOM," Navy CT History, July 13, 2008, <https://www.navycthistory.com/COMNAVTELCOMto-NETWARCOMHistory.txt>.

48 Sharon Anderson, "Why We Need the Navy Marine Corps Intranet," *CHIPS*, July–September 2004, <https://www.doncio.navy.mil/Chips/ArticleDetails.aspx?ID=3296>.

49 Danelle Barrett, "Developing a Community of C4IW Professionals," *Proceedings* 126, no. 6 (June 2000), <https://www.usni.org/magazines/proceedings/2000/june/developing-community-c4iw-professionals>.

50 Robert L. Buchanan and Sean Donohoe, "Is Navy 'Information Management' Becoming an Oxymoron?" *Proceedings* 125, no. 6 (June 1999), <https://www.usni.org/magazines/proceedings/1999/june/navy-information-management-becoming-oxymoron>.

51 Lori Turley, "The Feasibility of Specialized Subcommunities within the General Unrestricted Line Officer Community," Master's Thesis, Naval Postgraduate School, 1990; Barrett, "Developing a Community of C4I Professionals."

52 Barrett, "Developing a Community of C4I Professionals."

Threat-Oriented Approaches to Computer Network Defense

Computer scientists working with intelligence agencies recognized early on that even if they could create systems that would enforce security policies perfectly, an insider could wittingly or unwittingly compromise the system.⁵³ This recognition led to the development of one of the first threat-oriented approaches to computer network defense — intrusion detection systems — that would monitor computers and networks for suspicious behavior and alert security officers about potentially unauthorized activity. The National Security Agency, the Navy, and the Air Force all sponsored research into intrusion detection systems in the 1980s, and by the early 1990s were using such systems to monitor select networks.⁵⁴ They also developed new kinds of expertise associated with intrusion detection systems, as security officers learned how to evaluate alerts about suspicious activity and determine what actions, if any, should be taken.⁵⁵

Another early threat-oriented approach to computer network defense came in the form of computer emergency response teams, also known as computer incident response teams. These teams were first created in response to the Internet worm of Nov. 2, 1988.⁵⁶ The worm was the first to significantly disrupt the Internet, which was then primarily a research network sponsored by the Defense Department. The Computer Emergency Response Team Coordinating Center, a federally funded, non-governmental organization based at Carnegie Mellon University, was established in January 1989 with

the goals of preventing future incidents, providing a network of elite experts who could be called upon to diagnose future attacks, and facilitating the creation of a network of similar response teams.⁵⁷

Defense Department units and the national nuclear laboratories were among the first organizations to form their own computer emergency response teams. In the early 1990s, the Defense Intelligence Agency formed an incident response team for its classified Intelligence Information Systems network, which, in late 1992, was renamed the Automated Systems Security Incident Support Team and moved to the Defense Information Systems Agency, where it was tasked with responding to incidents across the Defense Department.⁵⁸ Each of the services also began to form incident response capabilities.⁵⁹

In the early 1990s, response teams helped to identify and make visible intrusions that might otherwise have gone unnoticed. For example, the Department of Energy's Computer Incident Advisory Capability helped discover that between April 1990 and May 1991, at least 34 of the Defense Department's computers had been hacked.⁶⁰ Further investigation eventually concluded that the hackers were teenagers in the Netherlands who called themselves "High Tech for Peace" and had gained access to a computerized logistics management system. During preparations for Operation Desert Storm in Iraq, the hackers offered to sell the capabilities gained through that system to Saddam Hussein for \$1 million. Had the Iraqi government responded to the offer, which fortunately it did not, the hackers could have disrupted the flow of sup-

53 James P. Anderson, *Computer Security Threat Monitoring and Surveillance*, Fort Washington, PA, Feb. 26, 1980, revised April 15, 1980, <https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/ande80.pdf>. This is the earliest known study of threat monitoring. Anderson was an independent computer security expert who worked as a contractor primarily for military and intelligence agencies. While it is unclear what agency commissioned this report, it was very possibly the National Security Agency. And despite its opaque origins, the report was widely circulated and became very influential.

54 The early history of this work is described well in Jeffery R. Yost, "The March of IDES: Early History of Intrusion-Detection Expert Systems," *IEEE Annals of the History of Computing* 38, no. 4 (October–December 2016): 42–54, <https://doi.org/10.1109/MAHC.2015.41>. Systems were deployed by the Navy's Space and Naval Warfare Systems Command, the Air Force Cryptologic Support Center, and the National Computer Security Center.

55 For example, one of the earliest such systems, the Intrusion Detection Expert System (IDES), had separate interfaces for systems administrators, security officers, and analysts. Yost, "The March of IDES."

56 "Internet" is capitalized here to highlight that it refers to a specific network developed under contract to the U.S. Department of Defense. This was an important predecessor to the much larger and more public network that is known as the "internet." Internet is also capitalized throughout this paper in references to this specific worm.

57 For a more detailed history, see Slayton and Clarke, "Trusting Infrastructure."

58 Author interview with Kenneth van Wyk, Feb. 20, 2018, Alexandria, VA.

59 The exact date on which each service formed an incident response team is unclear from the historical record. The Computer Emergency Response Team (CERT) Coordinating Center held invitational workshops each year immediately following the worm and by 1990, presentations discussing a preliminary "CERT System" indicated the involvement of all three services. Mention of the Air Force Computer Emergency Response Team can be found at the 15th National Computer Security Conference, sponsored by the National Institute of Standards and Technology and the National Computer Security Center in October 1992. However, White's thesis dates the formation of the Navy's Computer Incident Response Team to 1995 and the Army's Computer Emergency Response Team to September 1996. See White, "Subcultural Influence on Military Innovation," 67, 307. Most likely, all services had nascent incident response capabilities by 1990 but subsequently strengthened those capabilities.

60 John Markoff, "Dutch Computer Rogues Infiltrate American Systems with Impunity," *New York Times*, April 21, 1991, <https://www.nytimes.com/1991/04/21/us/dutch-computer-rogues-infiltrate-american-systems-with-impunity.html>. The attackers had broken into computers at national laboratories that served as hosts for the MILNET, a non-classified military network.



plies to U.S. troops preparing for Desert Storm.⁶¹

Intrusion detection systems and incident response teams were important not only for identifying and stopping intruders, but also for making the argument that computer networks were increasingly under attack. Response teams tracked an exponential rise in incidents that paralleled the exponential rise in internet host sites in the 1990s.⁶² By presenting these statistics to policymakers both within and beyond the military, they could make an argument for devoting more resources to defending networks.

But intrusion detection and incident response did more than simply demonstrate the growth of threats and the need to confront them. Incident investigators also worked to identify the causes of the breaches and, in the process, repeatedly underscored the importance of a prior layer of defense: the systems administrators and personnel who were charged with deploying and maintaining secure networks. The 1989 Internet worm, the Dutch hacking incident, and many other breaches were enabled by a lack of security knowledge, skills, and practice among systems administrators.⁶³ In 1999, an analysis by the Air Force Office of Special Investigations showed that a majority of root intrusions in the previous year had resulted from noncompliance with security policies or emergency response team advisories. Only 13 percent were definitively determined to be “unpreventable.”⁶⁴

Thus, the Defense Department’s threat-oriented approaches to network defenses became critical in the mid-1990s in no small part because of failings in the first line of defense: the systems administrators and maintainers who were uniquely positioned to prevent and mitigate vulnerabilities. Although both threat-oriented and vulnerability-oriented forms of expertise would eventually be incorporated into a

new conception of warfighting, that transition was slower and more difficult for vulnerability-oriented expertise, as discussed in more detail below.

The Rise of Information Warfare and Information Assurance

In the mid-1990s, computer network operations began to find an organizational and conceptual home in “information warfare.” To be clear, information warfare was not primarily about computer network operations. When military officers described Operation Desert Storm as the “first information war,” they were discussing much older traditions of work such as gathering intelligence through satellites and airborne reconnaissance systems, using such intelligence to bomb command-and-control facilities, and setting up an in-theater communications system.⁶⁵

Similarly, when the Department of Defense issued a top secret directive on information warfare in December 1992, it devoted little, if any, attention to the opportunities and risks inherent to using computer networks in military and intelligence operations.⁶⁶ The directive defined information warfare as the “competition of opposing information systems” through methods such as “signals intelligence and command and control countermeasures.”⁶⁷ Such countermeasures, also known as command-and-control warfare, were defined as the “integrated use” of five elements — “operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW), and physical destruction” — all “mutually supported by intelligence.”⁶⁸ Information warfare thus encompassed a very diverse range of military special-

61 John J. Fialka, “Pentagon Studies Art of ‘Information Warfare’ To Reduce Its Systems’ Vulnerability to Hackers,” *Wall Street Journal*, July 3, 1995; Brock, *Hackers Penetrate DOD Computer Systems*; author phone interview with William Gravell, May 22, 2020.

62 See, for example, the testimony of Computer Emergency Response Team Coordination Center Director Richard Pethia in the hearing, “Security in Cyberspace,” 306–23. Although Pethia was focused on civilian security incidents, he spoke in hearings that were motivated by intrusions of Department of Defense networks. Additionally, a presentation from January 1999 demonstrates that the Air Force Computer Emergency Response Team and Office of Special Investigations were collecting similar statistics by the late 1990s. See “Information Assurance Update,” U.S. Air Force, Jan. 29, 1999, <https://nsarchive.gwu.edu/dc.html?doc=6168264-National-Security-Archive-US-Air-Force>.

63 General Accounting Office, *Virus Highlights Need for Improved Internet Management*, 20–21; Brock, *Hackers Penetrate DOD Computer Systems*, 1; Government Accountability Office, *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*, 6.

64 U.S. Air Force, “Information Assurance Update.”

65 Alan D. Campen, ed. *The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War* (Fairfax, VA: AFCEA International Press, 1992). Edward Mann, “Desert Storm: The First Information War?” *AirPower Journal* VIII, no. 4 (Winter 1994): 4–14, https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-08_Issue-1-Se/1994_Vol8_No4.pdf.

66 It is possible that the directive mentioned attacking and defending computer systems — approximately 14 lines of the four-page document remain classified — but computer network attack and defense are not mentioned in the declassified portion of the document, which is much larger than the classified portion. Donald J. Atwood, “Information Warfare,” Department of Defense Directive TS 3600.1, Dec. 21, 1992.

67 Atwood, “Information Warfare,” 1.

68 “Electronic Warfare (EW) and Command and Control Warfare (C2W) Countermeasures,” Department of Defense Directive 3222.4, July 31, 1992, 1. Revisions issued on Oct. 22, 1993 included replacing all references to “command, control, and communications countermeasures” with “command and control warfare.”

izations, all of them long predating computers.⁶⁹

Nonetheless, information warfare provided the primary conceptual and organizational context for efforts to raise the status of computer network defense and attack in the mid-1990s.⁷⁰ As discussed further below, each of the services approached computer network operations somewhat differently, but they all built upon incident response and intrusion detection work that had begun in their signals intelligence organizations rather than their communications and computing units.

Air Force: Cyberspace as a New Warfighting Domain

Of the three services, the Air Force was the most willing to see computer network operations as a new area of warfighting. Nonetheless, its initial response to the 1992 information warfare directive was not to create a new warfighting unit. Instead, it merged the security functions of the Air Force Cryptologic Support Center with the Air Force's Electronic Warfare Center, thereby creating the Air Force Information Warfare Center at Kelly Air Force Base in San Antonio, Texas.⁷¹ About half of the center's personnel had backgrounds in signals intelligence, while the rest came from a variety of fields.⁷² At its founding in September 1993, the Information Warfare Center was within the Air Force Intelligence Command, but in October 1993 this command was demoted from a major command to a field operating agency, the Air Intelligence Agency. The Information Warfare Center was co-located

with the Joint Electronic Warfare Center, which became the Joint Command and Control Warfare Center in September 1994.⁷³ Despite the "warfare" moniker, both of these centers played supporting roles, helping integrate various information warfare methods into combat operations.

In the early 1990s, the Air Force also began to integrate some computer network operations into warfighting through the Special Technical Operations system. Air Force Col. Walter "Dusty" Rhoads, a fighter pilot who was assigned to the planning division of Tactical Air Command in 1991, recalls that he began to integrate an early version of computer network operations into war plans after helping set up a Special Technical Operations office for Tactical Air Command, which would soon become Air Combat Command.⁷⁴ The Special Technical Operations system provided a means for regional commands to integrate highly classified capabilities — such as computer network attack — into military operations.⁷⁵ When he briefed the general who was directing Tactical Air Command operations, the general told him, "You're going to make this information warfare."⁷⁶ As a result, Rhoads became the director of a new information warfare branch at the Air Combat Command, with the Special Technical Operations office as a focus of the new branch.⁷⁷

In 1994, the information warfare branch, under Rhoads' direction, put together a plan to support Operation Uphold Democracy, which aimed to undo the 1991 coup of democratically elected Haitian President Jean-Bertrand Aristide. It worked with the Air Force Information Warfare Center,

69 In March 1993, the chairman of the Joint Chiefs of Staff issued a revised memorandum of policy on command-and-control warfare, calling it "the military strategy that implements information warfare." "Memorandum of Policy Number 30: Command and Control Warfare," Department of Defense, March 1993, 3, <https://archive.org/details/JCSMemoofPolicyNumber30CommandandControlWarfare>. This was a revision to a 1990 memo on command, control, and communications countermeasures (C3CM). This revision replaced C3CM with C2W. It also added "psychological warfare" as one of five elements of C2W.

70 In December 1996, Directive S-3600.1, Information Operations, replaced the 1992 Directive on Information Warfare, and explicitly acknowledged the threat that "computer network attack" posed to command-and-control systems. The 1996 directive expanded the focus of the 1992 directive on winning in military conflict and included the goal of securing "peacetime national security objectives" through civil and public affairs activities. It was only in 1998 that Joint Doctrine on Information Operations noted that offensive information operations "may include computer network attack." John P. White, "Department of Defense Directive S-3600.1: Information Operations," Department of Defense, Dec. 9, 1996, 1-1, <http://www.iwar.org.uk/iwar/resources/doctrine/DOD36001.pdf>.

71 "EW Expands Into Information Warfare," *Aviation Week & Space Technology* 141, no. 10 (October 1994): 47–48.

72 White, "Subcultural Influence on Military Innovation," 195.

73 *Aviation Week & Space Technology*, "EW Expands Into Information Warfare."

74 Author phone interview with Walter Rhoads, June 4, 2020.

75 The Joint Staff's Operations Directorate was home to the Special Technical Operations Division, which monitored dozens of "black" programs. Regional commands maintained Special Technical Operations divisions and could help integrate these highly classified capabilities into military operations. William M. Arkin, "Phreaking Hacktivists," *Washington Post*, Jan. 18, 1999, <https://www.washingtonpost.com/wp-srv/national/dotmil/arkin011899.htm>. The Special Technical Operations office was also part of Atlantic Command's Information Warfare Cell.

76 Author phone interview with Rhoads, June 4, 2020.

77 Similarly, at the Atlantic Command, the Special Technical Operations office also played a role in expanding the range of "information warfare" to include computer network attack. A 1995 depiction of Atlantic Command's Information Warfare Cell structure included the five traditional pillars of command-and-control warfare along with the Special Technical Operations office, which served as a liaison to the Joint Command and Control Warfare Center and the Special Technical Operations Division of the Joint Staff (J-33). Joanne Sexton, "A Combatant Commander's Organizational View of Information Warfare/Command and Control Warfare," Naval War College, 1995. The Special Technical Operations office also shows up in 1998 joint doctrine on information operations.

where a junior officer who had once been a “demon dialer” — someone who manipulates the phone system to make free long-distance calls — figured out how to tie up all the phone lines in Haiti. This in turn would shut down Haiti’s air defense system because the system communicated via phone lines, allowing the Air Force to fly over undetected.⁷⁸

Although Operation Uphold Democracy was called off after a delegation led by Jimmy Carter persuaded the military leaders of Haiti to step down, the phone hacking plan impressed Maj. Gen. Kenneth Minihan, commander of the Air Intelligence Agency. In the fall of 1994, Minihan became the assistant chief of staff for intelligence at the Defense Department and began to advocate for creating an information warfare squadron — a warfighting unit that would have Title 10 authorities (military operations) rather than Title 50 authorities (intelligence).⁷⁹ Rhoads also helped make the case for such a squadron, briefing the commander of Air Combat Command who, in turn, briefed the Air Force chief of staff.⁸⁰

Meanwhile, the Air Force was developing doctrine that highlighted the uniqueness of computer network operations. In 1995, Air Force Maj. Andrew Weaver, who had a background as a weapons operator but was working in the doctrine division of the Air Staff, wrote a paper titled “Cornerstones of Information Warfare,” which was published with a preface signed by the Air Force chief of staff and the secretary of the Air Force.⁸¹ Weaver emphasized that the “revolution” associated with information technology was doing more than simply increasing the efficiency of traditional combat operations. Rather, he argued that “information age technology is turning a theoretical possibility into fact: *directly* manipulating the adversary’s information.”⁸²

To the five elements of information warfare established in the 1992 directive, Weaver added “in-

formation attack” as a sixth element. He argued that, unlike other elements of information warfare, direct information attack bypassed the enemy’s observations. He contended that direct information attack could have the same result as one causing physical destruction, but with more certainty, less time, and less cost, suggesting a similarity between bombing a telephone switching station and destroying its software. And he argued that information should be understood as a new “realm” or “domain” for operations, akin to land, sea, and air, noting “strong conceptual parallels between conceiving of air and information as realms.”⁸³

The arguments of Minihan, Rhoads, and Weaver proved persuasive to Air Force leadership.⁸⁴ In August 1995, the Air Force ordered the formation of the 609th Information Warfare Squadron under the 9th Air Force at Shaw Air Force Base. The squadron was charged with conducting both defensive and offensive missions in support of the 9th Air Force and Central Command’s Air Operations Center. The squadron thus remained a kind of operations support, but unlike the Air Force Information Warfare Center, it operated under the authority of Title 10.⁸⁵

Rhoads was selected as commander of the new unit and Weaver was chosen as the operations officer. Rhoads and Weaver handpicked eight additional individuals to serve as the first cadre. Rhoads recalls that since nobody “knew what a cyber warrior was,” they put together “a combination of past war fighters, J-3 [Operations] types, a lot of communications people and a smattering of intelligence and planning people.”⁸⁶ Of the initial 10-person team, five had a background in computers or networking, but the leadership — Rhoads and Weaver — came from traditional operational backgrounds.⁸⁷

Since many of the initial members of the squadron lacked an understanding of computer networking,

78 Author phone interview with Rhoads, June 4, 2020. Also, Kaplan, *Dark Territory*, 58.

79 Kaplan, *Dark Territory*, 108.

80 Author phone interview with Rhoads, June 4, 2020.

81 Although Weaver’s name does not appear on this document, his authorship has been acknowledged elsewhere. See, e.g., Joseph A. Ruffini, *609 IWS: A Brief History, Oct 1995-Jun 1999*, Department of the Air Force, 1999, <https://pdf4pro.com/fullscreen/departement-of-the-air-force-securitycritics-org-5b034d.html>.

82 “Cornerstones of Information Warfare,” Department of the Air Force, 1995, 2, <https://hdl.handle.net/2027/uc1.31210023608514>. Although Andrew Weaver’s name does not appear on this document, his authorship has been acknowledged elsewhere. See, e.g., Ruffini, *609 IWS: A Brief History*.

83 Department of the Air Force, “Cornerstones of Information Warfare,” 8.

84 Kaplan, *Dark Territory*.

85 The potential legal problem of having the Air Force Information Warfare Center engaged in “warfighting” in Operation Uphold Democracy was one rationale for creating an operational information warfare unit. Kaplan, *Dark Territory*.

86 “Transcript: Lessons from Our Cyber Past — The First Military Cyber Units,” Atlantic Council, March 5, 2012, <https://www.atlanticcouncil.org/commentary/transcript/transcript-lessons-from-our-cyber-past-the-first-military-cyber-units/>.

87 Ruffini, *609 IWS: A Brief History*, 36. Specifically, the five communications or networking backgrounds listed are communications networking, space operations, telecom information warfare at the Information Warfare Center, computer security, and information management. The backgrounds of the other five members are listed as fighter pilot (Rhoads), weapons system operator (Weaver), acquisition, intelligence, and security police.

they took a three-day course on computer networking in April 1996. This is described in the squadron's official history as "a huge success," but the squadron needed a more comprehensive training

fensive operations.⁹³ The squadron also privileged offensive work by requiring individuals to do defensive duty before they were allowed to take the offensive.⁹⁴ At Blue Flag 1998, one of the Air Force's annual operational exercises, this approach led to an easy victory for the offense. The squadron's official history recounts that the squadron's red team "created a steep learning curve" for the defense.⁹⁵ A National Research Council committee that witnessed the exercise offered a less varnished assessment: "The defensive cell ... was overwhelmed by its red team counterpart. (For example, the red team was able to download the air tasking order before it was transmitted.)"⁹⁶ The committee critiqued the squadron's overall emphasis on offense:

The squadron's emphasis on offense, however, makes perfect sense from the perspective of a new unit eager to demonstrate its value to warfighters. Offensive operations could create dramatic military effects, at least in theory.

program, particularly as the initial 10-person team grew.⁸⁸ It considered existing Defense Department courses, but concluded that none would work because the courses were geographically dispersed and only portions of the courses were relevant to what the squadron needed to know. So instead, the squadron arranged for a series of commercial courses to provide training in June and July of 1996.⁸⁹

In keeping with an emphasis on warfighting, the squadron's work appears to have been focused on threat-oriented activities, such as intrusion detection and response, rather than vulnerability mitigation, which would have included password management, configuration management, and training.⁹⁰ Shortly after undergoing initial training, the squadron tested and selected a "defensive system," a network-monitoring and intrusion-detection system.⁹¹ Over the next two years, this equipment allowed the squadron to demonstrate its defensive capabilities to hundreds of "distinguished visitors" in numerous exercises.⁹²

While the squadron's official history emphasizes the defensive mission, Rhoads recalls that the majority of its mission time was actually spent on of-

With a culture that values the taking of the offensive in military operations, the military may well have difficulty in realizing that defense against information attack is a more critical function than being able to conduct similar operations against an adversary, and indeed is more difficult and requires greater skill and experience than offensive information operations.⁹⁷

The National Research Council committee went on to note that "the National Security Agency requires code-breaking experience before an analyst can begin to develop encryption algorithms."⁹⁸ In other words, the agency required trainees to practice offense before graduating to the more difficult work of defense.

The squadron's emphasis on offense, however, makes perfect sense from the perspective of a new unit eager to demonstrate its value to warfighters. Offensive operations could create dramatic military effects, at least in theory. By contrast, the effects of a successful defense are unremarkable: Military operations and networks would continue to function as planned.

88 Ruffini, *609 IWS: A Brief History*, 10.

89 Ruffini, *609 IWS: A Brief History*, 11.

90 See, e.g., discussion of Exercise Fort Franklin V in Ruffini, *609 IWS: A Brief History*, 14.

91 Ruffini, *609 IWS: A Brief History*, 11.

92 Ruffini, *609 IWS: A Brief History*, 13.

93 Atlantic Council, "Transcript: Lessons from Our Cyber Past — The First Military Cyber Units."

94 *Realizing the Potential of C4I: Fundamental Challenges* (Washington, DC: National Academy Press, 1999), 161, <http://nap.edu/6457>.

95 Ruffini, *609 IWS: A Brief History*, 25.

96 National Academy Press, *Realizing the Potential of C4I*, 161.

97 National Academy Press, *Realizing the Potential of C4I*, 161.

98 National Academy Press, *Realizing the Potential of C4I*, 161.



While the 609th Squadron was widely regarded as successful, in June of 1998, senior Air Force leadership decided to change the organization of information operations in an effort to cut costs and personnel requirements. This led to the termination of the squadron. Most of its functional responsibilities were transferred to what soon became the 67th Information Operations Wing within the Air Intelligence Agency at Kelly Air Force Base, returning computer network operations to its intelligence roots.⁹⁹

Navy: Net-Centric Warfare

Like the Air Force, the Navy responded to the 1992 information warfare directive by reorganizing ongoing work within the Naval Security Group, the Navy's cryptologic unit. Navy cryptologists perform functions similar to signals intelligence and electronic warfare personnel in other services but have held a special place in the Navy since their decisive role in the Battle of Midway and similar clashes during World War II.¹⁰⁰ In the Navy, cryptology and intelligence are distinct career fields with a history of rivalry, despite the close connection between the two. In July 1994, the Naval Information Warfare Activity was formally launched within the Naval Security Group, building on earlier, highly classified work on command-and-control warfare.¹⁰¹ The activity was staffed by handpicked technical experts who developed new information warfare capabilities.¹⁰²

The Navy also established the Fleet Information Warfare Center under Atlantic Command in October 1995 to help operationalize capabilities developed by the activity.¹⁰³ The center had a defensive focus: The Navy's director of command-and-control warfare explained that it would ensure "the battle groups are buttoned up against" information threats.¹⁰⁴ He described the Fleet Information Warfare Center as the Navy's "911" service for information warfare, which was likely a reference to the new Navy Computer Incident Response Team that was formalized within the Fleet Information Warfare Center at its founding.¹⁰⁵ The center was a tiny organization comprised of warfighters — its first director was a former fighter pilot — along with cryptologists, electronic warfare technicians, and intelligence officers.¹⁰⁶

The Naval Information Warfare Activity and the Fleet Information Warfare Center played supporting roles similar to the Air Force's Information Warfare Center, but the Navy did not create a warfighting unit focused on computer network operations, akin to the Air Force's 609th Squadron. Instead, it sought to integrate the much broader field of information warfare into its composite warfare commander construct, wherein each battlegroup designates an officer to command a particular mission area. In 1989, well before the 1992 information warfare directive was issued, the Navy designated space and electronic warfare as a major warfare area, equal to surface, underwater, and air

99 Ruffini, *609 IWS: A Brief History*, 27.

100 White, "Subcultural Influence on Military Innovation," 984.

101 "Navy C4I Budget Safe for Now," *Defense Daily* 184, no. 41, Aug. 29, 1994, 321.

102 White, "Subcultural Influence on Military Innovation," 304. The Naval Information Warfare Activity grew to 200 to 300 people by the early 2000s and was primarily focused on developing technology and capabilities. Eventually it became the Navy Cyber Warfare Development Group within Tenth Fleet. Mario Vulcano, "Navy Information Warfare Activity Was Established in July, 1994," Station HYPO, July 22, 2017, <https://station-hypo.com/2017/07/22/navy-information-warfare-activity-was-established-in-july-1994/>.

103 Bryan Bender, "Navy Chief Commissions Fleet Information Warfare Center," *Defense Daily* 189, no. 17, Oct. 25, 1995. Also, "Implementing Instruction for Information Warfare/Command and Control Warfare," OPNAV Instruction 3430.26, Office of the Chief of Naval Operations, Jan. 18, 1995, http://www.iwar.org.uk/iwar/resources/opnav/3430_26.pdf.

104 Bender, "Navy Chief Commissions Fleet Information Warfare Center."

105 It is not entirely clear when the Navy Computer Incident Response Team was established. On May 31, 1990, the Naval Electronic Systems Security Engineering Center hosted a meeting that included representatives from all of the services to discuss cooperation among computer emergency response teams that dealt with national security information. This suggests that the Navy and other services already had some nascent incident response capabilities. However, some date the formation of the incident response team to the formation of the Fleet Information Warfare Center in October 1995. See, e.g., David Finley, "Navy Cyber Defense Operations Command Celebrates Its Past, Present and Future," *CHIPS*, Feb. 11 2016, <https://www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=7445>.

106 Bender, "Navy Chief Commissions Fleet Information Warfare Center." The exact size of the Fleet Information Warfare Center is difficult to establish. According to a 1996 Government Accountability Office report, only three of 30 personnel spots were granted for the Fleet Information Warfare Center. *Computer Attacks at Department of Defense Pose Increasing Risks*, Government Accountability Office, May 1996, 38. On the other hand, the Navy Computer Incident Response Team, formed at the same time within the Fleet Information Warfare Center, is described as having five people at its founding, growing to 250 people by 2003, and becoming the operational arm of the Fleet Information Warfare Center. Finley, "Navy Cyber Defense Operations Command Celebrates Past, Present, Future." One of White's interviewees states that the Fleet Information Warfare Center started as a "handful" of officers and contractors. White, "Subcultural Influence on Military Innovation," 306. Most likely, the discrepancies in numbers relate to the question of whether new billets were created or simply reassigned. Reportedly, the "Navy did not create new billets for the command, but rather, 'extracted' operation and maintenance funds from facilities which have been stood down." Bender, "Navy Chief Commissions Fleet Information Warfare Center."

operations.¹⁰⁷ Two years later, the Space, Command and Control Directorate was renamed the Space and Electronic Warfare Directorate, and a new billet was created within the composite warfare commander construct — the space and electronic warfare commander.¹⁰⁸ By the late 1990s, this had become the command and control warfare commander, and by the early 2000s it was changed to the information warfare commander.¹⁰⁹

Nonetheless, there was little consensus on what role information warfare should play in naval operations. Was it really a new area of warfare on par with surface, subsurface, and air, or was it a disparate set of tools to be used in support of more established warfighting areas? The Navy did not issue any formal doctrine on information warfare in the mid-1990s, and discussions in the *Proceedings of the U.S. Naval Institute* from this period indicate a wide range of views.

For example, one naval intelligence officer argued that the wide-ranging methods of information warfare could not be assigned to a single commander. Activities such as destruction belonged to all warfare commanders and operational security was everyone's responsibility. He suggested that the only "unique" thing brought by an information warfare commander was "computer war," which was coming to be seen as "the sixth element of information warfare." However, he argued that "for the foreseeable future, such capabilities most likely will remain under theater-level and strategic planners" rather than at the battlegroup level.¹¹⁰

An officer specializing in electronic warfare similarly noted that many areas of information warfare were the domain of others including computer network defense, which was managed by information system security personnel. Furthermore, because there was no focused career field for officers specializing in computing or communications in the

1990s or a corresponding warfare qualification, the officers assigned to be the information warfare commander typically did not have substantial expertise in computing or any other aspects of information warfare.¹¹¹ However, rather than suggesting that the information warfare commander position should be abolished, this officer argued that the Navy should create a career specialization to provide adequate training.¹¹²

In general, naval officers were more skeptical than their Air Force counterparts about the notion that cyberspace constituted a new domain. Naval intelligence officer Robert Gourley objected to discussions of "fighting in cyberspace" and of creating teams of 'cyberwarriors' to lead those fights."¹¹³ Gourley insisted that "we cannot fight in cyberspace any more than we can walk inside a Picasso painting" and framed information warfare in terms of its intelligence impact, arguing that it "has the potential to do for today's military what Ultra and Magic did for our forces during World War II—provide insight into enemy intentions and form the basis of our deception plans."¹¹⁴ Another naval intelligence officer went further, arguing that while the "military has viewed information services (traditionally, intelligence and communications) as supporting inputs to the actual warfare functions of fire, maneuver, and strike," information warfare "might not always be a supporting function; in some future campaigns, it might take a leading role."¹¹⁵

The most influential articulation of the growing importance of computer networking came from Vice Adm. Arthur K. Cebrowski, a fighter pilot who had earned a master's degree in Information Systems Management from the Naval Postgraduate School in 1973.¹¹⁶ In the early 1990s, Cebrowski became the Navy's director for space, information warfare, and command and control.¹¹⁷ In 1994, he became the director of the Joint Staff's Command,

107 John Morton, "Space and Electronic Warfare Comes of Age," *Proceedings* 117, no. 1 (1991): 94–95. The elevation of the information warfare commander was driven, in part, by the growing volume of over-the-horizon targeting data that were being transmitted from shore to ship, without the corresponding ability for shooters to use them.

108 White, "Subcultural Influence on Military Innovation," 301–02.

109 For these uses, compare Erik J. Dahl, "We Don't Need an IW Commander," *Proceedings* 125, no. 1 (January 1999), <https://www.usni.org/magazines/proceedings/1999/january/we-dont-need-iw-commander> and Mitch Houchin, "Get Serious About Tactical Information Ops," *Proceedings* 129, no. 10 (October 2003), <https://www.usni.org/magazines/proceedings/2003/october/get-serious-about-tactical-information-ops>.

110 Dahl, "We Don't Need an IW Commander."

111 Barrett, "Developing a Community of C4I Professionals." Houchin, "Get Serious About Tactical Information Ops."

112 Houchin, "Get Serious About Tactical Information Ops."

113 Robert D. Gourley, "The Devil Is in the Details," *Proceedings* 123, no. 9 (September 1997), <https://www.usni.org/magazines/proceedings/1997/september/devil-details>.

114 Gourley, "The Devil Is in the Details." Gourley went on to become the first intelligence officer for the Joint Task Force-Computer Network Defense.

115 George F. Kraus, Jr., "Information Warfare in 2015," *Proceedings* 121, no. 8 (August 1995), <https://www.usni.org/magazines/proceedings/1995/august/information-warfare-2015>.

116 "About the Cebrowski Institute," Naval Postgraduate School, accessed Oct. 19, 2020, <https://nps.edu/web/cebrowski/about>.

117 "Cebrowski Will Return to Post as Chief of Navy IT Operations," *Government Computer News* 15, no. 17, July 15, 1996.



Control, Communications and Computers Directorate and established a new unit for defensive information warfare, described further below. In 1996, Cebrowski returned to his position as director for space, information warfare, and command

operational experience in these areas. These are the new operators.¹¹⁹

The Navy did make some changes to its information technology specializations in the late 1990s. In 1998, it merged the enlisted radioman and data processing technician ratings, and in 1999 this new rating was dubbed the information systems technician.¹²⁰ In October 2001, the Navy created a new, restricted line specialization — information professional — to be filled by members of the fleet support officer community.¹²¹ However, individuals in these specializations continued to face limitations in career advance-

Because specialization was not typically a path to career advancement, the Army faced a shortage of technically deep personnel in the mid-1990s. This was one reason that the Army established a task force to redesign the officer personnel management system in 1996.

ment. Since warfare qualifications were important milestones for promotion, individuals specializing in fields related to computer networking or other areas of information warfare often spent time pursuing those qualifications rather than developing technical depth in their own field.¹²²

and control, and in this role, he co-authored a *Proceedings* article outlining the concept of “network-centric warfare.”¹¹⁸ Cebrowski and his co-author, John Garstka, technical adviser to the Command, Control, Communications and Computers Directorate, argued that computer networks were revolutionizing military affairs, but not because they were part of a new domain. Rather, just as computer networks were transforming U.S. business operations and making them more profitable and productive, computer networking should transform naval operations. The article advocated shifting from platform-centric operations (i.e., focusing on ships, submarines, and aircraft) to network-centric operations.

Importantly, Cebrowski and Garstka argued that this shift entailed elevating the status of individuals with particular technical talents, noting that “the military fails to reward competence” in information-based processes:

“Operator” status frequently is denied to personnel with these critical talents, but the value of traditional operators with limited acumen in these processes is falling, and ultimately they will be marginalized ... The services must both mainstream and merge those with technical skills and those with

Army: The Global Information Environment

Like the Air Force and Navy, the Army responded to the 1992 information warfare directive by reorganizing its intelligence units. Since the mid-1980s, the Army’s Intelligence and Security Command had maintained a highly classified Studies and Analysis Activity, which worked with other intelligence groups to explore ways of getting inside enemy command-and-control systems. In 1995, the Studies and Analysis Activity was absorbed into a new Land Information Warfare Activity, also within the Intelligence and Security Command. This activity began with 55 personnel, including 11 enlisted and roughly a dozen government civilians, and grew to about 250 by October 1997. The majority of the personnel were field-grade or higher-level officers from signals or intelligence. In the late 1990s, the Land Information Warfare Activity sought to incorporate more traditional operators, and it often augmented its technical capabilities by hiring

118 According to the article, the term was introduced by Chief of Naval Operations Adm. Jay Johnson in an address to the U.S. Naval Institute Annapolis Seminar and 123rd Annual Meeting on April 23, 1997, where Johnson described “a fundamental shift from what we call platform-centric warfare to something we call network-centric warfare.” Arthur K. Cebrowski and John H. Garstka, “Network-centric Warfare: Its Origin and Future,” *Proceedings* 124, no. 1 (January 1998): 28, <https://www.usni.org/magazines/proceedings/1998/january/network-centric-warfare-its-origin-and-future>.

119 Cebrowski and Garstka, “Network-centric Warfare.”

120 “Navy Information Systems Technician,” U.S. Navy, accessed Oct. 22, 2020, <https://www.navyjobs.com/navy-jobs/information-systems.html>.

121 “Establishment of Information Professional and Human Resources Officer Communities and Fleet Support Officer (FSO) Transition,” Chief of Naval Operations, July 25, 2001, <https://www.public.navy.mil/bupers-npc/reference/messages/Documents3/NAV2001/nav01182.txt>.

122 James Murphy, “Give Information Personnel More Training and Credibility,” *Proceedings* 134, no. 9 (September 2008), <https://www.usni.org/magazines/proceedings/2008/september/professional-notes>.

contractors, with one member recalling that it was half contractors at one point in its history.¹²³

Although the Land Information Warfare Activity was administratively within the Army's Intelligence and Security Command, it reported to the assistant chief of staff for operations and training rather than intelligence.¹²⁴ This helped to move what had primarily been an operations support function — intelligence — toward warfighting. But the Land Information Warfare Activity was explicitly in a supporting role. Like the Air Force Information Warfare Center and the Fleet Information Warfare Center, it helped commands plan information operations but did not conduct them. It deployed two kinds of teams: Field support teams would help Army units plan and integrate information warfare into their operations, while vulnerability assessment teams would help identify weaknesses.¹²⁵ In September 1996, the Land Information Warfare Activity also established the Army Computer Emergency Response Team, which engaged in defensive operations.¹²⁶

Like the Air Force, in the mid-1990s, the Army began to explicitly discuss computer network operations in its publications. Army "Field Manual 100-6: Information Operations," published in 1996, highlighted "database corruption" and "malicious software" as means of attacking information systems.¹²⁷ It also featured discussion of the Internet worm and Rome Labs breaches, which was excerpted in the Joint Doctrine for Command and Control Warfare, issued in February 1996.¹²⁸ The Army's "Field Manual 100-6" did not suggest that information comprised a new domain akin to land,

sea, and air, but focused on a "global information environment" that was undergoing rapid transformation due to "modern information technology" and the associated "explosive potential of rapid dissemination and use of information."¹²⁹

In 1998, the Army began creating a dedicated computer network operations force within Intelligence and Security Command's signals intelligence group, as discussed further below. However, the Army struggled to grow a computer network operations capability in the late 1990s because its personnel management system did not reward technical depth. The Army trained its officers to be generalist-leaders, with the expectation that technical work would be conducted primarily by enlisted personnel.¹³⁰ Because specialization was not typically a path to career advancement, the Army faced a shortage of technically deep personnel in the mid-1990s.¹³¹ This was one reason that the Army established a task force to redesign the officer personnel management system in 1996. The task force director, Gen. David Ohle, noted that with "information age technology, we see that officers have to be more specialized."¹³² He explained that he had been given "the mission to broaden the definition of warfighting to include not only combat, but also stability and support operations" as a means of improving opportunities for individuals outside of traditional warfighting roles.¹³³

In July 1997, the task force's final report noted the "propensity of promotion boards to select officers with a warfighting background (commonly referred to as the 'command track') over those possessing

123 My discussion of the Land Information Warfare Activity draws primarily on White, "Subcultural Influence on Military Innovation," 61–71.

124 White, "Subcultural Influence on Military Innovation," 64. For discussion of the Army's general staff structure, see "Field Manual 100-5: Staff Organization and Operations," Department of the Army Headquarters, May 31, 1997, <https://www.globalsecurity.org/military/library/policy/army/fm/101-5/f540.pdf>.

125 According to White, they viewed their work as "educational." White, "Subcultural Influence on Military Innovation," 62.

126 As noted previously, it appears that all of the services were involved in discussions about incident response by 1990, but the formalization of a coordinated incident response team came later. White cites a source that dates the formation of the Army Computer Emergency Response Team to September 1996. White, "Subcultural Influence on Military Innovation," 67. However, public announcements of the Army Computer Emergency Response Team only appeared in March 1997. Bryan Bender, "Army Stands Up Computer Security Coordination Center," *Defense Daily*, March 18, 1997; David L. Grange and James A. Kelley, "Victory through Information Dominance," *Army* 47, no. 3 (March 1997).

127 "Field Manual 100-6: Information Operations," U.S. Army, Aug. 27 1996, <https://www.hsdl.org/?view&did=437397>. The field manual broadened information operations to include civil and public affairs as well as command-and-control warfare, but did not expand the five elements of command-and-control warfare to include computer network operations.

128 "Joint Pub 13-13.1: Joint Doctrine for Command and Control Warfare," Joint Chiefs of Staff, Feb. 7, 1996, https://www.bits.de/NRANEU/others/jp-doctrine/jp3_13_1.pdf. Although "Field Manual 100-6" was not formally published until August 1996, this discussion is quoted in the joint doctrine issued in February 1996, suggesting that "Field Manual 100-6" was far along in its development earlier in that year.

129 "Field Manual 100-6: Information Operations," 1-1.

130 White discusses this problem, which continues to manifest today in the fact that the Army relies primarily on enlisted personnel rather than officers for its cyber operations, despite lower rates of success. Officers tend to have college degrees and thus are more likely to be better suited for cyber operations. However, they are encouraged to be generalists rather than specialists. White, "Subcultural Influence on Military Innovation," 46–48, 152–65.

131 Stephanie Ahern, "Breaking the Organizational Mold: Why the Institutional U.S. Army Has Changed Despite Itself since the End of the Cold War," Doctoral Dissertation, University of Notre Dame, 2009.

132 Mary Blake French, "OPMS XXI—an Integrated Strategy," *Army* 47, no. 2 (1997): 52.

133 French, "OPMS XXI—an Integrated Strategy," 50.



functional area skills.”¹³⁴ It recommended leaving intact the system for developing company-grade officers. But for the development of field-grade (major) or higher levels, it recommended creating four distinct career fields through which individuals could be promoted: operations, information operations, operations support, and institutional support.¹³⁵

Operations consisted of the Army’s 16 branches, including the Signal Corps and Military Intelligence Corps, and two functional areas: psychological operations and civil affairs and multifunctional logistics. The new information operations career field included two previously established functional areas — telecommunications engineering and information systems management — which were relevant to computer network operations. Information operations also included simulation, space operations, strategic intelligence, and public affairs — an eclectic mix. A new, seventh area was created for information operations generalists.¹³⁶ Unfortunately, this last area gained a reputation for mediocrity. It suffered from a lack of adequate training — information operations was a very broad field and the training regimen established for it was too short — and it tended to attract officers who were not excelling in any other specialization.¹³⁷

Although the revised Officer Personnel Management System formally provided a path to promotion for officers specializing in computer networking, this did not necessarily increase their cultural status. Senior officers continued to argue that people chose to specialize in a functional area simply because they couldn’t succeed in a warfighting branch.¹³⁸ Then, in 2006, a new Officer Personnel Management System eliminated the information operations career field, establishing only three broad career areas: maneuver, fire, and effects (previously operations); operations support; and operations sustainment. Most of the functional areas previously in the information operations field, including telecommunications engineering and information systems management, were placed

within operations *support*, reaffirming that even if individuals could advance professionally in these areas, they were playing a support role.¹³⁹

The Problem of Defense

By the late 1990s, the services were exploring various forms of computer network operations, but their formal doctrine and tactics, organizational hierarchies, and career structures still framed these activities as warfighting support rather than warfighting in its own right. Nonetheless, computer network operations were increasingly seen as the only “new” aspect of information warfare.

Additionally, as discussed further below, the mid-1990s saw a growing concern about one sense in which computer network operations were crucially different from other methods for information warfare: They depended upon civilian assets that the U.S. military could not control. This reliance made the problem of defense both more urgent and more difficult. In February 1994, the Joint Security Commission, which had been established by the secretary of defense and the director of central intelligence, described “the security of information systems and networks” as “the major security challenge of this decade and possibly the next century,” arguing that “there is insufficient awareness of the grave risks we face in this arena.” The commission noted the challenge of “protecting systems that are connected and depend upon an infrastructure we neither own nor control.”¹⁴⁰ A 1994 Defense Science Board task force echoed these concerns, noting that out of necessity “DoD [the Department of Defense] has tied its information systems to the private/commercial sector and routinely use [sic] INMARSAT, INTELSAT, EUROSAT, etc. Additionally, many DoD users are directly hooked to the INTERNET.”¹⁴¹ The task force was “persuaded that DoD is currently spending far too little on defensive IW [information warfare], and that the gravity and potential urgency

134 OPMS XXI Final Report, OPMS XXI Task Force, U.S. Department of the Army (July 1997), 5-1. <https://cgsc.contentdm.oclc.org/digital/collection/p4013coll11/id/1951/>

135 Maxwell S. Thibodeaux, “Organizing the Army for Information Warfare,” Strategy Research Project submitted in partial fulfillment of the requirements for the Master of Strategic Studies degree, U.S. Army War College, 2013, <https://apps.dtic.mil/dtic/tr/fulltext/u2/a590350.pdf>.

136 Thibodeaux, “Organizing the Army for Information Warfare.”

137 White, “Subcultural Influence on Military Innovation,” 78–79.

138 Ahern, “Breaking the Organizational Mold,” 117.

139 The exceptions were public affairs and information operations, which were moved to maneuver, fire, and effects. Ahern, “Breaking the Organizational Mold,” 390–91.

140 *Redefining Security: A Report to the Secretary of Defense and the Director of Central Intelligence*, Joint Security Commission, (Feb. 28, 1994), chap. 8 and chap. 1, <https://fas.org/sgp/library/jsc/>.

141 *Report of the Defense Science Board Summer Study Task Force on Information Architecture for the Battlefield*, Office of the Undersecretary of Defense for Acquisition and Technology (1994), 30, <https://www.hsdl.org/?abstract&did=464955>.

of the problem deserves [sic] redress.”¹⁴²

Articles in the trade press at the time also suggest that defense was not a major focus in the early 1990s. An August 1994 *Defense Daily* article noted that “[a]ll of the services’ information warfare tactics are currently focused more heavily on the offensive mission.”¹⁴³ Reporting on an Information Warfare Conference in October 1995, one technology journalist described “Pentagon skeptics who joke that information warfare is just ‘computer security with money.’”¹⁴⁴ As this suggests, computer security — a defensive activity — was seen as something that was different and less important than warfare.

Nonetheless, some military leaders worked to elevate the status of computer network defense.¹⁴⁵ As noted earlier, when Cebrowski became the director of the Joint Staff’s Command, Control, Communications and Computers Directorate in 1994, he established an information warfare division. Cebrowski brought in William Gravell, a captain in the Naval Security Group, to set it up. Gravell was not a technologist — he had entered the Naval Security Group through language training — but he had developed some important concepts in command, control, and communications countermeasures while assigned to the Office of the Chief of Naval Operations in the mid-1980s. There, he had also demonstrated to Cebrowski and others his ability to reduce highly technical subjects into compelling briefings.¹⁴⁶ A part of Gravell’s work, as head of the Joint Staff’s Information Warfare Division, was to persuade both military and private organizations to improve the security of computers and other information systems

upon which military operations depended. The division soon commissioned a comprehensive review of laws, policies, and initiatives related to defensive information warfare and produced several educational publications targeted at both the private sector and portions of the defense establishment.¹⁴⁷

As Gravell recalls, while he “was going to military commands and conferences, but also trade associations, conferences, [and] boards of directors,” trying “to drum up support” for defensive information warfare, he quickly concluded that “private sector organizations and their lawyers and stockholders did not want to hear that they were engaged in ‘warfare.’ Such associations threatened, and sometimes even stymied, the collaboration which was needed to secure military networks.”¹⁴⁸ Roger Callahan, a colleague from the National Security Agency, suggested that Gravell instead adopt the term “information assurance.” This term was seeing growing use among computer scientists seeking to broaden conceptions of information security beyond privacy, and the National Security Agency had recently changed the name of its Information Security Directorate to the Information Assurance Directorate.¹⁴⁹ By 1995, the Joint Staff’s Information Warfare Division had been officially renamed the Information Assurance Division.¹⁵⁰

In the Defense Department, information assurance was sometimes treated as synonymous with defensive information warfare.¹⁵¹ However, “information assurance” could also connote something that went beyond the military, as it was concerned with the vulnerability of critical infrastructure that the mili-

142 Report of the Defense Science Board Summer Study Task Force, 32.

143 Defense Daily, “Navy C4I Budget Safe for Now.”

144 Paul Constance, “From Bombs to Bytes: Era of On-line Weaponry Is Here,” *Government Computer News* 14, no. 21, (October 1995).

145 In January 1995, the Defense Information Systems Agency elevated its Center for Information Systems Security out of the Joint Interoperability Engineering Organization and made it the operating arm of a new Information Warfare Division. The center included a focus on reducing vulnerabilities within the Defense Department. For example, it aimed to develop a standardized information security training program for the Defense Department. It also continued to include operational aspects of defense, such as the Defense Department’s incident response team ASSIST, which was moved into the Defense Information Systems Agency’s Global Control Center. Vanessa Jo Grimm, “In War on System Intruders, DISA Calls In Big Guns,” *Government Computer News* 14, no. 3 (1995).

146 Gravell recalls a particularly well-received briefing to Chief of Naval Operations James Watkins in 1985. Cebrowski was present. Telephone interview with Gravell, May 22, 2020, and subsequent email correspondence.

147 See, e.g., *Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance*, 2nd Edition, The Joint Staff, Department of Defense, July 4, 1996, <https://nsarchive.gwu.edu/dc.html?doc=5989661-National-Security-Archive-Joint-Chiefs-of-Staff>.

148 Phone interview with Gravell, May 22, 2020.

149 For example, in 1993, computer scientist Fred Cohen discussed “information assurance” as something that means integrity and availability rather than simply confidentiality. Fred Cohen, *Planning Considerations for Defensive Information Warfare — Information Assurance*. Prepared for DISA Joint Interoperability and Engineering Organization (JIEO) Center for Information Systems Security, Dec. 15 1993, <http://all.net/books/iwar/index.html>. This is similar to the discussion in Defense Science Board, *Report of the Defense Science Board Task Force on Information Warfare-Defense (IW-D)* (November 1996), E-2–E-3.

150 Email correspondence with Gravell, July 20, 2020.

151 For example, the December 1996 Defense Department directive on information operations defined “information assurance” as “Information Operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation.” White, “Department of Defense Directive S-3600.1: Information Operations.” The equation of information assurance and defensive information warfare is explicit in an analysis commissioned by the Joint Staff’s Information Warfare Division. *Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance*, 1-1.

tary did not own or control.¹⁵² And even within the military, information assurance was sometimes seen as something focused more on technology management than warfighting, as noted below.

Despite the efforts of the Joint Staff's Information Assurance Division, the decentralized procurement and management of information technology posed challenges to information assurance.¹⁵³ Recognizing that "the complexity of managing DOD's [the Department of Defense's] information assurance efforts had increased due to the proliferation of networks across DOD and that its decentralized information assurance management could not deal with it adequately," the Information Assurance Task Force, led by the Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence and the Joint Staff's Information Assurance Division, began developing a more comprehensive and integrated approach in 1997.¹⁵⁴ This led to a Defense-Wide Information Assurance Program, which was launched by the assistant secretary of defense for command, control, communications and intelligence in his capacity as the Defense Department's chief information officer in January 1998.¹⁵⁵

The Defense-Wide Information Assurance Program aimed to combine "centralized oversight with decentralized execution" of information assurance activities.¹⁵⁶ But it was not given the authority or resources needed to fulfill its charter. Although the program was initially approved for between 30 and 34 personnel, by 2001 the greatest number of positions that had ever been filled at one time was 16. The Joint Staff, services, and other defense agencies were all directed to provide staff to the program, but there was no mechanism to enforce

these directives, and most of the staff were detailed from the National Security Agency and the Defense Information Systems Agency. In 2001, the Government Accountability Office found that while some Defense Department officials "expressed a need for products and activities" from the Defense-Wide Information Assurance Program, others "cited a lack of DOD [Department of Defense] leadership and support for DIAP [the Defense-Wide Information Assurance Program] and stated that individual components should continue to manage their own IA [Information Assurance] activities without DIAP involvement."¹⁵⁷

Ultimately, elevating the status of computer network defense required more than an information assurance program from the Defense Department's chief information officer. The path to elevating computer network defense to the level of warfighting went through the Joint Staff's Operations Directorate.

The Need for a Joint Operational Defense

In 1997, the Joint Staff's annual no-notice interoperability exercise, known as Eligible Receiver, included a computer network intrusion for the first time. The intrusion was proposed by Minihan, who, as noted earlier, had become familiar with the potential impact of computer hacking on military operations as director of the Air Intelligence Agency. However, in subsequent positions as the Air Force's assistant chief of staff for intelligence and then as the director of the Defense Intelligence Agency, he struggled to persuade others to take computer security seriously. When Minihan became director of the National Security Agency in February 1996, he finally had the chance to demonstrate the problem

152 For example, in his 1996 congressional testimony, Deputy Secretary of Defense John White explained that "information assurance ... goes beyond what we traditionally think of as computer or information security" and "is not the realm of just security specialists," but rather "is the responsibility of all who plan operations, manage enterprises, and are responsible for the delivery of critical infrastructure services." See "Security in Cyberspace," 418. Information assurance was thus directly related to the increasingly visible problem of critical infrastructure protection. See, for example, discussion in Kaplan, *Dark Territory*.

153 By 1997, a report for the assistant secretary of defense for command, control, communications and intelligence noted that "the complexity of managing DOD's information assurance efforts had increased due to the proliferation of networks across DOD and that its decentralized information assurance management could not deal with it adequately." Quote in Li, "DOD's Information Assurance Efforts," 4.

154 Quote is the summary of a November 1997 report from the assistant secretary of defense for command, control, communications and intelligence, found in Li, "DOD's Information Assurance Efforts," 4. The interim report of the task force was presented on Jan. 27, 1997, and the final report, "Improving Information Assurance: A General Assessment and Comprehensive Approach to an Integrated IA Program for the Department of Defense," is dated March 1997. These latter two documents are described in J.V. Gray, *Information Operations: A Research Aid*, Institute for Defense Analysis, September 1997, 31.

155 In response to fiscal years 1999–2003 planning guidance, the assistant secretary of defense for command, control, communications and intelligence developed "A Management Process for a Defense-wide Information Assurance Program (DIAP)," published Nov. 15, 1997. See Li, "DOD's Information Assurance Efforts," 4, note 3. The assistant secretary of defense for command, control, communications and intelligence was made the Defense Department chief information officer in response to the 1996 Clinger-Cohen Act, which required that all federal agencies appoint a chief information officer and use performance-based management to oversee information technology acquisition and use.

156 *Serious Weaknesses Continue to Place Defense Operations at Risk*, Government Accountability Office, Aug. 26, 1999, 15, <https://www.gao.gov/products/GAO/AIMD-99-107>.

157 *Information Security: Progress and Challenges to an Effective Defense-wide Information Assurance Program*, Government Accountability Office, March 30, 2001, 22.

persuasively by including computer network attack in Eligible Receiver.¹⁵⁸

In June 1997, as part of the exercise, a National Security Agency red team comprised of about 25 personnel successfully broke into the computer systems of the U.S. Pacific Command, the National Military Command Center, and a number of other joint command facilities. Eligible Receiver was set to run for two weeks, with an additional two weeks set aside if necessary, but the National Security Agency red team was so successful that it ended after just four days.¹⁵⁹

The Joint Staff had assigned a new Division for Information Operations to monitor the exercise around the clock and make recommendations. The division was spun off from the Joint Staff's Operations and Plans Division and was headed by Brig. Gen. John "Soup" Campbell, an Air Force fighter pilot. Campbell recalls that, after a few weeks of gathering observations and recommendations, his group began to brief the Joint Staff's director of operations, Gen. Peter Pace. It quickly became clear that the recommendations were directed to organizations that "were scattered all over the map" and that no single organization could be given primary responsibility for implementing them.¹⁶⁰ Pace ended the meeting early and sent the briefers off to figure out who should lead the effort to remediate the problems identified by Eligible Receiver.

Representatives of three directorates in the Joint Staff — intelligence; operations; and command, control, communications, and computers — and the Defense Information Systems Agency joined the operations deputies of each of the services in exploring who should be in charge. By November of 1997, the services' operations deputies were considering several possible organizational structures, including augmenting the Information Operations Response Cell (a group led by the Joint Staff's Division for Information Operations), or assigning the task to an existing military command or an agency such as the Defense Information Systems Agency or the National Security Agency.¹⁶¹ However, Campbell recalls

"resistance from the Services who didn't want any outside agency telling them how to run their networks, and having a Combat Support Agency (e.g. DISA [the Defense Information Systems Agency] or NSA [the National Security Agency]) do so was a non-starter."¹⁶² Campbell and others eventually concluded that they should establish a new task force to direct computer network defense. They also recognized the importance of making sure that the task force would be "doctrinally correct," so that it would have proper authorities.¹⁶³

Efforts to establish the task force were made more urgent by the discovery of new intrusions. On Feb. 3, 1998, monitors at the Air Force's Information Warfare Center noticed an intrusion at Andrews Air Force base, just outside Washington, D.C. Within a few days, a task force that included members of the Joint Staff's Information Operations Directorate, the FBI, the Defense Information Systems Agency, and the National Security Agency were investigating. After determining that the hackers had exploited a known vulnerability in its operating systems, known as Sun Solaris 2.4 and 2.6, the operation was dubbed "Solar Sunrise."¹⁶⁴ Further investigation determined that the hackers were a couple of teenagers in the suburbs of San Francisco who were getting help from an 18-year-old hacker in Israel. By the end of the month, they had all been arrested by the authorities in their respective governments.¹⁶⁵ Nonetheless, the breach demonstrated the ease with which the military's information systems could be compromised.

Not long after the discovery of Solar Sunrise, Deputy Secretary of Defense John Hamre called a meeting of about 30 people in the Pentagon. He asked the same question that had been looming since Eligible Receiver: Who's in charge? Recounting the meeting 14 years later, Campbell stated that he couldn't recall "if I raised my hand or if somebody poked me and I jumped," but as the director of the Joint Staff's Information Operations Division ("the J-39 Bubba"), he became the answer to Hamre's question.¹⁶⁶ Eventually Campbell became the

158 Kaplan, *Dark Territory*.

159 Kaplan, *Dark Territory*, 68. Kaplan states that "the entire defense establishment's network was penetrated" in four days, though the video briefing by the National Security Agency red team targeting officer Keith Abernethy indicates that one target was denied to the team.

160 Email to author from John Campbell, Sept. 28, 2020.

161 "DOD Organization for Computer Network Defense: Summary of Proposals," Joint Chiefs of Staff, Slide 4, June 1998, National Security Archive, <https://nsarchive.gwu.edu/dc.html?doc=6168257-National-Security-Archive-Joint-Chiefs-of-Staff>. Kaplan states that the Information Operations Response Cell was formed shortly before Solar Sunrise, but slides showing the timeline for discussion of options for computer network defense show it starting earlier. Campbell recalls that it was established before Eligible Receiver. Email to author from Campbell, Sept. 28, 2020.

162 Email to author from Campbell, Sept. 28, 2020. Emphasis in original.

163 Email to author from Campbell, Sept. 28, 2020.

164 Kaplan, *Dark Territory*, 74.

165 Kaplan, *Dark Territory*, 78.

166 Atlantic Council, "Transcript: Lessons from our Cyber Past."

Eligible Receiver demonstrated the need for improvements in both mitigating vulnerabilities and responding to threats. Some of the vulnerabilities were about poor security awareness and training: Personnel at targeted units gave out their passwords over the phone or left them in the trash to be discovered by dumpster divers.

commander of the new Joint Task Force-Computer Network Defense that the Information Operations Division was helping to organize.

By May 1998, two different proposals for the new task force were under consideration: It could be in San Antonio with the Joint Command and Control Warfare Center or it could be located in the Defense Information Systems Agency's facilities in Washington D.C.¹⁶⁷ At a meeting in May 1998, the services' deputy secretaries for operations endorsed the San Antonio option.¹⁶⁸ But subsequently, Defense Information Systems Agency Director and Army Lt. Gen. David Kelley made a strong case for locating the new unit at his agency. He offered the new task force use of the agency's Global Network Operations and Security Center, a sophisticated facility with network monitoring capabilities. This was a "big piece" of why ultimately the Joint Task Force-Computer Network Defense was established there, where it could leverage the agency's technical expertise.¹⁶⁹

What Does an Operational Computer Network Defense Do?

But what exactly would the new task force do? The answer to this question was shaped not only by analysis of the results of Eligible Receiver, but also by distinctive conceptions of the kinds of expertise and work that might constitute "warfighting."¹⁷⁰

Eligible Receiver demonstrated the need for improvements in both mitigating vulnerabilities and responding to threats. Some of the vulnerabilities were about poor security awareness and training: Personnel at targeted units gave out their pass-

words over the phone or left them in the trash to be discovered by dumpster divers. Other vulnerabilities were well-known technological weaknesses that nonetheless remained unmitigated. Threat-oriented defenses had also failed. In an after-action report on Eligible Receiver, the National Security Agency red team targeting officer noted that intrusion detection systems had worked well, but reporting on intrusions came two weeks late: "They now know that the horse is out of the barn after it burned down and the ashes are cold."¹⁷¹ He concluded, "We tend to fight everything by throwing technology and money at it and not spending the time it takes to get the people to learn how to use it effectively."¹⁷²

These weaknesses suggested that the new computer network defense task force needed to address both vulnerability mitigation and threat response. And indeed, representatives from the Defense Information Systems Agency and the Joint Staff's Command, Control, Communications, and Computing Directorate argued that the task force should include vulnerability assessment, red teaming, and other kinds of work to prevent successful intrusions.¹⁷³ However, according to an October 1998 background paper by Air Force Capt. Jay Healey, an intelligence officer in the Air Staff, efforts to prevent intrusions "are not part of the JTF's [Joint Task Force's] computer network warfighting role and have been strongly resisted by the Services."¹⁷⁴ In a later briefing, Healey described computer network defense as outward-focused, engaging enemies, active, and requiring operational expertise. By contrast, he depicted information assurance as inward-focused, not engaging enemies, passive,

167 In the San Antonio option, the task force would consist of 23 members of the Joint Command and Control Warfare Center and 20 members of the Air Force's Information Warfare Center, with nine representatives drawn from the Defense Information Systems Agency and the Army's and Navy's computer emergency response teams. With the Defense Information Systems Agency option, it would consist of 29 members, four of which were already at that agency. This option would be less expensive and would allow for ready coordination with related agencies in Washington, but would require more personnel to be identified prior to startup.

168 Joint Chiefs of Staff, "DOD Organization for Computer Network Defense," Slide 4.

169 Atlantic Council, "Transcript: Lessons from our Cyber Past."

170 Some documents related to Eligible Receiver, including an after-action report summarizing the major lessons of the exercise, have been declassified and are available at the Digital National Security Archive as part of an electronic briefing book. Michael Martelle, ed., "Eligible Receiver 97: Seminal DOD Cyber Exercise Included Mock Terror Strikes and Hostage Simulations," Department of Defense, Briefing Book no. 634, Aug. 1, 2018, <https://nsarchive.gwu.edu/briefing-book/cyber-vault/2018-08-01/eligible-receiver-97-seminal-dod-cyber-exercise-included-mock-terror-strikes-hostage-simulations>. Other weaknesses revealed by Eligible Receiver are based on interviews conducted by Fred Kaplan and reported in his book, *Dark Territory*.

171 "Eligible Receiver '97 After Action Report," in Martelle, ed., "Eligible Receiver 97." Also available on YouTube: "Eligible Receiver '97 After Action Report," YouTube, accessed Dec. 22, 2020, <https://youtu.be/iI3iZAqONh0>.

172 YouTube, "Eligible Receiver '97 After Action Report," at 9:40. Interestingly, the exercise also demonstrated the potential *effectiveness* of operational defenses: One marine at Pacific Command had recognized an intrusion underway and reconfigured his firewall to shut out the red team. As a result, Abernethy reported, "a major strategic target ... was denied to us." YouTube, "Eligible Receiver '97 After Action Report," at 8:40.

173 Jay Healey, "Bullet Background Paper on Computer Network Defense-Joint Task Force (CND-JTF)," Office of the Deputy Chief of Staff for Air and Space Operations, Oct. 14, 1998, 3, <https://nsarchive.gwu.edu/dc.html?doc=6168259-National-Security-Archive-Captain-Healey-US-Air>. Emphasis in original.

174 Healey, "Bullet Background Paper." Emphasis in original.

and requiring network management expertise.¹⁷⁵ Consistent with the services' preference for a war-fighting focus, Healey noted that the task force would be "staffed mostly by traditional operators (pilots, combat arms, etc.), relying on DISA [the Defense Information Systems Agency] for technical comm-computer expertise."¹⁷⁶ Specifically, the task force was projected to consist of 19 billets, 10 of which were dedicated to operations, four to communications, and five to intelligence.¹⁷⁷

This tiny task force functioned by leveraging technological expertise within the Defense Information Systems Agency and the services, as well as contractors. By 2000, it was composed of about one-third contractors, one-third military personnel, and one-third government civilian personnel.¹⁷⁸ The services were each tasked with designating component forces and an associated commander that the Joint Task Force would have authority to coordinate and direct. Consistent with the emphasis on responding to threats, each of the services drew on its computer emergency response teams and information warfare units from its respective intelligence organizations.¹⁷⁹ The Defense Department's computer emergency response team was also placed under the Joint Task Force-Computer Network Defense.¹⁸⁰

The operational focus was partly driven by the need to persuade warfighters of the value of this new activity. As Campbell recalls:

[I]f you're going to have any credibility with the war fighters, you had to have operation-

al people... . We thought the best approach was to start with people who had some credibility in the operational side of the house, and then provide them with training and additional help that they needed to be technically proficient.¹⁸¹

For example, some members of the task force took courses provided by James Madison University, which, in May 1999, was certified by the National Security Agency as one of seven initial Centers of Academic Excellence in Information Assurance.¹⁸²

Although the Joint Task Force-Computer Network Defense was initially chartered as a defensive organization, by January 1999, the Joint Chiefs of Staff had agreed that it would become part of U.S. Space Command and that it would integrate both offensive and defensive operations.¹⁸³ The task force remained physically co-located at the Defense Information Systems Agency, and the commander of the joint task force was made its vice director, allowing the task force to leverage the technical expertise at the agency. But members of the task force continued to distinguish their work from the technical support focus of the Defense Information Systems Agency. In October 1999, Army Col. Larry Frank, the chief of the task force's operations division, asserted, "We bring an operational focus" to defense and "We don't fix computers."¹⁸⁴

The joint task force's charter in December 1998 made it "responsible for coordinating and directing the defense of the Department of Defense's computer systems and computer networks," a po-

175 "Organizing for Information Warfare: An Air Staff Perspective," U.S. Air Force Office of the Director of Intelligence, Surveillance, and Reconnaissance, 1999, slide 25, <https://nsarchive.gwu.edu/dc.html?doc=6168263-National-Security-Archive-US-Air-Force-Office-of>. Jay Healey confirmed that he was the author of this presentation in an email to the author dated May 15, 2020.

176 Healey, "Organizing for Information Warfare," slide 2.

177 Jay Healey, "JTF Computer Network Defense Update," U.S. Air Force Office of the Director of Intelligence, Surveillance, and Reconnaissance, October 1998, slide 17, <https://nsarchive.gwu.edu/dc.html?doc=6168258-National-Security-Archive-US-Air-Force-Office-of>.

178 Atlantic Council, "Transcript: Lessons from our Cyber Past."

179 Specifically, the Army's component was the Army Computer Emergency Response Team Coordination Center, directed by Land Information Warfare Activity. The Air Force's component was the Air Force Computer Emergency Response Team under the command of the Air Force Information Warfare Center. And the Navy formed a 14-person task force at the Naval Computer and Telecommunications Command, which worked in coordination with the Fleet Information Warfare Center and Navy Computer Incident Response Team. Marines also formed a new force. Each contribution to the Joint Task Force-Computer Network Defense is described in articles in the Fall 1999, Volume 2, Number 3 edition of *Information Assurance*, a newsletter for information assurance technology professionals published by the Information Assurance Technology Analysis Center within the Defense Information Systems Agency. See <https://assets.documentcloud.org/documents/5798613/National-Security-Archive-Information-Assurance.pdf>.

180 The organization of the Joint Task Force for Computer Network Defense can be found in John H. Campbell, "Computer Network Defense: Computer Network Defense Update to the Defense Science Board," National Security Archive, Jan. 18, 2000, slide 13, <https://nsarchive.gwu.edu/dc.html?doc=3145117-Document-03>.

181 Atlantic Council, "Transcript: Lessons from our Cyber Past."

182 "NSA Designates First Centers of Academic Excellence in Information Assurance Education," National Security Agency, Release No. PA-224-18, May 11, 1999, <https://www.nsa.gov/news-features/press-room/Article/1636090/nsa-designates-first-centers-of-academic-excellence-in-information-assurance-ed/>.

183 Healey, "Organizing for Information Warfare," slide 6.

184 Dan Verton, "DOD Boosts IT Security Role," *Federal Computer Week*, Oct. 3, 1999, <https://fcw.com/articles/1999/10/03/dod-boosts-it-security-role.aspx>.

tentially enormous range of activities.¹⁸⁵ However, many vulnerability mitigation activities were effectively delegated to the Defense Information Systems Agency or the services' communications organizations. For example, the Defense Information Systems Agency developed the Information Assurance Vulnerability Alert process, wherein all of the Defense Department's systems administrators were required to receive, acknowledge, and report on their compliance with vulnerability alerts.¹⁸⁶

Nonetheless, in briefings before Congress, Campbell explicitly included red teaming and the Information Assurance Vulnerability Alert process within the category of "operations," alongside the Joint Task Force-Computer Network Defense. As this suggests, the concept of computer network operations was beginning to broaden, despite the task force's threat-oriented focus. And yet, this expanding concept of operations still excluded certain forms of vulnerability mitigation, such as training and certifying systems administrators and users.¹⁸⁷

The Rising Status of Joint Cyber Operations and Service Responses

Computer network operations, both defensive and offensive, grew in influence, size, and authority in the 20 years following the establishment of the Joint Task Force-Computer Network Defense. That task force became the Joint Task Force-Computer Network Operations in 2000, when it assumed responsibility for both offensive and defensive operations.¹⁸⁸ After the terrorist attacks of Sept. 11, 2001, operations in Afghanistan and Iraq underscored the importance of defense. Thus, in 2004, the joint task force was returned to its initial defensive focus, with the new name, the Joint Task Force-Global Network Operations.¹⁸⁹ Offensive operations were moved to

a new Joint Functional Component Command-Network Warfare within the National Security Agency. Both defensive and offensive components were commanded by Strategic Command, which had taken over several functions of Space Command when the latter dissolved in 2002.¹⁹⁰

But the Joint Task Force-Global Network Operations did not discover the first known breach of classified U.S. military networks in October 2008. Instead, it was the National Security Agency's Information Assurance Directorate that first detected the problem and within a day had devised a software solution to neutralize it (although implementing that solution across all of the Defense Department's networks would take well over a year).¹⁹¹ The National Security Agency's rapid response to the problem — code-named "Buckshot Yankee" — bolstered its case for unifying computer network attack and defense under the agency's authority. In June 2009, Secretary of Defense Robert Gates announced the formation of U.S. Cyber Command, a unified command under Strategic Command that merged the Joint Task Force-Global Network Operations and the Joint Functional Component Command-Network Warfare. He also announced his intention to make the director of the National Security Agency dual-hatted as a four-star commander of U.S. Cyber Command.¹⁹² After decades of arguing for the importance of computer network operations, leaders in the intelligence community had finally gained the authority of a combatant command.

The services were all instructed to designate component commands, which were expected to be three-star commands. Additionally, in late 2012, U.S. Cyber Command began establishing standard training requirements to be used in building cyber mission forces — some 133 teams. These teams would be comprised of more than 6,200 personnel and would support Cyber Command's three

185 Campbell, "Computer Network Defense," slide 10.

186 For a discussion of this process, including questions about the role that the Joint Task Force-Computer Network Defense should play in it, see Department of Defense Inspector General, *DoD Compliance with the Information Assurance Vulnerability Alert Policy*, Department of Defense, Office of Inspector General, Dec. 1, 2000, <https://www.dodig.mil/reports.html/Article/1116364/dod-compliance-with-the-information-assurance-vulnerability-alert-policy/>.

187 Senate Armed Services Committee, "Department of Defense Authorization for Appropriations for Fiscal Year 2001 and the Future Years Defense Program," 19. In this testimony, Campbell presented "operations" as one part of "defense-in-depth," along with technology and people. Certifying systems administrators and users was in the "people" category, not "operations."

188 Senate Armed Services Committee, "Department of Defense Authorization for Appropriations for Fiscal Year 2001 and the Future Years Defense Program," 42.

189 Atlantic Council, "Transcript: Lessons from our Cyber Past."

190 For an overview of the evolution of the Joint Task Force-Computer Network Defense into U.S. Cyber Command, see "U.S. Cyber Command History," U.S. Cyber Command, accessed Oct. 21, 2020, <https://www.cybercom.mil/About/History/>.

191 Kaplan, *Dark Territory*, 180–85; Ellen Nakashima, "Cyber-intruder Sparks Response, Debate," *Washington Post*, Dec. 8, 2011, https://www.washingtonpost.com/national/national-security/cyber-intruder-sparks-response-debate/2011/12/06/gIQAxLuFgO_story.html; and William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89, no. 5 (September/October 2010): 97, <https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain>.

192 Robert Gates, "Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations," Memoranda, Department of Defense, June 23, 2009, <https://fas.org/irp/doddir/dod/secdef-cyber.pdf>.



primary missions: defending Defense Department networks, supporting combat operations, and defending the United States from cyber attacks with national security implications.¹⁹³

The following sections show how the elevation of joint computer network operations galvanized the services to elevate the professional and organizational status of computer network expertise. This process was slow and difficult because it entailed reorganizing existing organizations, career fields, and training programs — particularly those associated with signals intelligence and communications — to give them greater warfighting status. Ultimately, some kinds of expertise, particularly threat-oriented expertise that tended to reside within signals intelligence communities, were more readily promoted into an operational role than the technology-oriented expertise of communications and computing communities.

Air Force: Transforming Communications into “Operations”

Just as in the 1990s, the Air Force remained the most eager of the services to establish cyberspace as a warfighting domain. In November 2005, it revised its mission statement to include “to fly and fight in air, space and cyberspace.”¹⁹⁴ In 2006, the Air Force also began to centralize its acquisition and management of computer networking, recognizing that many of its vulnerabilities resulted from decentralization and the associated lack of enforcement of strong security standards.¹⁹⁵

However, the Air Force Communications Agency was not put in charge of centralizing computer networking. Instead, in July of 2006, the Air Force established a new Network Operations Command under the 8th Air Force — the previous home of the 609th Information Warfare Squadron — with-

193 DOD Training: U.S. Cyber Command and Services Should Take Actions to Maintain a Trained Cyber Mission Force, U.S. Government Accountability Office, March 6, 2019, <https://www.gao.gov/products/GAO-19-362>.

194 Elaine M. Grossman, “Sovereign Options: Say What? Air Force Mission Statement Leaves Many Officials, Experts, Baffled,” *Inside the Air Force* 16, no. 50 (Dec. 16, 2005): 8–11, <https://www.jstor.org/stable/24794921>. This announcement was criticized by many, including people who saw it as a power grab.

195 Maryann Lawlor, “Command Takes Network Control,” *Signal* (October 2006), <https://www.afcea.org/content/command-takes-network-control>. As this article noted, “vulnerabilities that exist in the Air Force’s networks are the result of more than a decade of individual commands and bases acquiring individual technologies that met their own needs.”

in Air Combat Command.¹⁹⁶ At the same time, the 67th Information Operations Wing, which, as noted previously, inherited many of the tasks assigned to the 609th squadron, was renamed the 67th Network Warfare Wing. Its responsibilities were explicitly expanded to include attack, and its defensive role also increased as the wing took control of network operations and security centers that had previously been dispersed across 10 different locations, serving 17 different units.¹⁹⁷

In November 2006, the Air Force announced plans to establish a major cyberspace command under the 8th Air Force “that stands alongside Air Force Space Command and Air Combat Command.”¹⁹⁸ The Air Force also began planning for a new career field that would “ensure a full career with full opportunities for advancement to the highest ranks of the Air Force.”¹⁹⁹ The new field would draw on specializations within four existing fields: communications, intelligence, electronic warfare, and space.²⁰⁰

However, these plans slowed significantly after 2007, when nuclear mismanagement led to the 8th Air Force being put in charge of all nuclear operations and nothing else, leaving the proposed command without a home.²⁰¹ The Air Force nonetheless established the headquarters of Air Force Cyber Command (Provisional), which began planning for a more permanent home for the Air Force’s cyber command.²⁰² In 2008, the provisional command proposed creating a three-star command consisting of a headquarters, a numbered Air Force, and four wings: the 67th Network Warfare Wing; 688th Information Operations Wing (which had evolved

from Air Force Information Warfare Center); 689th Cyber Wing (a reactivated unit that had been retired when the Air Force Communications Command was demoted to a field operating agency); and a new 450th Electronic Warfare Wing.²⁰³ In 2009, the Air Force followed through on this proposal by activating the 24th Air Force/Air Forces Cyber as a three-star command under Space Command, which would also serve as the Air Force component to U.S. Cyber Command.²⁰⁴ Additionally, the Air Force Communications Agency was put under Space Command and renamed the Air Force Network Integration Center so that it could better support the 24th Air Force.²⁰⁵

Thus, the Air Force built its operational Cyber Command upon the earlier work of intelligence organizations — particularly the 67th Network Warfare Wing and the 688th Information Operations Wing — while keeping communications organizations in a support role. However, when the Air Force finally established a new cyber operations career field, it drew most heavily on the communications career field. This was not because such personnel were seen as the natural operators, but because Air Force Combat Command was unwilling to surrender its electronic warfare personnel to the new field and the Air Force Intelligence, Surveillance and Reconnaissance Agency (formerly the Air Intelligence Agency) was unwilling to lose personnel to a field that it would not control. By contrast, computing-communications personnel were eager to raise their status by becoming the core of a new career field in cyber operations.²⁰⁶

On April 30, 2010, the entire communications and

196 Lawlor, “Command Takes Network Control.”

197 Lawlor, “Command Takes Network Control.”

198 Michael W. Wynne, “Cyberspace as a Domain in Which the Air Force Flies and Fights,” Remarks to the C4ISR Integration Conference, Crystal City, VA, Nov. 2, 2006, <https://www.airforcemag.com/PDF/SiteCollectionDocuments/Reports/2006/November/Day03/Wynne110206.pdf>.

199 Wynne, “Cyberspace as a Domain.”

200 White, “Subcultural Influence on Military Innovation,” 222.

201 Specifically, on Aug. 30, 2007, a munitions crew at Minot Air Force Base in North Dakota mistakenly loaded six nuclear missiles onto a B-52. The error was discovered only after the B-52 had flown the missiles to Barksdale Air Force Base in Louisiana and had been parked for about nine hours without any special guards. Peter Grier, “Misplaced Nukes,” *Air Force Magazine*, June 26, 2017, <https://www.airforcemag.com/article/misplacednukes/>.

202 Approximately 55 percent of the staff in the provisional command came from the Air Force Communications Agency. Markus Rogers, “Air Force Network Integration Center’s Journey to Consolidated Cyber Capabilities,” *CHIPS*, May 14, 2019, <https://www.doncio.navy.mil/CHIPS/Article-Details.aspx?ID=12434>.

203 The organization is shown in William T. Lord, “USAF Cyberspace Command: To Fly and Fight in Cyberspace,” *Strategic Studies Quarterly* 2, no. 3 (Fall 2008): 5–17, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-02_Issue-3/Lord.pdf. For more on the 689th Cyber Wing (subsequently called the Combat Communications Wing) see “689 Combat Communications Wing (AFSPC),” Air Force Historical Research Agency, Nov. 24, 2010, <https://web.archive.org/web/20140512213403/http://www.afhra.af.mil/factsheets/factsheet.asp?id=15897>.

204 Initially, the 24th Air Force was named Air Forces Strategic. This changed in 2010. Scott McNab, “24th AF Becomes AFCYBER,” U.S. Strategic Command, Dec. 9, 2010, <https://www.stratcom.mil/Media/News/News-Article-View/Article/983649/24th-af-becomes-afcyber/>.

205 Katherine Kebisek, “Behind the Scenes: Air Force Network Integration Center Shapes the Future of Air Force Cyberspace Operations,” Air Force Space Command, Nov. 17, 2010, <https://www.afspc.af.mil/News/Article-Display/Article/250078/behind-the-scenes-air-force-network-integration-center-shapes-the-future-of-af/>.

206 These developments are described in White, “Subcultural Influence on Military Innovation,” 251–52.

information officer field, which included over 3,000 officers, changed to a new cyberspace officer field.²⁰⁷ This marked an explicit shift from a support field to an operational field, but many legacy support functions remained.²⁰⁸ The cyberspace and information officer field quickly became a very broad career field that included both vulnerability reduction roles (e.g., DODIN operations) and threat-oriented roles (e.g., offensive and defensive cyber operations).²⁰⁹ Personnel could also enter cyberspace operations through intelligence specializations.²¹⁰

However, Air Force officers continue to view threat-oriented roles as preferable to vulnerability-oriented roles, by virtue of their greater warfighting status. For example, in 2013, 1st Lt. Robert Lee, a cyber team leader in the Air Force Intelligence, Surveillance, and Reconnaissance Agency, argued against categorizing the roles of establishing, maintaining, and overseeing networks as “operations,” i.e., warfighting. He recognized that these vulnerability-oriented roles were very important, and “maybe even more important than a defense operator’s role when done correctly.” But he insisted on differentiating them from operational defense: “Applying vendor-issued software patches is not defense; it is maintenance.”²¹¹ Lee argued that combining these different kinds of activities into a single career field, with a single training pipeline, undermined the Air Force’s ability to develop both kinds of expertise.

Similarly, in a recent survey of the Air Force’s cyberspace operations officers (17D), one officer asserted that “all 17Ds should be executing cyber operations, whether on the offensive line or defending a weapon system. Not supporting and

maintaining.”²¹² Another criticized senior Air Force leadership for not understanding “that cyberspace operations = maintaining the network, i.e., email.”²¹³ Yet another argued that they were “making ‘support’ and ‘maintenance’ dirty words by calling everything ‘operations,’ and the true operational community sees that a huge portion of what we do is support or maintenance, and our marketing campaign costs us credibility.” This officer argued for the need to both be honest with officers in this field about the kind of work they would probably be doing and to build “understanding and appreciation for how critical cyber support and maintenance are for EVERY other mission area.”²¹⁴

Navy: Organizing an Information Warfare Community

The Navy began consolidating its computer networks even earlier than the Air Force, recognizing significant inefficiencies and vulnerabilities associated with decentralization. In October 2000, it awarded a contract for the development of the Navy Marine Corps Intranet, which would merge up to 200 different networks, many of which were not interoperable, into a single seamless network.²¹⁵ By 2004, the Navy intranet had reduced the number of distinct applications from 90,000 to 10,000. The secretary of the Navy noted that the “most deficient aspect” of legacy information technology was insecurity, acknowledging that it “was insecure because we bought it and built it that way.”²¹⁶ This was a management as well as an acquisition problem: “It wasn’t just that we weren’t following our own rules; in many cases we weren’t even aware

207 This field was labeled 17D. Golembiewski, “From Signals to Cyber.” Additionally, on Nov. 1, 2009, roughly 43,000 enlisted and 8,800 civilian personnel in communications fields were transitioned into a new cyberspace support career field, the 3DXXX series. Rita Boland, “Military Branch Undertakes Massive Troop Conversion,” *Signal*, Feb. 2, 2010, <https://www.afcea.org/content/military-branch-undertakes-massive-troop-conversion>.

208 In the Air Force, the first digit of the Air Force Specialty Code indicates the career group, with “3” indicating a support field and “1” indicating an operational field. For more on legacy support functions, see Katrina A. Terry, “Overcoming the Support Focus of the 17D Cyberspace Operations Career Field,” Master’s Thesis, Air Force Institute of Technology, 2011.

209 Initially, the Air Force created two “shreds” of the 17D field, one for cyberspace operators (17DXA) and another for network maintainers (17DXB). Less than 10 percent of the officers initially fell into the “operator” shred, but training for these shreds was similar and officers were rotated through the different roles. This was criticized in a 2015 paper which noted that “[t]he Air Force cannot cultivate a war-fighting culture in cyberspace operations if officers in the mission area are treated like a first-grade soccer team where ‘everybody needs an opportunity’ to play.” Matthew T. Hyland, “Operationalizing the 17D Workforce,” in *Cyber Compendium: Professional Continuing Education Course Papers 2*, no. 1, ed. Robert Mills (Wright-Patterson Air Force Base, OH: Air Force Institute of Technology, 2015), <https://apps.dtic.mil/dtic/tr/fulltext/u2/a617022.pdf>. Today, officers in the 17D career field are typically assigned to defending the DODIN — which, as noted earlier, focuses on maintenance and sustaining functions — but some receive additional training for 17S assignments, which are typically offensive or defensive cyber operations and are seen as more desirable. Chaitra M. Hardison et al., *Attracting, Recruiting, and Retaining Successful Cyberspace Operations Officers* (Santa Monica, CA: RAND Corporation, 2019), https://www.rand.org/pubs/research_reports/RR2618.html.

210 These include intelligence officers, fusion analysts (an enlisted specialization), and cyber warfare operations enlisted personnel. White, “Subcultural Influence on Military Innovation,” 239–42.

211 Robert M. Lee, “The Failing of Air Force Cyber,” *Signal*, Nov. 1, 2013, <https://www.afcea.org/content/failing-air-force-cyber>.

212 Hardison et al., *Attracting, Recruiting, and Retaining*, 57.

213 Hardison et al., *Attracting, Recruiting, and Retaining*, 56.

214 Hardison et al., *Attracting, Recruiting, and Retaining*, 56.

215 George I. Seffers, “Navy Intranet Sets Sail,” *Federal Computer Week*, Oct. 16, 2000.

216 Anderson, “Why We Need the Navy Marine Corps Intranet.”

of them.”²¹⁷ The Navy also greatly underestimated the complexity of its networks, which slowed the deployment of the intranet considerably. Efforts to speed up the process alienated many of the system’s users and created problems. Nonetheless, by 2006, the Navy Marine Corps Intranet had consolidated over 1,000 legacy networks and had greatly improved security.²¹⁸

The Navy also centralized security management by consolidating commands responsible for communications and computing. In 2001, it merged the Naval Computer and Telecommunications Command with the Task Force-Navy Marine Corps Intranet, forming a new Naval Network Operations Command. The following year, elements of that command and the Naval Space Command were incorporated into a new Naval Network and Space Operation Command.²¹⁹ On May 1, 2002, the Naval Network Warfare Command was established as a three-star flag-rank command. Subordinate commands included the Naval Network and Space Operation Command, the Fleet Information Warfare Center, and the Navy Component Task Force-Computer Network Defense.²²⁰ The Navy’s Computer Incident Response Team was moved from Fleet Information Warfare Center to the Navy Component Task Force-Computer Network Defense in 2003 and became the Navy Cyber Defense Operations Command in January 2006.²²¹

The establishment of the Naval Network Warfare Command expanded the authority and responsibilities of the Navy’s communications-computing personnel. While the Naval Network Warfare Command was a type command, meaning that it managed training for a particular kind of weapons system (cyber), it was also an operational command. For example, it included the Navy’s component of the Joint Task Force for Computer

Network Operations, which conducted both defensive and offensive operations. Network Warfare Command was initially staffed primarily by information systems technicians (enlisted) and information professional officers.²²²

However, the commander of the Naval Security Group and other leading cryptologists saw an opportunity in the growing prominence of computer network operations.²²³ As a result, in 2005, the Naval Security Group was transformed into the new Information Operations Directorate within Network Warfare Command, and the Naval Security Group’s detachments and activities became Navy Information Operations Commands within the Information Operations Directorate.²²⁴ For example, the Naval Information Warfare Activity became the Naval Information Operations Command in Suitland, Maryland.²²⁵ Around the same time, the Navy restructured the cryptology career field to emphasize the growing importance of computer network operations. In 2004, the secretary of the Navy approved a new enlisted rating, cryptologic technician networks, and converted over 240 enlisted information technology specialists into the new specialization.²²⁶ The following year, naval cryptology officers were redesignated as information warfare officers, a move intended to acknowledge their “expanded skill sets and responsibilities” associated with information operations.²²⁷

The Navy considered making more dramatic changes to professionalize cyber operations as something distinct from both communications and cryptology. In 2008, the Strategic Studies Group XXVI, an elite group of naval officers commissioned by Chief of Naval Operations Adm. Michael Mullen in 2006 to study the impacts of cyberspace on naval operations, delivered a report concluding that in order to “fight and win,” the Navy should

217 Anderson, “Why We Need the Navy Marine Corps Intranet.”

218 *Information Technology: DOD Needs to Ensure that Navy Marine Corps Intranet Program Is Meeting Goals and Satisfying Customers*, Government Accountability Office, (December 2006), 104, <https://www.gao.gov/assets/260/254360.pdf>.

219 Morris, “History of NAVNETWARCOM.”

220 “Spinning the Web,” *Sea Power* 46, no. 4 (April 2003): 61–65.

221 David Finley, “Navy Cyber Defense Operations Command Celebrates Its Past, Present, and Future,” Defense Visual Information Distribution Service, Jan. 29 2016, <https://www.dvidshub.net/news/188493/navy-cyber-defense-operations-command-celebrates-its-past-present-and-future>.

222 White, “Subcultural Influence on Military Innovation,” 331.

223 White, “Subcultural Influence on Military Innovation,” 333; Mike Lambert, “The Navy’s Cryptologic Community: A Transformational Phoenix?” *Proceedings* 131, no. 10 (October 2005).

224 Joseph Gunder, “Naval Security Group Aligns With NETWARCOM,” *U.S. Federal News Service*, Oct. 5, 2005.

225 Additionally, the Fleet Information Warfare Center was merged with the Navy Information Operations Commands at its two locations in Norfolk, VA and San Diego, CA. “OPNAV Notice 5450: Disestablish Naval Security Group Command (COMNAVSECGRU), Fort George G Meade, MD; Rename and Realign all Subordinate NAVSECGRU Commands and Detachments,” Chief of Naval Operations, Department of the Navy, Dec. 29, 2005, https://fas.org/irp/agency/navsecgru/5450_273.pdf.

226 Lambert, “The Navy’s Cryptologic Community.”

227 Teresa J. Frith, “Cryptology Officers Get New Name, Boss,” *U.S. Federal News Service*, Oct. 14, 2005. <https://coldwar-c4i.net/NSG/NNS051014-04.html>.

create “a Cyber Warfare Community comprised of warriors equal in every way to those who operate in traditional warfighting domains.”²²⁸ The report, which had been commissioned by Mullen two years earlier, argued that cyberspace officers should be trained “to be warfighters, not administrators” — individuals who possessed not only technical skill, but also the ability to command in a manner equal to commanders in the traditional areas of surface, subsurface, and air warfare.²²⁹

However, these recommendations were rejected. Both Mullen and the succeeding chief of naval operations, Adm. Gary Roughead, viewed cyberspace as just one component of a much broader problem in managing intelligence and information.²³⁰ This view was supported by the Navy’s cryptologic community, which saw cyber operations as part of cryptology.²³¹

Nonetheless, with the establishment of U.S. Cyber Command and associated directives to supply component forces, the Navy did elevate cyber operations. In 2009, it reactivated the 10th Fleet, which had played a critical role in anti-submarine warfare during World War II, making it Fleet Cyber Command, the Navy component of U.S. Cyber Command. By reactivating the 10th Fleet, the Navy underscored that “victory will be predicated on intelligence and information rather than fire power.”²³² The Navy moved all network organizations under Fleet Cyber Command/10th Fleet, including Network Warfare Command. But to emphasize the warfighting role of the new command, its first commander was Vice Adm. Barry McCullough, a sea-

soned surface warfare officer — not a cryptologist or communications-computing specialist.²³³

With growing demand for personnel with skills in computer network operations, the Navy also reorganized and elevated relevant career fields. In 2010, the Navy created the cyber warfare engineer specialization.²³⁴ Officers were directly commissioned into this new specialization based on records of excellence in academic computer science and engineering and were required to serve for a minimum of six years. After that, they would be encouraged to transfer to another community within the Information Dominance Corps, a new career field also established in 2010. The cyber warfare engineer became one of five specializations within the corps. The other four were meteorology and oceanography, information warfare, information professional, and intelligence.²³⁵ Perhaps most significantly, in 2010, the Navy made information dominance a warfare specialization with an associated qualification process and associated pin — something support fields typically lacked.²³⁶ In 2016, the Information Dominance Corps was renamed the Information Warfare Community to further “mainstream information warfare as one of four predominate warfare areas.”²³⁷

Despite this elevated status, Navy personnel specializing in cyber operations have yet to gain the full opportunities available to traditional warfighters. In general, officers within the Information Dominance Corps are restricted line officers, which means they are not eligible for command at sea.²³⁸ Some have called for an unrestricted line officer cyber warfare community that might “evolve

228 Quoted in White, “Subcultural Influence on Military Innovation,” 339. The Strategic Studies Group began in 1981 as a handpicked set of officers who would generate revolutionary concepts in naval warfare and continued through 2016. New officers were nominated each year for approximately one-year assignments.

229 Quoted in White, “Subcultural Influence on Military Innovation,” 339.

230 Roughead did make changes that elevated the authority of information operations, a much broader category than cyber operations. In early 2008, he elevated the deputy chief of naval operations for intelligence from a two-star to a three-star position and in 2009, merged the Office of the Director of Naval Intelligence (N2) and the Office of the Deputy Chief of Naval Operations (DCNO) for Communication Networks (N6) into one three-star office, the “deputy chief of naval operations for information dominance.” Jack N. Summe, “Navy’s New Strategy and Organization for Information Dominance,” *CHIPS* (January–March 2010), [https://www.doncio.navy.mil/\(vz3oz2uutryo0bujuhcxzrz\)/CHIPS/ArticleDetails.aspx?ID=2557](https://www.doncio.navy.mil/(vz3oz2uutryo0bujuhcxzrz)/CHIPS/ArticleDetails.aspx?ID=2557).

231 White, “Subcultural Influence on Military Innovation,” 342–43.

232 “Navy Stands Up Fleet Cyber Command, Reestablishes U.S. 10th Fleet,” *U.S. Department of Defense Information / Federal Information News Dispatch*, 2010.

233 White, “Subcultural Influence on Military Innovation,” 353–54.

234 “Establishment of the Cyber Warfare Engineer Designator,” Chief of Naval Operations, June 21, 2010, <https://www.public.navy.mil/bupers-npc/reference/messages/Documents3/NAV2010/NAV10205.txt>.

235 “Information Dominance Corps Officer Designator Alignment,” Chief of Naval Operations, June 22, 2010, <https://www.public.navy.mil/bupers-npc/reference/messages/Documents3/NAV2010/NAV10206.txt>. In 2016, the “Information Warfare” designator was changed to “Cryptologic Warfare.”

236 White, “Subcultural Influence on Military Innovation,” 357.

237 Ted N. Branch, “The ‘Information Dominance Corps’ is now the ‘Information Warfare Community,’” *CHIPS*, (January–March 2016), <https://www.doncio.navy.mil/Chips/ArticleDetails.aspx?ID=7307>.

238 “Information Warfare Community Overview,” Navy Personnel Command, last modified Oct. 21, 2019, https://www.public.navy.mil/bupers-npc/officer/communitymanagers/active/restricted/Pages/Information_Warfare_Community.aspx.

from its historic support role to an operationally proactive and predictive role.”²³⁹ Cyber warfare engineers must change specializations after their six-year service term, which means they cannot advance above the rank of lieutenant.²⁴⁰ Arguably, the limitations have been most significant within the information professional community — the Navy’s network maintainers. Information professionals saw dwindling command billets in the new mil-

Despite this elevated status, Navy personnel specializing in cyber operations have yet to gain the full opportunities available to traditional warfighters.

lennium, not only due to technology and mission changes but because of civilian outsourcing.²⁴¹ The information warfare community, which conducts defensive and offensive cyber operations, does not seem to have seen a similar reduction in command billets.²⁴² This suggests that individuals specializing in threat-oriented work continue to have more opportunities than those engaged in vulnerability reduction and maintenance work.

Army: Intelligence, Communications, and the Creation of Cyber Branch

Like the Navy, by the late 1990s, the Army recognized that security and efficiency both demanded a more centralized approach to computer network procurement and management. While the Army did not participate in Operation Eligible Receiver, it “got religion” after Solar Sunrise revealed that it

had no effective means of monitoring its networks for intruders.²⁴³ In response, U.S. Army Signal Command was tasked with developing intrusion detection systems. In 2002, Signal Command was absorbed by a new Network Enterprise Technology Command at Fort Huachuca, AZ, which was established to centralize the acquisition and management of the Army’s computer networks.

The new command was tasked with centralizing situational awareness and helping to defend networks, and it worked with U.S. Army Intelligence and Security Command to establish distinctive responsibilities for defense.²⁴⁴ The Army’s Network Operations and Security Center was part of the Network Enterprise Technology Command, but the former was co-located with the Army’s Computer Emergency Response Team at Fort Belvoir, VA, so that the response team could provide the center “direction without command” and help to coordinate network defense.²⁴⁵ Communications and intelligence commands thus came to share some responsibility for threat-oriented approaches to defense.

However, intelligence units continued to play the leading role. In 2002, Land Information Warfare Activity became the 1st Information Operations Command, with two battalions. The first consisted of field support teams and vulnerability assessment teams, and the second focused on computer network operations. The second battalion developed considerable expertise, in no small part by relying heavily on contractors. By the mid-2000s, it consisted of only eight active-duty personnel, supplemented by about 190 contractors, 30 government civilians, and 60 reservists.²⁴⁶

Intelligence and Security Command’s signals intelligence group, the 704th Military Intelligence Brigade, had been tasked with developing a computer network operations capability even earlier, in 1998. B company from the 742nd Military Intelligence Battalion took on this challenge. In June

239 Nancy Brown, Danelle Barrett, and Jesse Castillo, “Creating Cyber Warriors,” *Proceedings* 138, no. 10 (October 2012): 32, <https://www.usni.org/magazines/proceedings/2012/october/creating-cyber-warriors>. See also Vincent A. Augelli, “Information-Dominance Officers Need to Command,” *Proceedings* 138, no. 3 (March 2012): 79–81.

240 White, “Subcultural Influence on Military Innovation,” 358–59.

241 Augelli, “Information-Dominance Officers Need to Command.”

242 See, e.g., “Cryptologic Warfare Group 6 Stands Up New Commands,” Cryptologic Warfare Group 6 Public Affairs Office, Aug. 10, 2018, <https://www.dvidshub.net/news/288472/cryptologic-warfare-group-6-stands-up-new-commands>.

243 Thomas King, “Nonpassive Defense of the Army’s Computer Networks,” *Military Intelligence Professional Bulletin* 29, no. 3 (July–September 2003): 38, https://fas.org/irp/agency/army/mipb/2003_07.pdf.

244 Maryann Lawlor, “Information Systems Get Marching Orders,” *Signal* 57, no. 5 (January 2003). Interestingly, many announcements of Network Enterprise Technology Command only emphasized its goal of reducing costs. See, e.g., Hunter Keeter, “New Army NETCOM to Consolidate IT Acquisition Authority,” *C4I News*, Sept. 26 2002.

245 Robert K. Ackerman, “Network Center Ensures Security,” *Signal* 59, no. 12 (August 2005), <https://www.afcea.org/content/network-center-ensures-security>.

246 White, “Subcultural Influence on Military Innovation,” 72–73.

2000, it became Detachment Meade.²⁴⁷ Initially, Detachment Meade had trouble filling positions. Of an initial group of about three dozen people, only about half were technically qualified.²⁴⁸ Nonetheless, in the early 2000s, Detachment Meade grew rapidly, both in response to growing demand for cyber effects in the “War on Terror” and with the encouragement of Keith Alexander, who as a major general served as director of Intelligence and Security Command from 2001 to 2003 and who then as lieutenant general became the Army’s Deputy Chief of Staff for Intelligence from 2003 to 2005.²⁴⁹ After Alexander became the director of the National Security Agency in 2005, and as cyber operations continued to grow in national importance, Detachment Meade went through several organizational changes that increased its prominence. In 2009, it became the 744th Military Intelligence Battalion (also known as the Army Network Warfare Battalion).²⁵⁰

The rise of joint cyber operations further elevated the status of these activities. In 2009, Secretary of Defense Gates directed the services to establish component support to U.S. Cyber Command.²⁵¹ Both Intelligence and Security Command and Network Enterprise Technology Command lobbied for ownership of the new mission, recognizing that it would come with substantial resources and an increase from two- to three-star status. However, Network Enterprise Technology Command was seen as lacking the threat-focused orientation needed for an operational command.²⁵² In fact, it was reportedly inconsistent in cooperating with the Army’s computer emergency response team to remediate vulnerabili-

ties or otherwise respond to network incidents, likely because such actions could temporarily reduce network availability and otherwise inconvenience users — the primary focus of maintainers.²⁵³

Thus, Network Enterprise Technology Command was not given the cyber operations mission, but rather was put under the operational control of Army Cyber Command, a new unit established in October 2010 at Fort Belvoir, VA, home to both the Army’s Computer Emergency Response Team and the Army Network Operations and Security Center.²⁵⁴ While both of Intelligence and Security Command’s cyber-operational units — the 744th Military Intelligence Battalion and 1st Information Operations Command — were also put under the operational control of Army Cyber Command, they stayed under the administrative control of Intelligence and Security Command, which remained independent of Army Cyber Command.²⁵⁵ In 2011, the 744th Military Intelligence Battalion was reorganized as the 781st Battalion and placed under a new unit, the 780th Military Intelligence Brigade, within Intelligence and Security Command.²⁵⁶

As the scale of joint cyber operations grew, so did the need for trained personnel, spurring the Army to create new specializations.²⁵⁷ The Army’s signals branch created the information protection technician warrant officer in 2010, and the cyber network defender enlisted specialization in 2014. Similarly, the intelligence branch created the cryptologic cyberspace intelligence collector in 2012. In 2014, the Army finally created a new Cyber Branch, with three initial specializations: cyberspace officer, cyber operations technician (warrant officer), and cyber op-

247 “History,” 780th Military Intelligence Brigade, accessed Oct. 25, 2020, <https://www.inscom.army.mil/MS/780MIB/history.html>.

248 White, “Subcultural Influence on Military Innovation,” 88. The group developed its capability through a combination of targeted recruiting and ad hoc training by the National Security Agency and private companies. While these enabled it to develop a technically capable organization by the mid-2000s, it was still not well integrated into military operations, in part because of a lack of public guidance about how computer network operations were to be included in traditional military operations.

249 White, “Subcultural Influence on Military Innovation,” 92–93.

250 780th Military Intelligence Brigade, “History.”

251 Gates, “Establishment of a Subordinate Unified U.S. Cyber Command.” The Army began by establishing Army Forces Cyber Command headquarters within Army Space and Missile Defense Forces/Strategic Command, which had already been serving as a coordinating headquarters for computer network operations, helping to meet the Army’s requirements to support joint operations. White, “Subcultural Influence on Military Innovation,” 105–06.

252 White, “Subcultural Influence on Military Innovation,” 108–09.

253 White, “Subcultural Influence on Military Innovation,” 73–74.

254 “Army Establishes Army Cyber Command,” U.S. Army, Oct. 1 2010, https://www.army.mil/article/46012/army_establishes_army_cyber_command.

255 The 1st Information Operations Command was put under the operational control of Army Forces Cyber Command in 2011. “1st IO Command Overview,” 1st Information Operations Command, accessed Oct. 25, 2020, <https://www.1stiocmd.army.mil/Home/aboutus>.

256 780th Military Intelligence Brigade, “History.”

257 In the 2000s, the specializations most relevant to computer network operations were telecommunications engineering and information systems management. The commander of the second battalion within the 1st Information Operations Command, who was also in charge of the Army’s computer emergency response teams, typically came from one of these fields. White, “Subcultural Influence on Military Innovation,” 73. In late 2008, the Army chief of staff decided to create a set of additional skill indicators to indicate capabilities relevant to cyber operations, but both signals and intelligence branches felt they did not go far enough.

erations specialist (enlisted).²⁵⁸ In 2014, the Army announced the new cyber branch as one “that will take its place alongside infantry, artillery and the other Army combat arms branches.”²⁵⁹

Consistent with the tendency to treat threat-oriented activities as more akin to combat than vulnerability-oriented activities, it was Cyber Branch that became “a maneuver branch with the mission to conduct defensive and offensive cyberspace operations (DCO and OCO).”²⁶⁰ By contrast, the Army’s information protection technician warrant officers, an operations support field, conduct DODIN operations — activities that tend to be oriented toward reducing vulnerabilities.²⁶¹ Cyber network defenders, also a support field, conduct vulnerability assessments and other kinds of infrastructure support work, although they also conduct incident response, a threat-oriented activity.²⁶² Thus, while Army cyber operations gained considerable status after the establishment of Cyber Command, threat-oriented roles continue to have greater warfighting status than vulnerability-oriented roles.

Conclusion

Developing military cyber expertise has entailed much more than simply developing a supply of personnel with specialized skills, knowledge, and abilities. It has also involved persuading traditional warfighters of the critical importance of cyber skills, knowledge, and abilities and elevating certain work roles within organizational hierarchies. In other words, the relationships between and among distinctive kinds of cyber experts, other military personnel, and the computer networks with which they all must work to achieve operational goals had to undergo a transformation.

Key leaders in military operational and intelligence communities achieved this transformation by framing cyber operations as a kind of warfighting in their own right, rather than as being merely operations support. The leaders developed concepts of cyberspace and cyber operations that were analogous to well-accepted concepts of kinetic operations. Lead-

ers in the intelligence community grew particularly adept at using exercises to demonstrate the potential impact of cyber attacks on warfighting. Incident response teams made visible that these types of attacks were increasing. These efforts succeeded in formally raising the status of cyber offense and defense, culminating in the 2018 elevation of U.S. Cyber Command to become the nation’s 10th Unified Combatant Command.

Even as they highlighted the growing threats in cyberspace, leaders in the intelligence community recognized that such threats could not be successful unless there were vulnerabilities, which were partly of the Defense Department’s own making. While the Department of Defense succeeded in improving the security of commercial products, those products could be, and often were, deployed and managed in insecure ways. Many Defense Department intrusions were enabled by errors in network management and maintenance. But in the 1990s, most communications and computing personnel did not know how to configure and manage networks securely and had no immediate incentive to do so. The efficient mitigation of vulnerabilities was enhanced by some technological and organizational innovations, such as vulnerability scanning tools and the Information Assurance Vulnerability Alert process. But ultimately, these were innovations in the service of better management and maintenance. This history has thus highlighted the importance of maintenance as much as it has innovation.

By 2013, Joint Publication 3-12, “Cyberspace Operations,” explicitly included maintenance in its definition of DODIN operations. This was reiterated when the publication was reissued in 2018. Joint doctrine defines these operations in terms of mitigating a wide range of vulnerabilities, both technological and human. For example, DODIN operators are charged with training everyday users in good security practices as well as operating firewalls. However, as discussed above, these operations continue to be seen by many as lower in status than threat-focused activities, i.e., defensive and offensive cyber operations. This status difference is most visible in the Air Force, due to DODIN operations being placed in

258 Eventually all of the electronic warfare personnel were converted to two new specializations in the cyber branch: electronic warfare officer and electronic warfare technician. “Army Cyber Branch Offers Soldiers New Challenges, Opportunities,” Fort Gordon Public Affairs Office, U.S. Army, Nov. 25, 2014, https://www.army.mil/article/138883/army_cyber_branch_offers_soldiers_new_challenges_opportunities.

259 Fort Gordon Public Affairs Office, “Army Cyber Branch Offers Soldiers New Challenges, Opportunities.”

260 “Cyber Operations Officer (17A),” U.S. Army, accessed October 25, 2020, <https://www.goarmy.com/careers-and-jobs/browse-career-and-job-categories/computers-and-technology/cyber-operations-officer.html>. Interestingly, however, the Army’s Officer Personnel Management Directorate still classifies cyber operations officers as “operations support.” “Officer Personnel Management Directorate,” United States Army Human Resources Command, Nov. 17, 2020, <https://www.hrc.army.mil/Officer/Officer%20Personnel%20Management%20Directorate>.

261 “Warrant Officer Prerequisites and Duty Description: 255S - Information Protection Technician,” U.S. Army Recruiting Command, Aug. 18, 2020, <https://recruiting.army.mil/ISO/AWOR/255S/>.

262 “Cyber Network Defender,” U.S. Army, accessed October 26, 2020, <https://www.goarmy.com/careers-and-jobs/browse-career-and-job-categories/computers-and-technology/cyber-network-defender.html>.

the same career field with defensive and offensive cyber operations. Yet it is also visible in subtler ways in the Navy and the Army, where vulnerability-oriented roles tend to have less warfighting status and fewer opportunities for command.

This paper does not take a position on whether vulnerability mitigation should or should not be considered a kind of warfighting. Rather, my aim has been to analyze the historical process by which such activities came to be officially included in the scope of operations and how the cultural status of varying forms of cyber expertise has evolved over time. I have also sought to highlight the importance of vulnerability mitigation, regardless of its “warfighting” status.

Evidence suggests that vulnerability mitigation continues to be less of a priority than it should. In September 2015, the chairman of the Joint Chiefs of Staff and the secretary of defense launched a Cybersecurity Culture and Compliance Initiative, noting that “roughly 80 percent of incidents in the cyber domain can be traced to three factors: poor user practices, poor network and data management practices, and poor implementation of network architecture.”²⁶³ The initiative directed Cyber Command and the Department of Defense chief information officer to complete 11 tasks, including developing leadership training materials for combatant commanders and other units, establishing training requirements for providers of equipment and services, and recommending specific changes to technological capabilities for patching vulnerable systems. The initiative also directed all combatant commanders to introduce certain security principles into training, thereby reducing human vulnerabilities.

One month later, the commander of Cyber Command and the Defense Department chief information officer went further by creating a Cybersecurity Discipline Implementation Plan, arguing that Defense Department networks were “not defensible.”²⁶⁴ They noted “an unacceptable number of unpatched vulnerabilities,” and gave commanders and supervisors responsibility for verifying that “all servers and network infrastructure devices” were compliant with the

Information Assurance Vulnerability Alert process. This was just one of 17 tasks assigned to commanders and supervisors. Finally, consistent with Defense Department directives for information assurance training, the Defense Information Systems Agency in 2015 launched the Cyber Awareness Challenge training program to reinforce “best practices” among service members, civilians, and contractors.²⁶⁵

However, in 2020, the U.S. Government Accountability Office identified significant shortcomings in the implementation of each of these three programs. Seven of 11 tasks in the Cybersecurity Culture and Compliance Initiative were still not completed, despite 2016 deadlines. Four tasks in the Cybersecurity Discipline Implementation Plan were difficult to complete because of legacy equipment, and the status of another seven tasks was unknown because no one had been assigned responsibility for ensuring their completion. Similarly, units did not keep track of which computer users did or did not take the Cyber Awareness Challenge training.²⁶⁶ In 2019, the Defense Department’s inspector general concluded that the Defense Department had not consistently remediated vulnerabilities discovered by cyber red teams.²⁶⁷

By establishing DODIN operations as a kind of warfighting, along with offensive and defensive cyber operations, the Defense Department has sought to raise the status of vulnerability remediation and those who manage it. But ultimately, vulnerabilities cannot be completely eliminated by even the most expert of cyber forces. Rather, the complete elimination of vulnerabilities would require a transformation of everyday users — individuals who are *not* cyber experts but nonetheless can compromise systems by careless practices. Recognizing this problem, some officials have sought to frame everyday computer network users as warfighters.

In 2009, the Air Force began advocating the “Rise of the Cyber Wingman” philosophy, outlining 10 principles that all Air Force personnel should observe, and arguing that “every Airman is a defender in cyberspace.”²⁶⁸ By 2012, the Marines had come to consider “every Marine a cyber warrior” and instituted a cyber security training regimen analogous

263 Department of Defense, *Department of Defense Cybersecurity Culture and Compliance Initiative*, 1.


264 *DOD Cybersecurity Discipline Implementation Plan*, Department of Defense, October 2015, 16, <https://dodcio.defense.gov/Portals/0/Documents/Cyber/CyberDis-ImpPlan.pdf>.

265 A revised training directive was issued in November 2015: “Information Assurance Workforce Improvement Program, Incorporating Change 4, 11/10/2015,” Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer, Dec. 19, 2005, <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/857001m.pdf>. The Cyber Awareness challenge training program is described in, “CYBERSECURITY: DOD Needs to Take Decisive Actions to Improve Cyber Hygiene,” Government Accountability Office, April 13, 2020, <https://www.gao.gov/products/GAO-20-241>.

266 Government Accountability Office, “CYBERSECURITY: DOD Needs to Take Decisive Actions to Improve Cyber Hygiene.”

267 “Followup Audit on Corrective Actions Taken by DoD Components in Response to DoD Cyber Red Team-Identified Vulnerabilities and Additional Challenges Facing DoD Cyber Red Team Missions (DODIG-2020-067),” Department of Defense, Office of Inspector General, March 13, 2020, <https://www.dodig.mil/reports.html/Article/2114391/followup-audit-on-corrective-actions-taken-by-dod-components-in-response-to-dod/>.

268 “Rise of the Cyber Wingman,” U.S. Air Force, Nov. 12, 2009, <https://www.af.mil/News/Article-Display/Article/118545/rise-of-the-cyber-wingman/>.

to its well-known mantra, “every Marine a rifle-man.”²⁶⁹ A recent critical review of Navy cyber security, commissioned by the secretary of the Navy after multiple breaches, concluded that the “workforce is generally uneducated in cybersecurity, largely complacent,” and tends to see cyber security “as an ‘IT issue’ or ‘someone else’s problem.’”²⁷⁰ As a result, the review explained, “cybersecurity is undervalued, and often used as a bill-payer within programs of record.”²⁷¹ It proposed that the Navy inculcate an “Every Sailor a Cyber Sentry” mindset.²⁷² And a recent article entitled “Every Warrior a Cyber Warrior” argues for improving Army cyber security education because “every U.S. Army soldier must be ready to fight on the digital battlefield.”²⁷³ Whether these metaphors will ultimately be persuasive, however, remains to be seen. 

tor of Texas National Security Review, for carefully reviewing and improving the clarity and accessibility of the manuscript.

Image: U.S. Air Force, J.M. Eddins Jr.

Rebecca Slayton is associate professor at Cornell University and is jointly appointed in the Science & Technology Studies Department and the Judith Reppy Institute for Peace and Conflict Studies. Her first book, *Arguments that Count: Physics, Computing, and Missile Defense, 1949–2012* (MIT Press, 2013) shows how the rise of computing as a new field of expertise reshaped public policies and perceptions about the risks of missile defense in the United States. She is currently working on *Shadowing Cybersecurity*, a book that examines the history of cyber security expertise through the interplay of innovation and repair.

Acknowledgements: Thanks go to Captain Jason Healey for very informative emails and contacts and for donating documents to the National Security Archive. I also thank Gen. John Campbell for email correspondence about the formation of the JTF-CND and Col. Walter Rhoads and Capt. William Gravell for granting me phone interviews and email correspondence that answered numerous questions about their work. I am also grateful to Herb Lin for sharing a copy of the partially declassified 1992 Directive on Information Warfare. I thank two anonymous reviewers and Doyle Hodges, the executive editor of Texas National Security Review for constructive criticism that improved this paper. Finally, I thank Megan Oprea, managing edi-

269 Statement of Lt. Gen. Richard Mills in, “Digital Warriors: Improving Military Capabilities for Cyber Operations,” House Armed Services Committee, 112th Congress, 2nd Sess., July 25, 2012, 12, <https://www.govinfo.gov/content/pkg/CHRG-112hrg75668/pdf/CHRG-112hrg75668.pdf>.

270 Cybersecurity Readiness Review, Department of the Navy, March 2019, 12, https://www.wsj.com/public/resources/documents/CyberSecurityReview_03-2019.pdf?mod=article_inline.

271 Department of the Navy, *Cybersecurity Readiness Review*, 12.

272 Department of the Navy, *Cybersecurity Readiness Review*, 15.

273 Christopher J. Heatherly and Ian Melendez, “Every Soldier a Cyber Warrior: The Case for Cyber Education in the United States Army,” *Cyber Defense Review* (Spring 2019): 64, https://cyberdefensereview.army.mil/Portals/6/HEATHERLYMELENDEZ_CDR_V4N1.pdf?ver=2019-04-30-105206-983.