Subcultural Influence on Military Innovation: The Development of U.S. Military Cyber Doctrine

Subcultural Influence on Military Innovation:

The Development of U.S. Military Cyber Doctrine

A dissertation presented

by

Sarah Payne White

to The Department of Government

in partial fulfillment of the requirements

for the degree of

Doctor of Philosophy

in the subject of

Political Science

Harvard University

Cambridge, Massachusetts

July 2019

Dissertation Advisor: Stephen Peter Rosen Sarah Payne White

Subcultural Influence on Military Innovation:

The Development of U.S. Military Cyber Doctrine

ABSTRACT

Why do military organizations adopt different approaches to a new technology? History has demonstrated that the development of a new military technology does not presuppose its uniform application either cross-nationally or cross-organizationally. Rather, we have seen time and again that militaries vary in their interpretation and application of the same technologies. Over the past three decades, this same pattern of variation has begun to emerge through the development of different organizational and national approaches to cyberspace.

This dissertation will attempt to answer the question of why variation exists in patterns of military innovation by demonstrating the constraining effects of past operational experience on organizational innovation. Specifically, I argue that the background operational experiences that define various military subcultures can have a limiting effect on an organization's ability to consider alternative choices when presented with a new operational problem. This effect is higher under conditions of uncertainty, when the lack of clear top-down guidance affords these subcultures greater latitude for independent initiative. Under this framework, innovation will emerge as the evolutionary product of a process of interaction and bargaining based on patterns of behavior ingrained in service subcultures. Over time, tensions between these competing interpretations of the purpose of a new technology will be resolved in a way that aligns with the broader service mission and dominant service culture. I assess this hypothesis through a detailed study of the historical origins of cyberspace doctrine in the U.S Army, Navy, and Air Force. In addition to a new theoretical framework for military innovation, this paper makes a substantial empirical contribution to the history of cyberspace operations in the U.S. military.

CONTENTS

ACKNOWLEDGEMENTS

There are a number of people without whom I could not have completed this project, and to whom I owe my sincere thanks. Steve Rosen was a patient and inspiring mentor during my three years at Harvard. He has made me both a better scholar and a better officer. Iain Johnston likewise had an important impact on my thinking, and I am grateful for his influence. Michael Sulmeyer and the members of the Belfer Center Cyber Security Project welcomed me into the Harvard cyber community from the beginning, and kept me motivated to pursue a project with practical impact. Avishay Ben Sasson-Gordis served as a valued intellectual sparring partner, a sincere friend, and a reminder that the bonds of military service are not constrained by national boundaries. I am similarly thankful for the mentorship of Tyler Jost, whose invaluable guidance at all stages of the process ensured that my transition into academia would be a smooth one. The untiring efforts of Thom Wall and Dustin Tingley helped me to navigate the administrative requirements associated with the Army's three year timeline, and I am grateful for their support. The friendship of Amy Chandran and Evelyn Flashner made my time at Harvard immensely, and unexpectedly, rewarding, in ways that I will never be able to repay. I am further indebted to Colonel Suzanne Nielsen and the West Point Sosh Department for giving me the opportunity to pursue my doctorate, and to Brigadier General Joe Hartman for not trying too hard to convince me otherwise. I hope to continue to live up to the professional ideals that both officers represent. Finally, I owe a debt of gratitude to my son and to my husband: to my son for giving me a deadline, and to my husband for helping me meet it. I do not deserve either of them.

ABBREVIATIONS

ACC	Army Capstone Concept
ACC	Air Combat Command
ACERT	Army Computer Emergency Response Team
ACO	Army Cryptologic Office
ACOIC	Army Cyber Operations and Integration Center
ACOPC	Army Cyberspace Operations Planners Course
ADP	Army Doctrinal Publication
AETC	Air Education and Training Command
AFCERT	Air Force Computer Emergency Response Team
AFCYBER	Air Force Cyber Command
AFCYBER (P)	Air Force Cyber Command (Provisional)
AFDD	Air Force Doctrine Document
AFEWC	Air Force Electronic Warfare Center
AFGSC	Air Force Global Strike Command
AFIC	Air Force Intelligence COmmand
AFISRA	Air Force Intelligence, Surveillance, and Reconnaissance Agency
AFIWC	Air Force Information Warfare Center
AFNETOPS	Air Force Network Operations
AFOSI	Air Force Office of Special Investigation
AFRL	Air Force Research Laboratory
AFSC	Air Force Specialty Code
AFSPC	Air Force Space Command
AIA	Air Intelligence Agency
ANWB	Army Network Warfare Battalion
AOC	Air Operations Center
ARAT-TA	Army Reprogramming and Analysis Team-Threat Analysis

ARCYBER	Army Cyber Command
ARFORCYBER	Army Forces Cyber Command
ARSPACE	Army Space Command
ASA	Army Security Agency
ASCC	Army Service Component Command
ASI	Additional Skill Identifier
ATO	Air Tasking Order
ATSS	Army Targeting and Sensing Systems
BCT	Brigade Combat Team
BOLC	Basic Officer Leadership Course
C/EM	Cyber/Electromagnetic Activities
C2	Command and Control
C2W	Command and Control Warfare
C3M	Command, Control, and Communication Countermeasures
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CAC	Combined Arms Center
CBA	Capabilities Based Assessment
CCC	Captain's Career Course
CCNA	Cisco Certified Network Associate
CCoE	Cyber Center of Excellence
CCTC	Cyber Common Technical Core
CDX	Cyber Defense Exercise
CEMA	Cyber and Electromagnetic Activities
CENTCOM	U.S. Central Command
CERF	Cyber Effects Request Form
CERT	Computer Emergency Response Team
CEWI	Combat Electronic Warfare and Intelligence battalion
CFCOE	Cyber Forces Concept of Operations and Employment
CIC	Combat Information Center

CISSP	Certified Information Systems Security Professional
CJCS	Chairman of the Joint Chiefs of Staff
CMF	Cyber Mission Force
CNA	Computer Network Attack
CND	Computer Network Defense
CNE	Computer Network Exploitation
CNMF	Cyber National Mission Force
CNO	Computer Network Operations
CNO	Chief of Naval Operations
CNO-TF	Computer Network Operations Task Force
COMS	Cyber Operations Mission Sets
COOC	Cyber Operations Officer Course
CREW	Counter-RCIED Device
CSAW	Communications Supplementary Activities, Washington
CSCB	CEMA Support to Corps and Below
CSE	Cyberspace Solutions Engineer
CTAG	Critical Task Advisory Group
CTC	Combat Training Center
CTN	Cryptologic Technician-Network
CTO	Cryptologic Technician-Communication
CTT	Cryptologic Technician-Technical
CWC	Composite Warfare Commander
CWE	Cyber Warfare Engineer
CYBERCOM	U.S. Cyber Command
DARPA	Defense Research Projects Agency
DIRNSA	Director of the NSA
DISA	Defense Information Systems Agency
DoD	Department of Defense
DoDD	Department of Defense Directive

EDVAC	Electronic Discrete Variable Computer
EECS	Electrical Engineering and Computer Science Department
EMS	Electromagnetic Spectrum
ENIAC	Electronic Numerical Integrator and Computer
ESC	Electronic Security Command
EW	Electronic Warfare
FIWC	Fleet Information Warfare Center
FLTCYBERCOM	Fleet Cyber Command
FM	Field Manual
FST	Field Support Team
GURL	General Unrestricted Line Community
I2CEWS	Intelligence, Information, Cyber, Electronic Warfare, and Space Detachment
ICBM	Intercontinental Ballistic Missile
IDC	Information Dominance Center
IDC	Information Dominance Corps
INFOCON	Information Warfare Threat Condition
INSCOM	Intelligence and Securities Command
INWT	Intermediate Network Warfare Training Course
IO	Information Operations
IOC	Intelligence Operations Center
IOSS	Intelligence Organization and Stationing Study
IOTF	Information Operations Task Force
IOVAP	Information Operations Vulnerability Assessment Program
IP	Information Professional
ISR	Intelligence, Surveillance, and Reconnaissance
IT	Information Technician
IW	Information Warfare
IWS	Information Warfare Squadron
JACWC	Joint Advanced Cyber Warfare Course

JC2WC	Joint Command and Control Warfare Center
JCAC	Joint Cyber Analysis and Attack Course
JFCC-NW	Joint Functional Component Command-Network Warfare
JOCCP	Junior Officers Career Cryptologic Program
JP	Joint Publication
JRTC	Joint Readiness Training Center
JTF-CND	Joint Task Force-Computer Network Defense
JTF-CNO	Joint Task Force-Computer Network Operations
JTF-GNO	Joint Task Force-Global Operations
JWID	Joint Warrior Interoperability Demonstration
KSA	Knowledge, Skills, and Abilities
LDE&T	Leader Development, Education, and Training
LIWA	Land Information Warfare Activity
MDMP	Military Decision Making Process
METOC	Meteorology and Oceanography
MI	Military Intelligence
MILDEC	Military Deception
MOS	Military Occupation Specialty
NAF	Numbered Air Force
NAVCIRT	Navy Computer Incident Response Team
NAVELEX	Naval Electronic Systems Command
NAVSECGRU	Naval Security Group
NCAT	Navy Cyber Attack Team
NCDOC	Navy Cyberspace Defense Operations Command
NCTAMS	Naval Compute rand Telecommunications Area Master Station
NCTF-CND	Navy Component Task Force-Computer Network Defense
NCTS	Naval Computer and Telecommunications Stations
NCWDG	Navy Cyber Warfare Development Group
NETCOM	Network Enterprise Technology Command

NETWARCOM	Naval Network Warfare Command
NIOBC	Naval Intelligence Officer Basic Course
NIOC	Naval Information Operations Command
NIOD	Navy Information Operations Detachments
NIWA	Naval Information Warfare Activity
NMCI	Navy Marine Corps Intranet
NOC	Network Operations Center
NROC	Navy Remote Operations Center
NSA	National Security Agency
NSG	Naval Security Group
NSGA	Naval Security Group Activities
NSGD	Naval Security Group Detachment
NTC	National Training Center
NTDS	Naval Tactical Data System
OPE	Operational Preparation of the Environment
OPFOR	Opposing Force
OPSEC	Operations Security
OTS	Officer Training School
PSYOP	Psychological Operations
RCIED	Remote Control Improvised Explosive Device
REBM	Radio-Electronic Battle Management
RF	Radio Frequency
RM	Radioman
ROTC	Reserve Officer Training Course
SAA	Studies and Analysis Activity
SAC	Strategic Air Command
SAGE	Semi-Automatic Ground Environment
SCI	Sensitive Compartmentalized Informatioin
SEAD	Suppression of Enemy Air Defense

SEW	Space and Electronic Warfare
SEWC	Space and Electronic Warfare Commander
SIGINT	Signals Intelligence
SIOE	Space and Information Operations Element
SMDC/ARSTRAT	Space and Missile Defense Command/Army Strategic Command
SOTA	SIGINT Operational Tasking Authority
SPACECOM	U.S. Space Command
SPAWAR	Space and Naval Warfare Systems Command
SSG	Strategic Studies Group
STDA	SIGINT Technical Development Activity
STEM	Science, Technology, Engineering, and Math
STRATCOM	U.S. Strategic Command
TAO	Tailored Access Operations
TDQC	Tool Developer Qualification Course
TNOSC	Theater Network Operations Support Center
TRADOC	Training and Doctrine Command
TS	Top Secret
UCT	Undergraduate Cyber Training Course
UMBC	University of Maryland Baltimore County
UNIVAC	Universal Automatic Computer
UNWT	Undergraduate Network Warfare Training
USAFA	United States Air Force Academy
USAFSS	U.S. Air Force Security Service
USMA	United States Military Academy
USNA	United States Naval Academy
VAT	Vulnerability Assessment Team
WCCO	World Class Cyber OPFOR
WWMCCS	Worldwide Military Command and Control System

LIST OF TABLES AND FIGURES

CHAPTER ONE | **Introduction**

In August of 2008, the Russian military invaded the Republic of Georgia. Over the ensuing five days, Russian cyber attacks coincided with military operations on the ground to create an information blockade for the Georgian people. Thirty-five percent of Georgia's internet networks suffered decreased functionality during the attacks, with the highest levels of online activity coinciding with the Russian invasion of South Ossetia on August 8, 9, and 10.[1] While the war in the ground ended in largely the same place it began, the incorporation of large-scale cyber attacks made it clear that the contours of conflict had changed.

Internal appraisals of the Russian military's performance uncovered a number of operational deficiencies, not least of which was the failure of the cyber attacks, and the broader information campaign in which they were nested, to successfully control the war's narrative. This perceived failure resulted in a recommendation for the creation of a dedicated branch within the military that could manage the information component of future wars — a combination of hackers, journalists, linguists, and specialists in strategic communications and psychological operations. However, no such information branch materialized, due in part to disagreements over who should own the capability.[2] Did it belong to Russia's storied electronic warfare troops underneath their ensuing doctrine of electronic struggle? Did it belong in a new branch of the military? Did it belong in the military at all?

The intuition behind the questions that the Russian defense establishment asked of itself in 2008 — that where one places a new capability will have an impact on how it develops — serves as the primary motivation of this dissertation. Russia's prolific activity in cyberspace since 2008 suggests that they eventually found an answer to these questions. At the same time, the nature of this activity — with a

[1] Alison Lawlor Russell, "The Georgia-Russia War," in *Cyber Blockades,* (Washington, D.C.: Georgetown University Press, 2014).

[2] Keir Giles, "'Information Troops' — a Russian Cyber Command?" *3rd International Conference on Cyber Conflict*, C. Czosseck, E. Tyugu, T. Wingfield (Eds.) (Tallinn: CCD COE Publications, 2011).

heavy emphasis on large-scale narrative manipulation and ideological warfare — suggests that that answer varied substantially from the path taken by the United States when faced with a similar turning point.[3]

This dissertation will attempt to explain why variation in cyberspace doctrine exists by studying the interplay between organizational culture and military innovation. It argues that operational backgrounds will affect the manner in which organizations interpret new problems, and that those interpretations will then affect the trajectory of the innovation that follows. The resultant theoretical framework, grounded in the history of how cyberspace operations evolved in the United States military, will help us to understand problems of cross-national variation such as the one described above.

Military Innovation and Organizational Subcultures

THE ARGUMENT

The central argument of this dissertation is that the operational backgrounds of service members will have a decisive effect on the process of military innovation. Military innovation is measured through the output of doctrine, and operational backgrounds are assessed through the mechanism of organizational subcultures, which shape the behaviors and beliefs of those who belong to them. The manner in which these subcultures matter can be described in a two-part process. First, under conditions of high uncertainty, the primary determinant of the trajectory of an innovation will be the cognitive and behavioral predispositions of the service subcultures which are given responsibility for it. Second, as that uncertainty diminishes, competition among subcultures will resolve in a way that aligns with the broader service mission and the dominant service culture.

Theoretically, this argument drops the logic of organizational culture to the level of organizational subcultures, and then extends that logic to the question of how militaries innovate. Practically, the argument suggests that the type of personnel who are assigned to a problem is of decisive

[3] Keir Giles, "Russia's 'New' Tools for Confronting the West," *Chatham House: The Royal Institute for International Affairs* (London: March 2016). In the U.S. case, that turning point was the 2008 Buckshot Yankee network intrusion, which convinced Department of Defense leadership of the need to create a cyber command.

importance to how that problem will resolve. It matters, for example, whether responsibility for the development of cyberspace operations is given to an intelligence organization or a communications organization. The argument also suggests that the range of possible solutions for an innovation challenge will be constrained at the outset by the implicit beliefs and practices of the organization that owns it. In other words, people will be inclined to see things a certain way based on how they were professionally raised. If they see things differently, they will have difficulty convincing the remainder of their professional tribe that such a perspective is worth pursuing.

This argument is both descriptive and predictive. It is descriptive in the sense that it can help us to retroactively understand why certain outcomes transpired when others were possible, and were possibly more advantageous. It is predictive in the sense that it can help us to anticipate the shape of doctrinal outcomes given an understanding of the nature of the organizations that create them. This argument has further implications for how we see military innovation in general. It is well established that external constraints act upon the process of innovation.[4] Traditionally, these constraints are seen to either prevent or encourage the start of the process — to start or to stop militaries from innovating in the first place — but they do not say much on what that process will look like once it has begun. This theoretical framework will attempt to change that focus by examining the interactions within and between the organizations in which the innovation takes place. It does this through an investigation of the role of subcultures on the creation and evolution of military doctrine. In other words, how do the experiences derived from operational backgrounds contribute to, or detract from, the process of military innovation as measured by military doctrine?

---

[4] Barry R. Posen, *The Sources of Military Innovation: France, Britain, and Germany Between the World Wars* (New York: Cornell University Press, 1985); Stephen P. Rosen, *Winning the Next War: Innovation and the Modern Military* (New York: Cornell University Press, 1991); Kimberly Marten Zisk, *Engaging the Enemy: Organization Theory and Soviet Military Innovation 1955-1991* (Princeton University Press, 1993); Deborah D. Avant, *Political Institutions and Military Change: Lessons From Peripheral Wars* (Ithaca: Cornell University Press, 1994); Elizabeth Kier, *Imagining War: French and British Military Doctrine Between the Wars* (Princeton University Press, 1999); Deborah D. Avant, "From Mercenary to Citizen Armies: Explaining Change in the Practice of War," *International Organization* 54, 1 (Winter 2000): 41-72; Thomas G. Mahnken, *Uncovering Ways of War: U.S. Intelligence and Foreign Military Innovation*, 1918-1941 (New York: Cornell University Press, 2002).

CHALLENGES AND CONTRIBUTIONS

There is little research that examines cyberspace doctrine empirically, and even less that compares such doctrine across different foreign or domestic military organizations. The dearth of such research is due less to lack of interest than to challenges in the realm of data availability, data classification, and the lack of adequate or accepted comparative frameworks through which to assess cyberspace problems. This latter case is not helped by the fact that cyberspace means different things to different people. Russian cybersecurity doctrine, for example, reserves use of the word "cyber" for reference to Western activities rather than to anything that exists in its own conceptual framework.[5] Instead, Russia treats cyberspace as a subordinate component to its holistic doctrine of information warfare.[6] Cyber is then regarded "as a mechanism for enabling the state to dominate the information landscape," rather than as a way to achieve discrete effects on technical systems.[7] The challenges of any study of military doctrine are exacerbated when the underlying terms are in dispute.

These challenges are equally exacerbated by the fact that much of the narrative surrounding cyberspace, as well as the vast majority of cyberspace activity, is driven by actors in the private sector. As a result, many military decision-makers openly take their cues on how to behave in cyberspace from private sector developments, while governments that must react to a cyber incident often find themselves in negotiation with tech companies in addition to nation-states.[8] What this all means is that the landscape of cyber activity is far more complicated than that with which militaries must ordinarily contend on land, air, or sea.

---

[5] Giles, "Russia's 'New' Tools."

[6] "Military Doctrine of the Russian Federation," *carnegieendowment.org,* last modified 5 February 2010, http://carnegieendowment.org/files/2010russia_military_doctrine.pdf; Keir Giles, "The Military Doctrine of the Russian Federation 2010," *NATO Research Review*, February 2010.

[7] Michael Connell and Sarah Vogler, "Russia's Approach to Cyber Warfare," *CNA Occasional Paper Series*, (2017).

[8] An excellent example of this phenomenon took place in the 2008 Russia-Georgia War. When Georgia came under cyber attack, the owner of Tulip Systems (TSHost), a private web hosting company in Atlanta, contacted the president of Georgia to offer assistance in reconstituting their internet capabilities. The following day, the Georgian government transferred critical internet capabilities to TSHost servers in the US, to include the websites of the Ministry of Defense and the President. The Russian cyber attackers then brought their DDoS capabilities to bear on American targets. See Stephen W. Korns and Joshua E. Kastenberg, "Georgia's Cyber Left Hook," *Parameters* (Winter 2008-2009).

Concerning sources of data, there is a common assumption that much of the substance of cyberspace activity is classified. This assumption is only partially true. Certainly, many of the details of cyberspace operations — the technical specifications of how they are executed, and often the identities of those who perpetrate them — are classified or otherwise inaccessible to academic researchers. However, many of the structural inputs to those operations are not. I thus circumvent the problem of classification by focusing not on the operations themselves, but on the structural inputs to those operations: on the personnel management processes, organizational reform, and conceptual development that can all be included under the phrase "doctrine." In compiling this data, I rely heavily on interviews, professional service journals, and press releases in addition to the unclassified doctrinal content that is publicly available.

This dissertation thus makes both a theoretical and an empirical contribution to the study of cyberspace and cyber conflict. Empirically, it contains the first historical account of the development of cyberspace operations in the U.S. military services. Theoretically, the dissertation's analytic framework extends familiar arguments of organizational culture to the level of organizational subcultures to demonstrate the strong effect that subcultural influences can have on the process of innovation.

Case Justification

New technologies and the processes of military innovation that embrace them always contain an element of uncertainty. However, there are a number of attributes of cyberspace that render it unique among historical military innovations, five of which I will highlight here.[9]

First, cyberspace is not a strictly military technology, nor does it exist in a strictly military space. Rather, cyberspace is global, interconnected, and is used by a variety of governmental and non-governmental actors for diverse purposes. This means that there is a substantial element of private sector

[9] A good summary of other these and other attributes can be found in Matthew Miller, Jon Brickey, and Gregory Conti, "Why Your Intuition About Cyber Warfare is Probably Wrong," Small Wars Journal, November 29, 2012.

influence in cyberspace both inside and outside the contours of conflict. This influence affects how cyber technology evolves as well as the types of decisions military actors must make when engaged in a cyber operation. It also erodes the military's monopoly on both use of force and the underlying technical and professional expertise required to engage in cyberspace operations.[10] Author Jason Healey goes so far as to say that it is the private sector, and not governments, which plays the primary role in cyber conflict.[11] Under these circumstances, militaries do not have the luxury of controlling the conditions of innovation as they otherwise would with a technology reserved strictly for battlefield use, and will likely have to rely more heavily on private sector expertise as a result.[12]

Second, cyberspace enables the creation of military effects which are neither violent nor enduring.[13] The intrusive yet non-violent nature of these effects eludes traditional legal categorization, and therefore increases the difficulty of formulating an appropriate response.[14] Some scholars have used this premise to argue that cyber war is not actually war and should not be treated as such.[15] Others argue that the very danger of cyberspace lies in its ability to drive interstate conflict into a realm that intentionally falls below the threshold of armed confrontation, and thus intentionally outside of traditional frameworks

---

[10] The role of private actors is not limited to their ownership of terrain or their invention of new technology. These private actors will also both formally and informally engage in cyberspace operations themselves. For example, a distinguishing characteristic of Russian cyber operations is their regular employment of non-state actors in support of state military and political objectives. For example, the cyber attacks in the 2008 Russia-Georgia war were perpetrated by hackers whose official ties to the Russian state were never definitively proven — this in spite of the fact that the cyber attacks were perfectly synchronized with military operations on the ground. See Alexander Klimburg, "Mobilizing Cyber Power," *Survival* 53:1 (2011): 41-60.

[11] Jason Healey, ed. *A Fierce Domain: Conflict in Cyberspace, 1986-2012* (The Atlantic Council: Cyber Conflict Studies Association, 2013).

[12] I recognize that there has always been interplay between government and civilian sectors in the process of military innovation (for example, the impact of commercial air travel on the development of U.S. interwar air power), but the difference is that cyber "weapons," or the capabilities used by militaries to manipulate nation-state systems, are not strictly owned or controlled by militaries or governments, with the result that militaries must learn not only from each other, but from non-military entities. This is true at both the technical and conceptual levels.

[13] It goes without saying that cyberspace also enables effects which could be both violent and enduring. However, it is the non-violent, non-enduring effects which have proven most difficult to deal with from both a legal and a strategic standpoint. I argue, therefore, that those are the effects which make cyberspace unique in the realm of military operations.

[14] Matthew C. Waxman, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)," *The Yale Journal of International Law* Vol 36 (2011): 421-459.

[15] Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security Studies* 38 No 2 (2013): 41-73; Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies*, 35:1 (2012): 5-32; Thomas Rid and Robert M. Lee, "OMG Cyber!" *The RUSI Journal* 159:5 (2014) 4-12.

for response.[16] However, arguments over whether cyber war is or is not war because it is insufficiently casualty-producing "risks becoming a purely academic exercise if cyber conflict eventually supplants military violence as the ultimate arbiter of international politics. Cyberwar does not need to be war to make war obsolete."[17] The fact that this type of conflict tends to be nonlethal and nonviolent is exactly what makes it unique among historic military innovations, and is what partially drives the demand for its own set of analogous rules.[18] Thus, the conceptual, legal, and intellectual innovations required to develop a coherent strategic framework for cyber effects have become as important as the rote development of weapons and personnel. The immense difficulty of achieving such a framework is reflected in the history of cyberspace development that will appear in chapters to follow.[19]

This combination of globally interconnected terrain with the ability to achieve non-violent effects leads to a third unique characteristic of cyberspace: that it is defined by a condition of constant action. In other words, both government and non-government actors are perpetually in contact with one another and are perpetually attempting to achieve positional advantage, regardless of whether or not they exist in a state of overt physical conflict.[20] Traditional military distinctions between offense and defense, or between war and non-war, while still conceptually useful, thus provide an inadequate and even misleading

---

[16] Massimo Durante, "Violence, Just Cyber War, and Information," *Philosophy and Technology* 28 (2015): 369-385; John Stone, "Cyber War Will Take Place!" *Journal of Strategic Studies* 36:1 (2013): 101-108; Michael J. Mazarr, *Mastering the Gray Zone: Understanding a Changing Era of Conflict*. (Carlisle, PA: U.S. Army War College Press, 2015). For other examples of the discussion over the extent to which cyberspace is unique, see Thomas Rid, "More Attacks, Less Violence," *Journal of Strategic Studies* 36:1 (2013): 139-142; Timothy J. Junio, "How Probably is Cyber War? Bringing IR Theory Back Into the Cyber Conflict Debate," *Journal of Strategic Studies*, 36:1 (2013): 125-133; Sean Lawson, "Beyond Cyber Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber Threats," *Journal of Information Technology and Politics*, 10:1 (2013): 86-103; Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* Vol 22 No 3 (2013): 365-404; Stephan Haggard and J. Lindsay, "North Korea and the Sony Hack: Exporting Instability through Cyberspace." *Asia-Pacific Issues*, No. 117 (2015): 3-8.

[17] Gartzke, "The Myth of Cyberwar."

[18] Mazarr, "Mastering the Gray Zone."

[19] This trend echoes Stephen Rosen's theory that wartime innovations only succeed upon the creation of a new strategic vision for their employment — what he calls a "theory of victory." Rosen 1991

[20] The scholar Richard Harknett offered a useful analogy for understanding this predicament. He argued that conflict in cyberspace is akin to a wrestling match: because both opponents are in a state of constant entanglement, it is difficult to determine who is on offense, who is on defense, and who is winning or losing. See Michael P. Fischerkeller and Richard Harknett, "Deterrence is Not a Credible Strategy for Cyberspace," *Orbis* Vol 61(3) (2017): 381-393; Richard Harknett and Emily Goldman, "The Search for Cyber Fundamentals," *Journal of Information Warfare* Vol 15(2) (2016): 81-88; Brad Williams, "Meet the Scholar Challenging the Cyber Deterrence Paradigm," Fifth Domain, July 29, 2017, https://www.fifthdomain.com/home/2017/07/19/meet-the-scholar-challenging-the-cyber-deterrence-paradigm/.

description of this type of cyber activity in practice. What this means for theories of military innovation is that cyber presents a case of neither intra- nor interwar learning — instead, it is both and neither.[21] Given this state of constant conflict, we should thus expect military innovation in cyberspace to display a unique mix of wartime and peacetime innovation patterns.[22]

Fourth, the fact that cyberspace is a domain comprised of information — both the bits and bytes that fuel electronic systems as well as the intelligible content that such systems produce — makes cyberspace uniquely capable of enabling a type of narrative manipulation at a scale that is unprecedented in the history of warfare.[23] The information revolution of the latter half of the 20th century brought about a series of technological changes that dramatically altered the speed and the scope with which information could be collected, stored, processed, and communicated. These changes caused information itself to become a major strategic resource that has since restructured politics, economics, society, and war.

As communication technologies proliferated, the production and consumption of information decentralized, resulting in a diffusion of power beyond traditional state borders and institutions that has carried significant implications for the conduct of war. This diffusion of communication technology threatens to change warfare in the same way that it has changed society: through the proliferation of an information medium that is ubiquitous, instantaneous, and manipulable at the end user level. The resultant target-rich information environment enables a type of epistemological struggle in which it

---

[21] Stephen P. Rosen offers a useful contrast between peacetime and wartime innovation patterns in his book *Winning the Next War*. During peacetime, innovation happens when a new theory of victory is translated into new tasks and performance measures that affect how an organization behaves (20). In contrast, wartime innovation follows the development of new strategic measures of effectiveness that link together a military's strategic goal, the relationship of operations to that goal, and indicators of how well the operations are proceeding (35). Rosen argues that military innovation is required in wartime when either an inappropriate strategic goal is being pursued, or when the relationship between military operations and that goal has been misunderstood.

[22] The academic squabble over whether these persistent conflicts are or are not war is irrelevant to my theory. Perpetual conflict between adversaries, regardless of its formal legal categorization, creates the same sense of urgency and patterns of action-reaction that are necessary to spur wartime innovation impulses.

[23] Peter Singer's *LikeWar* (2018) touches upon this subject through its exploration of the implications of social media to modern conflict.

becomes difficult to discern the true from the false — a fact which certain militaries have been demonstrably more willing and able to exploit for competitive advantage than have others.[24]

From this perspective, the physical effects that cyberspace can or cannot create present less of a military innovation challenge than the cognitive effects produced when the domain is used to undermine or manipulate one's perception of reality. Cyberspace thus poses a unique type of problem for military innovation: how does one develop a new strategic framework for a weapon system whose effects cannot be quantitatively measured, and whose most dangerous employment potentially lies outside of the boundaries of military conflict itself? While militaries have grappled with information warfare for centuries, Western militaries in particular have had difficulty assimilating the non-kinetic aspects of information warfare into their theory and practice of war.[25] Given the evident manner in which cyberspace has changed the global information environment, we should expect to see the same patterns emerge in the U.S. military's choices on how to fight in this new terrain: difficulty in articulating new measures of strategic effectiveness, and a propensity to focus on the domain's technical and physical rather than cognitive potential.

Finally, cyberspace as a medium requires attributes of its practitioners that are not often cultivated in military personnel, and that are often seen as contrary to military good order and discipline: creativity, curiosity, individual autonomy, and a flat interpersonal structure. In order to build an effective cadre of cyber warfighters, one can expect that militaries will have to adapt their traditional personnel structures and promotion incentive programs to reward things that were previously considered counterproductive.

---

[24] Russia is currently the largest perpetrator of such narrative manipulation, both inside and outside the boundaries of military conflict. See Timothy Thomas, "Russia's 21st Century Information War: Working to Undermine and Destabilize Populations," *Defense Strategic Communications: The Official Journal of the NATO Strategic Communications Center of Excellence* 1:1 (2015): 10-25.

[25] As we shall see in later chapters, the trajectory of U.S. information warfare theorizing remained somewhat narrowly focused on denying the enemy use of his communication systems, rather than on manipulation of the content of those systems or the manipulation of the framework through which such content was interpreted. In other words, U.S. information warfare theory has tended to focus on achieving discrete effects on information systems rather than on achieving psychological effects on the mind of the system user.

A Word About Definitions

The terms "cyber" and "cyberspace" are admittedly confusing to those who are not familiar with them, and can often be even more so to those who are.[26] One of the recurring themes in conducting research for this dissertation was in just how much of the military's effort to innovate in cyberspace took place without a unified definition what cyberspace was. For this reason, describing how the military conception of cyberspace became what it is today requires adopting a broader historical perspective that encompasses the antecedent ideas — distinct but related — of information warfare, command and control warfare, and information operations. It also requires adopting a broader definition of cyberspace operations than what has made its way into current joint military doctrine.

Borrowing from Gregory Conti and David Raymond in their book, *On Cyber*, I define cyberspace operations as the attack, defense, or collection of information from other computers, "where computers is used broadly to mean electronic systems that collect, process, store, and communicate information."[27] In this fashion, cyberspace itself becomes "the sum of the computing systems, networks, and data which permeate our global environment."[28] The effects leveraged through this process can be either physical — in which the manipulation of information or an information system can lead to tangible effects in the physical world, such as frying a hard drive or causing a nuclear reactor centrifuge to change speeds — or virtual. This definition of cyberspace contrasts with the tautological offering in Joint Publication 3-12, which defines cyberspace operations as, "the employment of cyberspace capabilities where the primary purpose is to achieve objectives in and through cyberspace."[29]

The definition I have adopted also allows us to see that the the conceptual origins of cyberspace operations long predate the introduction of cyberspace as a term. This means that military service efforts

---

[26] In 2013, at the DEF CON Hacking Conference, the word "cyber" won a DEF CON Recognize award for the worst cybersecurity buzzword.

[27] Gregory Conti and David Raymond, *On Cyber: Towards an Operational Art for Cyber Conflict* (Kopidion Press, 2017), 4.

[28] Ibid., 5.

[29] Department of Defense. *Joint Publication 3-12 (R) Cyberspace Operations.* (Washington, D.C.: Department of Defense, February 5, 2013).

to come to grips with the idea preceded the recognition of what exactly it was that they were attempting to understand. In other words, the military has been attempting to puzzle its way through the problems and challenges of cyberspace for a very long time, albeit under different designations and different conceptual frameworks. The table at the end of this chapter offers a glimpse into this terminological and conceptual evolution at the joint level, while individual chapters will provide further detail into said evolution at the level of the individual services.

Dissertation Roadmap

The remaining chapters will explore the twin topics of military innovation in cyberspace and the role of subcultures on military innovation in greater detail. Chapter 1 introduces a theory of subcultural influence and discusses how that theory might be applied to a historical comparative case study. Chapter 2 tests this theory against the historical development of cyberspace doctrine in the U.S. Army. It demonstrates the effect of subcultures on the Army's approach to cyberspace through an exposition of the interactions between the intelligence, signal, space, electronic warfare, and information operations communities from the late 1980s to the present. These interactions concluded when Army senior leadership simultaneously elevated cyberspace into its own personnel branch and dropped its focus to the level of tactical maneuver.

Chapter 3 tests this theory against the historical development of cyberspace in the U.S. Air Force. The effect of subcultures on the Air Force's approach to cyberspace are made clear through demonstrated interactions of the signals intelligence, communications, space, and strategic nuclear communities over a twenty year period. This interaction concluded with the attempted integration of cyberspace operations into the dominant service culture as the final, digital manifestation of the Air Force mantra of strategic global strike. Chapter 4 provides a final comparative case through a historical study of the development of cyberspace operations in the U.S. Navy. This chapter reveals the critical influence of the Navy's strong

cryptologic community on cyberspace development, both within the service and in how the service interacted with the joint community.

Finally, Chapter 5 concludes by reviewing the dissertation's principle findings, revisiting the theory's implications for ongoing debates in the field, and discussing avenues for future work.

Table 1. Joint Cyberspace Doctrine, 1992-2018

Term	Date Introduced	Definition	Publication
Information Warfare	1992	The competition of opposing information systems to include the exploitation, corruption, or destruction of an adversary's information systems through such means as signals intelligence and command and control countermeasures while protecting the integrity of one's own systems from such attacks.	DoDD TS 3600.1
Command and Control Warfare	1993	The military strategy that implements information warfare on the battlefield and integrates physical destruction. Includes psychological operations and military deception.	JCS Memo of Policy No 30
	1996	The integrated use of psychological operations, military deception, operational security, electronic warfare, and physical destruction, supported by intelligence, to deny information to, influence, degrade, or destroy adversary C2 capabilities while protecting friendly capabilities against such actions.	JP 3-13.1
Information Operations	1996	Redesignated "information warfare" as "information operations" to reflect a sensitivity to domestic and foreign concerns about the potential militarization of the internet. Also introduced the term "computer network attack" as "operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."	DoDD S-3600.1
	1998	Described IO as a broadening of IW with the addition of computer network attack. IO takes place in the information environment, described as "the aggregate of individuals, organizations, or systems that collect, process, or disseminate information" as well as the information itself.	JP 3-13.1
	2003	Declares IO a core capability of future military forces that must be fully integrated into deliberate and crisis action planning.	DoD IO Roadmap
	2006	Removed IW from the joint doctrinal lexicon, updated the description of the five core IO capabilities, and established the computer network operations as consisting of computer network attack, computer network defense, and computer network exploitation. Adds "cyberspace" — "the notional environment in which digitized information is communicated over computer networks" — as a component of the information environment.	JP 3-13
Cyberspace Operations	2013	Cyberspace operations employ capabilities "to create effects which support operations across the physical domains and cyberspace," while IO employ "information-related capabilities […] to influence, disrupt, corrupt, or usurp the decision-making of adversaries." Marked the end of the DoD's conception of cyberspace as a subset of IO.	JP 3-12
	2018	Cyberspace operations is the employment of cyberspace capabilities where the primary purpose is to achieve objectives in and through cyberspace. Cyberspace is a global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.	JP 3-12

CHAPTER 2 | **A Theory of Subcultural Influence**

In this chapter, I propose a theory of subcultural influence on the process of military innovation. The central argument is that organizational subcultures exert a significant influence on the process of military innovation, and that this influence is higher when conditions of uncertainty about the nature of an innovation prevent the issuance of clear guidance from service senior leadership.

Organizations, Human Psychology, and Military Innovation

The classical model of rationality assumes that an actor knows all relevant alternatives, their consequences and probabilities, and operates in a predictable world without surprises.[30] When applied to organizations, this assumption presupposes that an organization knows both what it wants and how to get there. Yet what happens when an organization has to fundamentally redefine its goals in the face of change? What happens to the assumptions of rationality under conditions of uncertainty, when an organization may not know what it wants? This question is pertinent to the study of military innovation, since military innovation often has less to do with deciding *how* to achieve something than in deciding *what* exactly should be achieved.

New military technologies such as the submarine or unmanned aerial system require the development of what Stephen Rosen calls "new ways of war," or new conceptual frameworks on what the desired end state is and how to achieve it. For example, the British, French, and German armies had all seen the same new armored technologies, under the same war fighting conditions, on the battlefields of World War I, yet it was only the German army that could successfully envision how this technology would affect future warfare. As a result, they alone were able to use this vision to create an integrated concept of

[30] Herbert A. Simon, "The Scientist as Problem Solver." In *Complex Information Processing: The Impact of Herbert A. Simon,* ed. D. Klahr, K. Kotovsky (Hillsdale, NJ: Erlbau, 1989), 373-398.

operation for its employment.[31] Similarly, the American Army in Vietnam proved incapable of correctly interpreting the lessons of an unconventional battlefield through anything but its preexisting institutional biases toward conventional war, in spite of overwhelming evidence that such methods were ineffective.[32] More recently, the U.S. and Russian armies chose radically different strategies toward electronic warfare in the 1990s, with the U.S. Army largely abandoning both its material capabilities and its doctrine while the Russian Army steadily developed a new operating concept that proved more befitting of the future electronic battlefield. What accounts for these differences in approach?

A BRIEF REVIEW OF THE LITERATURE

Scholars of traditional military innovation have offered a number of explanations for divergent innovation outcomes. These may be broadly divided into a few different theoretical perspectives. Organization theory posits that a military's resistance to change is the result of structural factors that shape institutional behavior. An organization's behavior is less the result of choice than it is of procedural outputs.[33] Even when individual actors within an organization desire change, the structural mechanisms of the system can inhibit those actors from creating it.[34] Change within an organization therefore demands an exogenous catalyst in one of three forms: external pressure, a need for survival, or failure. The relative importance of the sources of these catalysts are a subject of debate among scholars.

Barry Posen, for example, argues that this external pressure often takes the form of civilian leadership forcing change from without based upon a superior understanding of the strategic environment.[35] Stephen Rosen argues that it takes the form of military leaders forcing change from within

---

[31] Williamson Murray, "Armored Warfare: The British, French, and German Experiences," in *Military Innovation in the Interwar Period*, ed. Williamson Murray and Allan R. Millett (New York: Cambridge University Press, 1996), 34-45.

[32] Andrew F. Krepinevich Jr., *The Army and Vietnam* (Baltimore: Johns Hopkins University Press, 1986).

[33] Graham Allison and Philip Zelikow, *Essence of Decision: Explaining the Cuban Missile Crisis (2nd Edition)* (New York: Longman, 1999), 2-11.

[34] Janine Davidson, *Lifting the Fog of Peace: How Americans Learned to Fight Modern War* (Ann Arbor: The University of Michigan Press, 2010), 11. Chapter 1 of this book inspired much of my summary on the military innovation literature.

[35] Posen, *The Sources of Military Innovation.*

through the deliberate adjustment of personnel promotion pathways.[36] Thomas Mahnken contends that intelligence about the enemy is the most important motivating force behind military innovation.[37] Kimberly Zisk places a similar emphasis on the role of threats to a military's survival, but, in a nod to bureaucratic politics theory, she argues that militaries are far more responsive to domestic threats to their resourcing than they are to foreign threats to national security.[38] Regardless of its source, organization theory posits that change will only last when the underlying structures and processes are also changed to create an enduring accommodation of the new system. This idea is well demonstrated by Rosen's work on the relationship between innovation and military career incentive structures, and can be seen more contemporarily in each of the services' respective decisions to establish cyber warfare career management structures.[39]

In contrast to the structural explanation of organization theory, the process-driven bureaucratic politics model argues that military leaders are fundamentally motivated by the need to promote the importance of their organization while preserving what Morton Halperin famously called their "organizational essence."[40] Bureaucratic politics is thus often summarized by the Graham Allison adage, "where you stand depends on where you sit."[41] Internal domestic rivalries, turf battles, and measurements of an organization's prestige are thus seen as the primary influencers on organizational behavior and decision-making. Under the bureaucratic politics model, an organization will reject any new innovation that challenges either its essence or its access to resources. As an example from within the U.S. cyber case study, the failure of the Army's information warfare community to exercise enduring influence on the shape of cyber doctrine could be partially attributed to this community's struggle to clearly articulate its

---

[36] Rosen, *Winning the Next War.*

[37] Mahnken, *Uncovering Ways of War.*

[38] Zisk, *Engaging the Enemy.*

[39] Rosen, *Winning the Next War.*

[40] Morton H. Halperin, *Bureaucratic Politics and Foreign Policy,* (Brookings Institution Press, 2002).

[41] Allison, *Essence of Decision*

own purpose, and to clearly advocate for that purpose among competing institutions. Halperin's idea of organizational essence could also partially explain the U.S. Army's institutional reluctance to embrace counterinsurgency doctrine throughout the 1960s and 70s, in spite of the President's urging, since small wars ran counter to the doctrine of large formations and massed firepower that was expected to defeat the Soviet Union.[42]

Finally, theories of organizational culture — which encompass the overlapping concepts of organizational essence, institutional memory, and organizational personality — suggest an iterative relationship between experience, culture, and learning that will determine "how effectively organizations can learn from their own experiences."[43] Elizabeth Kier defines organizational culture as, "the set of basic assumptions and values that shape shared understandings, and the forms or practices whereby these meanings are expressed, affirmed, and communicated to the members of an organization."[44] These shared beliefs generally emerge from an organization's formative experiences and are reinforced through successful practices over time.[45] Once codified, culture shapes how an organization responds to challenges, opportunities, and constraints by providing a set of heuristics with which to evaluate new information.[46]

Organizational culture is also closely related to the idea of institutional memory, or the conventional wisdom of an organization about how to perform its tasks.[47] Culture thereby contributes to Carl Builder's idea of organizational personality, described as a "'face' that can be remembered, recalled, and applied" in evaluating the future behavior of a military service.[48]

---

[42] Krepinevich, *The Army and Vietnam*. The U.S. Army's failure to embrace counterinsurgency is often used as a contrary argument to Posen's idea that civilian leaders can force military institutions to change.

[43] John A. Nagl, *Learning to Eat Soup with a Knife: Counterinsurgency Lessons from Malaya and Vietnam* (Chicago: The University of Chicago Press, 2002), 6.

[44] Elizabeth Kier, "Culture and Military Doctrine: France Between the Wars," *International Security* 19/4 (Spring 1995): 69

[45] Edward H. Schein, *Organizational Culture and Leadership*, 3rd ed. (San Francisco: Jossey-Bass, 2004),15-16.

[46] Austin Long, *The Soul of Armies: Counterinsurgency Doctrine and Military Culture in the U.S. and U.K.* (New York: Cornell University Press, 2016), 16.

[47] Nagl, *Learning to Eat Soup with a Knife*, 6.

[48] Builder, *Masks of War.*

By examining an organization's cultural predisposition toward certain concepts, organizational culture theory offers a possible explanation for why certain innovations are embraced while others are ignored. Terry Pierce offers an additional compelling answer to this question of enduring versus ephemeral innovation that is well nested within the theory of organizational culture. He argues that the most effective way to ensure an innovation lasts is to disguise it within an organization's existing language and culture.[49] Echoes of this principle can be seen in the Army's embrace of conventional maneuver terminology to describe cyber doctrinal concepts, or in the Air Force's assimilation of cyberspace capabilities into the weapons system format that governs the management of conventional Air Force platforms.

Dima Adamsky further extrapolates the importance of culture from the organizational to the national level in arguing that a nation's strategic culture dictates the process of how its military innovates.[50] He states that a national cognitive style will shape a state's strategic behavior, and will therefore constitute the ideational foundation of its military innovation.[51] Deborah Avant adds another layer to the cultural analysis by examining the impact of political systems on the internal elements of military organizations.[52] Avant argues that the overall government structure in which a military is situated, and the resultant pattern of military oversight it creates, can influence military culture by giving militaries varied degrees of flexibility or bias to change. Regardless of the name given to this cultural variable, scholars agree that an organization's history affects the development of an organization's personality, which in turn affects the ability of that organization to learn from new experience. In this sense, culture can provide a stable organizational essence that outlasts structural change.

---

[49] Terry C. Pierce, *Warfighting and Disruptive Technologies: Disguising Innovation* (New York: Frank Cass, 2004), 31.

[50] Dima Adamsky, *The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel* (California: Stanford University Press, 2010).

[51] Ibid. 15.

[52] Avant, *Political Institutions and Military Change.*

HUMAN PSYCHOLOGY AND ORGANIZATIONAL BEHAVIOR

However, simply recognizing the existence of these cultural influences on organizational learning does not give us a thorough understanding of why they work. For this, we must briefly discuss how organizations function, as well as the underlying psychological mechanisms that govern how individuals make decisions during periods of uncertainty and change. March and Simon, in their seminal work on organizations, describe an organization as a system of "coordinated action among individuals and groups whose preferences, information, interests, or knowledge differ."[53] Organization theories describe how these systems act to convert conflict into cooperation, to mobilize resources, and to coordinate effort among members to facilitate organizational survival. Organizations accomplish these shared goals through four primary structural mechanisms: control over information, control over incentives, task differentiation, and delegation of decision-making. Through these processes, organizations create shared stories, and weave them into an overarching organizational ethos that shapes the goals, loyalties, and incentives of their participants. In other words, organizations "weave supportive cultures, agreements, structures, and beliefs" around the natural functions and activities which are designed to increase efficiency and foster unity toward the achievement of organizational goals.[54]

Efforts to increase efficiency through task differentiation and specialization results in the creation of distinct organizational subunits. These subunits serve functions that nest within the organization's higher purpose, but they can develop unique personalities and goals of their own that can then conflict with the higher organization. The result is often fractionalization and an internal competition for resources, power, and prestige. Consider, for example, the historical tension between pilots and surface warfare officers in the U.S. Navy. The evolution of aircraft from a reconnaissance asset to an independent attack platform fundamentally transformed the role of surface ships in the Navy. As airplanes made the

---

[53] James G. March and Herbert A. Simon, *Organizations,* 2nd Ed. (Cambridge: Blackwell, 1993), 2.

[54] Ibid.

battleship obsolete, the surface community had to rethink the entire schema of how best to fight at sea.[55] This experience led to an intra-service feud between pilots and ship drivers over resources, prestige, and who controls the Navy's "organizational essence" that continues to the present day. One can see a similar phenomenon in the U.S. Air Force, in which the division between tactical fighters and strategic bombers led to significant intra-service competition for the first several decades of the service's existence.

These subunits possess many of the same mechanisms that work to mediate decision-making at the higher organizational level. Specifically, individuals within a certain sub-organizational community can develop a tendency to evaluate action only in terms of that specific community's perspective. March and Simon describe several mechanisms at work in this process:

> At the individual level, there is reinforcement through selective perception and rationalization. The propensity of individuals to see those things that are consistent with their established frame of reference is well established in individual psychology. Perceptions that are discordant with the frame of reference are filtered out before they reach consciousness, or are reinterpreted or "rationalized" so as to remove the discrepancy. The frame of reference serves just as much to validate perceptions as the perceptions do to validate the frame of reference. At the organizational level, there is reinforcement through the content of in-group communication, which affects the focus of information. Finally, there is reinforcement through selective exposure to environmental stimuli. The division of labor within the organization affects the information that members receive. Thus, perceptions of the environment are biased even before they experience the filtering actions of the frame of reference of the perceiver.[56]

In other words, the experiences derived from particular organizational subgroups bias decision-making by providing frames of reference through which new information is interpreted. These frames of reference will often appear as shared classification schemes or a common technical vocabulary. Anything that is easily described and discussed in terms of this shared vocabulary will be communicated readily in the organization; anything that is not will be communicated only with difficulty. Hence, the world tends to be perceived by the subunit's members in terms of the particular concepts that are reflected in the subunit's

---

[55] Murray and Millett, *Innovation in the Interwar Years*, chapter 5.

[56] March and Simon, *Organizations*, 174.

vocabulary.[57] To describe this phenomenon using the language of subgroups provided above, a Naval aviator will have an instinctively different conception of the purpose of air power to sea control — in which air power is the supported rather than supporting function — than would a surface warfare officer, based upon the goals, attitudes, and perceptions of their specific organizational subgroups. Likewise, a strategic bomber pilot will have a different set of beliefs on how to best to leverage air power than will a tactical fighter pilot, based upon the manner in which he has been trained and the unique strengths of his particular skill set.[58]

Efforts to foster unity at the level of organizational subunits and the organization writ large can have consequences for individual and collective decision-making. Because organizations are not optimized to contend with novelty, they often deliberately reduce the complexity of new situations in order to fit them into a preexisting decision-making schema. Many of the processes designed to reduce uncertainty ultimately do so by decreasing the individual and collective propensity to search for alternatives.[59] Structural mechanisms are then compounded by psychological mechanisms which can serve the same purpose at the individual level, such as an over-reliance on heuristics that deliberately ignore information in order to make decisions more quickly.[60] Use of heuristics tends to increase during periods of heightened uncertainty, when relevant alternatives, consequences, and probabilities are unknown — in other words, when the assumptions of the classical model of rationality may not apply.[61] Yuen Foong Khong offered just such an example of how heuristics can combine with analogical reasoning to affect leader decision-making. He argued that policymakers have a repertoire of historical analogies stored in their memories,

---

[57] March and Simon, *Organizations*, 174.

[58] A similar contrast can be found in recent Army debates about whether to add a 30mm cannon to the Stryker infantry carrying platform. Tankers, accustomed to fighting with and from their vehicles, tended to argue in favor of adding the cannon, while the infantry, accustomed to using vehicles to get to the fight before dismounting, argued against it. See Andrew Gregory, "Lethality Upgrade: Why a New Stryker Variant is Needed on the Modern Battlefield," War on the Rocks, April 12, 2017, https://mwi.usma.edu/lethality-upgrade-new-stryker-variant-needed-modern-battlefield/ for the armor perspective and James King, "Never Bring a Stryker to a Tank Fight," Modern War Institute, May 2, 2017, https://mwi.usma.edu/never-bring-stryker-tank-fight/ for the infantry perspective.

[59] March and Simon, *Organizations*, 58.

[60] Gerd Gigerenzer and Wolfgang Gaissmaier, "Heuristic Decision Making," *Annual Review of Psychology*, Vol 62 (2011) 451-482.

[61] Simon, "The Scientist as Problem Solver."

and will use the availability heuristic to draw upon the ones that come most readily to mind when confronted with a similar situation.[62]

Additional work has suggested that emotion and memory can play an outsized role on human decision-making during times of uncertainty.[63] Emotional reactions, which take place prior to conscious cognition, can affect human decision-making in social settings as can the strength of the memories we hold of certain events. Memories with a high emotional content may therefore be preferentially recalled over those with low emotional content.[64] The tendency to subliminally favor memories which are higher in emotional content has been demonstrated to affect decision-making in war and crisis, and suggests that the type of problem-solving strategy employed may depend as much on the problem-solver's past experiences as on the characteristics of the problem.[65] Emotion-based pattern recognition tends to further treat the connection between past events and current decisions as implicitly "obvious" such that further efforts to explain the requisite similarity between the two circumstances are seen as unnecessary.[66] Thus, lengthy searches for data that could confirm or disconfirm alternative strategies are often replaced by decisions which serve as a response to one's first exposure to the problem. This type of pattern recognition has value in that it enables people to react more quickly to complex situations by preparing the body for action; however, it can also unhelpfully skew decision-making at times when more rational deliberation might be necessary.

---

[62] Yuen Foong Khong, *Analogies at War: Korea, Munich, Dien Bien Phu, and the Vietnam Decisions of 1965* (Princeton University Press, 1992).

[63] Stephen P. Rosen, *War and Human Nature* (Princeton University Press, 2007).

[64] Stephen P. Rosen, *War and Human Nature*, 39.

[65] Ibid., 2.

[66] Ibid., 40.

A Theory of Subcultural Innovation

THEORY

Given the above, we can identify a number of mechanisms by which organizational culture can affect decision-making in a way that could influence processes of military innovation. First, culture can lead to patterns of behavior which are not deliberately considered, prepared, or pre-planned. In other words, cultural influences can act to preclude rational choice by enabling and encouraging ingrained behavioral habits within organizations at the expense of what might be strategically optimal. Culture can therefore mediate an organization's ability to perceive alternate choices by filtering those alternatives through preexisting frames of reference, through particular communication patterns, or by excluding their consideration entirely by virtue of biased perceptions of the external environment that are derived from the internal environment of the organizational subunit.

Based upon the natural tendency of organizations to simplify complexity, we can expect individual decision-makers within those organizations to do the same through a reliance on heuristics, memory, and emotion such that the final outcome is likely to conform to pre-existing organizational patterns of behavior. Furthermore, we can expect these effects to be higher during periods of uncertainty. Military culture should thus have a significant influence on how a military organization perceives an innovation problem: by infusing the decision-making process with a specific logic, culture will shape the parameters of the problem before the exercise of instrumental rationality.

One could also envision an alternate hypothesis about the effect of uncertainty, in which conditions of chaos lead to an increased willingness to question existing systems and to discard existing culture in order to bring about rapid change. Under this hypothesis, uncertainty would not cause an organization's reversion to preexisting habits, but would increase its willingness to "do whatever it takes" to achieve an objective or solve a problem. What determines which of these pathways an organization will take during the process of learning? What determines the balance between old and new ways of doing things?

Military innovation in cyberspace appears to include a mix of both strategies during two distinct phases of change: the period from the early 1990s to the creation of U.S. Cyber Command in 2009, and the period since. The impact of service subculture was most evident during the initial exploration phase of the 1990s and early 2000s, when each service pursued its own conception of network warfare largely independently from one another. Because concepts of network and information warfare were both poorly defined and poorly understood during this initial period, the bottom-up interaction among service subcultures was far more consequential to the ultimate shape of service doctrine than was any centralized strategic vision from on high.[67] Subcultural influences affected everything from the intellectual development of doctrine to patterns of personnel management and training. As such, they help to explain a substantial amount of variation in the services' ultimate cyber output during the early years of cyber innovation.

In contrast, the expansion of joint cyber organizations in the late 2000s, particularly the creation of Cyber Command in 2009, had the effect of formalizing the interactions among the military services and partially standardizing the thinking. The creation of Cyber Command thereby decreased the relevance of individual service subcultures to the process of innovation, while it increased the relevance of the dominant service culture. This period of joint expansion resulted in the creation of both joint and individual service doctrine as well as the partial standardization of operations and training across the military services. Importantly, however, the management of cyberspace personnel was not standardized, which allowed us to continue to observe differences across the services through this period.

The above suggests a two-stage process of innovation. During the first stage, when a technology and the conditions surrounding it are poorly understood, the shape of an innovation will be driven by the cultural instincts of whichever organizational subcommunities are given responsibility for the technology. This subcultural influence will be especially salient for those innovations, like cyberspace, which exist at the boundaries of other domains in a way that makes it difficult to ascribe ultimate responsibility for

[67] See Michael Warner, "Notes on Military Doctrine for Cyberspace Operations in the United States: 1992-2014," *The Cyber Defense Review*, August 27, 2015, for background into what the joint doctrine looked like during this period.

them.[68] Furthermore, these cultural instincts will often persist past the point of their original functional relevance, and as a result will unduly shape the approach towards a new technology regardless of what that technology's intrinsic attributes and requirements might demand. As clarity over the nature of a technology starts to emerge, organizations will engage in a learning process that allows for deviation from routine based upon a clear vision of that technology's purpose. This learning process will be driven by a combination of exogenous shocks, and by the process of bargaining between different organizations and organizational subcultures over how to interpret those shocks.

HYPOTHESES

Building upon these specific mechanisms, I hypothesize that the path of a military innovation is driven by patterns of behavior ingrained in service subcultures, and that the influence of these subcultures is higher during periods of uncertainty, when the impact of an exogenous shock is unclear. When confronted with an unstructured problem, one that does not fit readily into preexisting processes or schemas, an organization's behavior will be determined by the prior skills and competencies of its personnel. In other words, organizations do not innovate from a blank slate, even when that is what they may desire. Instead, they do what they know how to do, in the way they know how to do it, with the resources readily at hand. These skills and competencies, in turn, are shaped by the subcommunities from which the personnel emerged. We can therefore predict the shape of the doctrinal outputs based on the specific natures of the groups that have influenced them.

Furthermore, because organizational cultures are not monolithic, competing groups within a service will have differing interpretations of the purpose and potential of a new technology. These groups will compete for influence over whose interpretation of the problem should prevail. Studying the development of an idea within an organization will therefore require studying the evolution of that idea among the different functional subcommunities an organization contains. The mechanism described

[68] Murray and Millett, in *Military Innovation in the Interwar Period*, documented a similar effect with the evolution of amphibious landings (at the border between land and sea) and close air support (at the border between land and air).

above at the level of the broader organization will still apply at the level of an organization's subcultures, such that we can expect these various subunits to frame a new idea from within the existing parameters of their own experience rather than from a so-called blank slate.

Given the above, I argue that under conditions of high uncertainty about the emerging character of warfare, when there is no shared consensus about the potential impact of a new technology, and thus little top-down guidance as to what direction that technology should take, organizational service culture will be the primary determinant of the character of new doctrine: as information regarding the nature of a change is filtered through established frames of reference, an organization or a sub-component of that organization will implicitly revert to an interpretation of change that does not disrupt what it already knows how to do. Consequently, this reversion will increase the likelihood that the application of a new technology will fall within existing operational frameworks, at least initially, rather than demand a new one. The driving condition for this theoretical framework is uncertainty about the emerging character of warfare and about the nature of the particular innovation under question. This uncertainty, and the resultant lack of top-down guidance it creates, will afford greater bottom-up latitude for the service subcommunities to advocate for their specific vision across the broader military force.

These principles lead to the following predictions:

> **H1:** When uncertainty about the nature of an innovation is high, and top-down guidance about how to proceed is lacking, the initial path of an innovation will be driven by patterns of thought and behavior ingrained in the service subcultures which are given responsibility for it. Conversely, when uncertainty about the nature of an innovation is low, the path of an innovation will be driven by clear direction given from senior service leadership, with less opportunity for contrary subcultural development.
>
> **H2:** As clarity about the nature of an innovation emerges over time, a process of learning will emerge in which the role of subcultures will diminish, replaced by the broad vision of the military service writ large and the increasingly clear strategic incentives created by external threats. Competition among different ideas will be resolved in a way that aligns with the broader service mission and the dominant service culture.

What do I mean by service culture and service subculture?[69] By service culture, I am referring to the overarching shared identity of a military service — as in the shared identity of the Army, Navy, or Air Force. By service subculture, I am referring to the same sense of identity found in the task-specialized subunits that exist within each of the bigger services, such as pilots versus submariners in the Navy, or infantry versus artillery in the Army. Military subcultures are differentiated according to what function they perform for the larger organization and, importantly, by the extent to which that function exists at the core or the periphery of the service's main purpose. Identity can be shared across subcultures, independent of task-differentiation, according to this core versus peripheral distinction, a phenomenon which is captured by the U.S. Army's traditional distinction between the combat and combat support functions.[70] Military policing, for example, would be considered a peripheral — albeit at times essential — function to the Army's core purpose of closing with and destroying the enemy, in contrast to the functions performed by the infantry and armor branches.

How will interaction among these communities be resolved? What dictates the nature of the final doctrinal outcome? As clarity about the nature of an innovation emerges over time, driven largely by exogenous shocks — in other words, by vivid examples of an innovation put to use — a process of learning will emerge in which the role of subcultures will diminish, replaced by the broad vision of the military service writ large and the increasingly clear strategic incentives created by external threats. Competition among different ideas will thus be resolved in a way that aligns with the broader service mission and the dominant service culture.

There are a number of subcultures of interest in the historical evolution of cyber doctrine across the services, to include electronic warfare, intelligence, and communications. By studying the interaction of these and other subcultures over time — as in, who owned the mission when, and what happened as a

[69] For the remainder of this dissertation, I will use the terms subculture and subcommunity interchangeably.

[70] Formerly, this distinction fell into three classes: combat arms, combat support, and combat service support. Now, it falls into two classes: operations and operations support. The Army's removal of branch insignia from the new Army Combat Uniform in 2004 was an attempt to soften these types of combat/non-combat distinctions, based partially on an understanding of the current Iraq and Afghanistan engagements as lacking geographic divisions between forward and rear areas. Each of the services maintains a similar distinction between its fighting and support components.

result — we can gain a better understanding of how bargaining among competing theories of war can affect the way a service learns in the face of change.

MEASURING CULTURE

For the purpose of this study, I define culture as a set of shared norms, beliefs, and assumptions about an organization and its mission. Because the shared beliefs that comprise culture are often unstated, the influence of culture can be difficult to measure even while the phenomenon of culture can be relatively easy to observe. Rather than attempting to measure culture, I will instead anchor my assessment of service cultures and subcultures along four dimensions that were selected for their relevance to the cyberspace domain: tolerance of risk, delegation of decision-making, mission orientation, and technological aptitude. Organizations that differ on some or all of these dimensions are expected to adopt different approaches to cyberspace operations.

Acceptance of the above dimensions as the basis for a cultural comparison rests upon the assumption that cyberspace has a particular nature, and that those who most readily adapt to this nature will be able to operate in cyberspace more successfully than those who cannot or do not. This assumption treats cyberspace just as it would the air, land, and sea domains whose particular characteristics shape the perspectives of the services that operate in them. Because cyberspace is comprised of shifting and manipulable terrain, it requires a level of speed and flexibility in its operations that in turn demands a relatively flat organizational structure. In the language of the dimensions described above, success in cyberspace requires a high tolerance of risk, low delegation of decision-making, and high technological aptitude.

Tolerance of risk refers to the extent to which a community is risk acceptant or risk averse. It is closely related to delegation of decision-making, which refers to whether consequential decisions are retained at high or low echelons of leadership. More risk-acceptant communities are expected to delegate decision-making and decision-making authority to low levels of leadership, based on a principle of trust

that those decisions will implicitly support the best interest of the organized whole. Risk acceptant communities will prize individual initiative, and will rely more upon things like professional judgment or expertise as a guarantor of sound decision-making than on procedures or checklists. As a result, risk acceptant communities will tend to have a faster decision cycle than their risk averse counterparts.

In contrast, risk-averse communities tend to centralize decision-making at high levels of authority, where plentiful information and a wider perspective support a more comprehensive and holistic cost-benefit analysis. For the risk-averse, standardized procedures, checklists, and lengthy review processes act as safeguards against human error. These methods become habitual, and are relied upon even when circumstances might otherwise allow or encourage deviation. Low-level initiative is discouraged, which results in a slower and more time-consuming decision-making cycle. Taken together, the dimensions of risk aversion and delegation of decision-making can anticipate the extent to which management within a community is hierarchical or flat, as well as the consequent level of individual initiative the community encourages. These management practices will in turn have an effect on the speed and efficiency of organizational operations.

The category of mission orientation describes different concepts depending on the level at which it is applied. When speaking at the level of an entire military service, mission orientation describes the service's relationship to the levels of war: strategic, operational, and tactical. Specifically, it describes whether the service is strategic or tactical in its focus, in terms of both how the service is employed and how its leaders tend to think. Strategy concerns itself with national objectives and the instruments of national power. It addresses the general question of "what is it that we must accomplish." Tactics concerns itself with the employment of forces to achieve victory in specific military engagements. Accordingly, the strategic level of war is the realm of ends and means. The tactical level of war is the realm of skirmishes, engagements, and battles.[71]

---

[71] *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms* (Feb 15, 2016), 227, 234.

While each service ultimately fulfills a strategic purpose as an instrument of national policy, the manner and the environment in which the services pursue that purpose will foster different ways of thinking that can be usefully categorized according to the rough bifurcation between strategic and tactical. Broadly speaking, a strategic-minded service will maintain an expansive understanding of its own purpose that will support an institutional self-perception of global application and flexibility. For example, the Air Force, as an instrument of global strike born of the boundless air domain, describes itself and its conception of purpose in distinctly strategic terms. Air Force Doctrine Document 1, *Basic Doctrine*, states that "Airpower is an inherently strategic force" due to the fact that its forces "can hold an enemy's strategic centers of gravity and critical vulnerabilities directly at risk immediately and continuously."[72] This global, strategic focus is integral to the concept of Airmindedness, or a broad way of thinking about war that is unique to the Air Force alone.

A tactically-minded service, on the other hand, will be more concerned with individual theaters, battles, and campaigns, and will think in terms of objectives which are clearly delineated in both temporal and terrestrial terms. The Army and Marine Corps provide examples of a tactically-minded service. However, this classification between strategic and tactical is necessarily imprecise, and is not meant to be exclusive: to say that a service is strategic, for example, does not imply that it cannot be used tactically, or that it never finds itself in tactical engagements. Similarly, a tactically-oriented service like the Army is still, writ large, employed in strategic fashion for the pursuit of national objectives, and thus must foster a degree of strategic-mindedness in its senior leadership. Nevertheless, the general strategic/tactical bifurcation can help to describe, in general terms, the intellectual and operational tendencies of a service's personnel.

At the level of the service subculture, mission orientation describes the subculture's relationship to the service's warfighting center. In other words, does the subculture engage in direct combat, or not? Does it execute operations, or does it support them? How far from the proverbial tip of the spear does the

---

[72] *Air Force Doctrine Document 1: Basic Doctrine* (Feb 27, 2015), 34.

service subculture fall? Each of the services has a different way of describing these core and peripheral communities, but all share an institutional distinction between the so-called warfighters and those who support them.[73] A service subculture's placement as either a core operational function or a mission support function will dictate a number of its subsequent cultural attributes and management practices, from personnel management and promotion, to how the subculture thinks about war, to the broader levels of institutional prestige it does or does not enjoy.

Finally, technological aptitude describes the subculture's relationship to technology. Is the subculture technologically-dependent, or technologically averse? To what extent does it value or cultivate individual technological aptitude and skill? Does it encourage specialization or generalization? The answers to these questions are largely, but not entirely, a reflection of the subculture's proximity to different types of technology and technological platforms. Aircraft pilots, for example, will tend to place a higher priority on technological aptitude than would, say, the community of Army infantrymen.[74]

It is important to note that technological dependence does not necessarily breed the level or type of technological competence that defines today's cyberspace community. The communications communities of each military service, for example, must be familiar with the different types of communications technology that the service operates. This familiarity leads to a type of technical competence in the specific functioning and application of those systems. However, the service provider mindset from which these communities operate has the simultaneous effect of dulling the type of creative or exploratory instinct that has come to define the technologist cult of cyberspace. This dulled creative instinct helps to explain the difficulty that communicators across the services have had in adapting to the paradigm shift that cyberspace operations demand. Thus, the dimension of technological aptitude refers

---

[73] These distinctions, by service, are as follows: combat arms and combat support (Army), operations and operations support (Air Force), unrestricted line and restricted line (Navy).

[74] *Air Force Officer Classification Directory (AFOCD): The Official Guide to Air Force Officer Classification Codes*. Air Force Personnel Center. April 30, 2018.

to the extent of a subculture's technological curiosity as well as its level of baseline technological familiarity.

These four dimensions are obviously not exhaustive. Furthermore, they do not address the competing technical and psychological orientations toward cyberspace that most notably contrasts U.S. cyber doctrine with the information security doctrine of Russia. However, they represent a useful reference point upon which to anchor an initial exploration of the relationship between organizational culture and cyberspace operations in the case of the U.S. military. In the following chapters, I begin my characterizations of each service with a description of the domains in which they operate, and then go on to describe the cultural attributes that result. I then describe the service subcultures — and the services, where appropriate — according to the dimensions outlined above. I derive these characterizations from a combination of written doctrine, service histories, professional journal articles, and interviews.

MEASURING DOCTRINE

The distinction between military culture and military doctrine is often misunderstood. Broadly speaking, culture constitutes what an organization implicitly believes, while doctrine defines what an organization explicitly does. These two concepts are distinct but related. Doctrine is the formal expression of how a military organization intends to fight. It further serves as the "conceptual core around which decisions must be made concerning how the force should be organized, trained, and equipped."[75] As such, it is typically articulated and transmitted through physical means, such as formal publications, professional journal articles, operations orders, and the like. Culture, which provides the framework on which doctrine is built, is more often transmitted through inarticulate means such as shared experiences and shared environments. Furthermore, doctrine changes over time in every military organization, but culture does not. The U.S. Army, for example, is currently on its fifth iteration of doctrine since the 1950s, each of

[75] Harold R. Winton, "On Military Change," in *The Challenge of Military Change* ed. David R. Mets and Harold R. Winton.

which has emphasized a slightly different vision of war while remaining constant with an unchanging Army culture.[76]

Doctrine also permeates the entire organizational structure of a military service: it influences how a service organizes, what it prioritizes, and how it promotes. Doctrine facilitates communication between personnel, establishes a shared professional culture and approach to operations, and serves as the basis for curriculum in a service's professional schooling system. Doctrine is thus an ideal place to forge an understanding of how a service sees itself and its role. Furthermore, the totality of doctrine to a service means that we can understand doctrine not only by how it is written, but by how it affects organizations, personnel development, and training — an important point, given that the release of written doctrine often lags behind these larger, more visible service shifts.[77] Accordingly, the use of the word "doctrine" refers to the whole of how a service approaches a particular aspect of warfighting, and can be measured by both its codified written doctrine as well as its organizations, training, and personnel management practices.

A service's specific cyber doctrine can be further understood to describe a military's behavior in and through cyberspace — how a military conceptualizes of cyberspace, how a military uses cyberspace to achieve its objectives, and how it integrates cyberspace with operations. One can thus measure the centrality of cyberspace operations to a service's core conception of itself by the centrality of cyberspace operations to a service's core doctrine. One can further measure this centrality by assessing changes in how the service organizes, trains, and equips for cyberspace operations, as well as how it approaches personnel management.

---

[76] In order, these iterations have emphasized: dispersal and atomic firepower (1950s), conventional mechanized offenses supported by helicopter mobility (1960s), conventional mechanized defense (1970s), combined air-ground operations incorporating deep attacks (1980s), and the most recent concept of multi-domain battle (2000s). See Robert Doughty, *The Evolution of U.S. Army Tactical Doctrine, 1946-1976* (Leavenworth, KS: Combat Studies Institute, 1979), Ingo Trauschweizer, *The Cold War U.S. Army: Building deterrence for Limited War* (Lawrence: University Press of Kansas, 2008), and Benjamin M. Jensen, *Forging the Sword: Doctrinal Change in the U.S. Army* (Stanford: Stanford University Press, 2016).

[77] Consider that the creation of both Army Cyber Command and the 17-series career field proceeded the release of the Army's first cyber doctrinal publication, Field Manual 3-12, *Cyberspace Operations*, by several years.

Finally, in studying doctrine, it is important to note two things. First, while doctrine is authoritative, it is not dogmatic.[78] Doctrine is less a prescribed set of rules than it is a set of principles from which service members may deviate if the situation warrants.[79] Second, written doctrine itself often represents the culmination of a slow process of institutional change across a variety of measurable dimensions. In other words, doctrine tends to reflect shifts that are already underway within a service; rarely does the release of doctrine drive these shifts. As such, written doctrine is as much a description of how things already are as it is a prescription for how things ought to be. Studying doctrine as an output thus requires looking at changes to service organizations, training strategies, and personnel management practices as well as changes to formal written publications.[80] I use each of these metrics to assess doctrinal change in the remaining chapters.

Alternative Explanations

There are a number of alternative explanations that could explain an organization's behavioral trajectory in the face of an innovation problem. I will present two such explanations here. The difficulty of effectively describing and measuring culture as a scientific variable makes these alternative explanations tempting to indulge, but I argue that, by themselves, these alternative explanations are ultimately incomplete.

[78] Joint Publication 1-02, 71.

[79] The freedom to deviate from doctrine is not license to discard it, however. Deviation from a principle requires that one first understand when and where it applies, and more importantly when and where it might not.

[80] Dr. Matt Hunter, lead writer for the Army's first iteration of FM 3-12, helped me to arrive at this critical insight.

PATH DEPENDENCE

Path dependence describes a system in which past choices have a constraining effect on future possibilities.[81] In other words, the decisions that an organization has made in the past will inherently limit the scope of possible decisions available to that organization in the future, even though the past circumstances that surrounded those decisions may no longer be relevant.[82] Organizational decision-making patterns can become locked in due to the unintended consequences of past action and the positive feedback processes that led to them. Path dependent processes lead to inefficient outcomes when this lock-in binds an organization to a historical solution for which present circumstances no longer apply. The result is an organization that is unable to adapt to change requirements.[83]

Path dependence differs from a cultural explanation in two ways. First, path dependence does not specify the underlying mechanisms that lead to choice restriction.[84] In its broadest form, it simply argues that past decisions will necessarily impact future ones by shaping the process through which those future decision points emerge. It further argues that this process can become deterministic, such that organizations risk engaging in inefficient behavior when conditions change. Path dependence theory thus leaves room for a variety of cognitive, normative, or resource-based theoretical arguments to describe exactly *why* it is that an organization's path becomes restricted.[85]

Second, and following from the above, path dependence is not a predictive theory. In other words, given a set of initial conditions, a path dependent approach will not necessarily be able to predict the shape of the final outcome. Instead, it argues that organizational outcomes are a product of the process

---

[81] Olof Brunninge, "Imprinting and Organizational Path Dependence: Studying Similarities, Differences and Connections Between Two Concepts Along the Case of a Large Swedish Bank," (2011).

[82] Jorg Sydow, Georg Schreyogg, and Jochen Koch, "Organizational Path Dependence: Opening the Black Box," *Academy of Management Review*, Vol 34 No 4 (2009), 689-709.

[83] D.A. Leonard-Barton, *Wellsprings of Knowledge: Building and Sustaining the Sources of Innovation.* (Boston: Harvard Business School Press, 1995); Georg Schreyo¨gg and Martina Kliesch-Eberl, "How dynamic can capabilities be?" *Strategic Management Journal*, 28 (2007): 913– 933.

[84] Sydow, Schreyogg, and Koch, "Organizational Path Dependence."

[85] Ibid.

itself, which can only be understood historically and sequentially. This means that the nature of an organization's path will be initially unclear because it emerges as the product of unforeseeable processes that unfold over time.

By providing a predictive model that offers an explanation for the underlying mechanisms that lead to inefficient organizational behavior, my theoretical framework both contrasts with and complements path dependence theory. It complements the theory by offering a cultural explanation for the type of constrained organizational behavior and inefficient organizational outcomes that path dependence anticipates. It contrasts with the theory by providing a decidedly predictive approach to explaining organizational behavior. My argument is that, while circumstances can generate multiple possible paths within an organization's decision space, culture will have a deciding influence which of those paths result.[86] Understanding the landscape of initial cultural conditions can help us predict the shape of the final outcome and explain why that outcome prevailed over others.[87]

FUNCTIONALISM AND RATIONAL CHOICE

In a functionalist argument, an institution's behavior is the result of the function that institution is expected to perform. Outcomes will be determined based upon the rationalist principle of utility maximization: when given a new task, the organization will simply behave in a way that will lead to the best possible outcome. Organizational behavior under this framework can be explained as the rational response to a given mission set. Functionalist arguments tend to treat culture as one of two things: either culture is seen as a maladaptive ideology that causes deviation from a clear "rational judgment" of evidence, or culture is seen as inseparable from what the organization does. The weakness of the former lies in its presupposition that such a rational judgment always exists, while the weakness of the latter is that it effectively eliminates culture as a cause of organizational behavior.

---

[86] See Jenna Bednar and Scott E. Page, "Culture, Institutional Performance, and Path Dependence," *UC Berkeley: Institute of Governmental Studies.* (February 2, 2006).

[87] This point on the predictive nature of culture reflects a similar sentiment shared by Austin Long in his book *The Soul of Armies*.

However, what if there is more than one way to maximize utility? Or what if the path to utility maximization is not clear? What if, moreover, the behavior that would maximize utility under an initial set of conditions fails to maximize utility when those conditions change? Are organizations able to rationally change their behavior to achieve efficient outcomes under a new set of circumstances? If not, why? These are the inflection points at which I argue that culture emerges as a deciding variable. When presented with multiple possible outcomes, or with an ambiguous path to one outcome, organizational behavior will be influenced by organizational culture, such that the new method, concept, or task is adapted to fit within the prior competencies and predispositions of an organization's personnel. In this sense, the functionalist and cultural arguments both reinforce one another: what an organization does influences its culture, and its culture in turn is a reflection of what an organization does.[88]

However, when what an organization is asked to do changes, its culture will not necessarily change at the same pace. When applied to a scenario in which an organization must decide how to respond to new challenges, culture then becomes not simply an existing set of practices, but the belief that that those practices will be appropriate for future challenges.[89] Because that belief is resistant to change, it acts independently of the actual requirements on and capabilities of the organization. In other words, cultural influences can prevent an organization from effectively fulfilling the new function to which it has been committed by shaping the organization's interpretation of that function as fitting within the scope of its previous duties. While organizational culture has its origins in appropriate, functional behavior, it can cause inappropriate responses to novel challenges through the mechanism described above.

Conclusion

[88] Bednar and Page, "Culture, Institutional Performance, and Path Dependence."

[89] I am indebted to Steve Rosen for this observation.

This chapter proposed a theory of subcultural influence on the process of military innovation. It argued that, under conditions of high uncertainty about the nature of a new technology or circumstance, the predominant influence on the process of military innovation will be the ingrained predispositions and tendencies of those military subcultures which are given responsibility for it. As clarity about the nature of an innovation emerges over time, a process of learning will take place in which the role of subcultures will diminish, replaced by the broad vision of the military service writ large and the increasingly clear strategic incentives created by external threats. Competition among different ideas will be resolved in a way that aligns with the broader service mission and the dominant service culture.

In the next three chapters, I will test these theoretical propositions. In chapter 3, I assess the extent to which organizational subcultures affected the trajectory of cyberspace innovation in the U.S. Army. I argue that subcultural influence was high prior to the embrace of cyberspace by senior service leadership and its subsequent movement into the operational mainstream. At this point, cyberspace operations assumed a tactical focus as they shifted to support ground force maneuver. In chapter 4, I test the theory against cyberspace development in the Air Force. I find that subcultural influence manifested itself most heavily in the debate between cyberspace as intelligence or operations, with additional significant effects from the movement of cyberspace into the space and communications communities. Finally, chapter 5 examines the influence of subcultures on cyberspace development in the U.S. Navy. In contrast to the preceding two chapters, the Navy story is defined by the singular influence of the service's cryptologic community, culminating in the service decision to subsume cyberspace operations underneath a broad umbrella of information dominance.

CHAPTER 3 | **Cyberspace Development in the U.S. Army**

Based on the theoretical framework described in the preceding chapter, how might we expect to see cyberspace operations evolve within the U.S. Army? How might we expect the Army to resolve the challenges inherent to the introduction of a new, highly technical, non-kinetic warfighting capability that runs counter to many long-held tenets of its institutional culture? The story of cyberspace in the U.S. Army begins in the aftermath of the first Gulf War, when the creation of an organization dedicated to information warfare spurred experimentation in ways to attack adversary command and control systems. Concurrently, the evolution of enemy communications technology inspired the signals intelligence community to explore new methods of penetrating digital networks in order to gain access to sensitive intelligence. The increasing realization of the Army's own network vulnerability eventually led to the introduction of defensive techniques into the signal community's practice of network operation and maintenance.

However, because these early efforts to harness the warfighting potential of cyberspace were localized to a few peripheral units, they were neither widely known nor widely understood by the rest of the Army. Movements to expand these capabilities beyond their niche applications were thwarted by a low-tech institutional Army culture, which was not predisposed to embrace new technologies or the communities that primarily dealt in them. The lack of a clear strategic vision as to what cyberspace meant for the Army, combined with an institutional apathy that saw cyberspace as largely irrelevant to fighting and winning land wars, kept cyberspace from entering the mainstream of Army thinking for the first several years of its existence. Conversation during this period was thus dominated by competing subcultures whose parochial visions precluded the development of a more holistic, integrative approach. After nearly two decades of inconsistent development, cyberspace was normalized through the abandonment of these competing claims of purpose and the adoption of a new conceptual framework that was derived from and built upon traditional Army ways of thinking about war.

This new conceptual framework took the form of an expansion of cyberspace operations to the level of individual maneuver units. There, a dedicated subset of the Army's cyber personnel could devote their resources to the types of problems that were relevant to small units, such as the proliferation of aerial drones, the defensibility of tactical communication networks, or the impact of the adversary's use of cyberspace within the maneuver commander's assigned area of operations.[90] In a sense, this effort to embrace tactical cyber represented a resurrection of the forgotten concepts of both electronic warfare and information operations — the former having fallen into neglect at the end of the Cold War, and the latter having slipped into irrelevance based on internal doctrinal confusion and career field mismanagement. By increasing the relevance of cyberspace to the broader Army mission of fighting and winning land wars, the push for tactical cyber allowed the Army's cyber branch to enjoy a level of mainstream success that its closely related predecessors did not.[91] This normalization of cyberspace into the mainstream of Army operations and culture led to a series of institutional reforms that caused the Army to emerge as an unexpected cyber leader among the military services.

The Army

ORIGINS, HISTORY, AND CULTURE

Understanding the Army's culture starts with understanding the Army's purpose. As described in Army Doctrinal Publication (ADP) 1, *The Army*, the mission of the Army is to fight and win the nation's wars by engaging in sustained ground combat. Founded on 14 June 1775, the U.S. Army predates the Declaration of Independence and the Constitution, while still relying upon both documents as a source of

[90] Issie Lapowsky, "The Pentagon is Building a Dream Team of Tech-Savvy Soldiers," *Wired*, July 2, 2018; Association of the United States Army, "AUSA Cyber Hot Topic 2018, Panel 3: Cyber Support to Corps and Below," Filmed August 2, 2018, YouTube video, 1:15.23, Posted August 6, 2018, https://www.youtube.com/watch?v=ccjt7gCjnV0.

[91] By predecessors, I mean the information operations, psychological operations, and electronic warfare communities. While similar in both concept and function to cyberspace operations in that they are intended to attack adversary information systems and modify adversary behavior, these fields have never had the level of institutional attention that the Army's cyber branch currently enjoys.

its institutional ethic.[92] The Army also possesses a keen awareness of its history, framed in terms of the experiences of its soldiers, that bears on its self-perception in the present. The introduction of ADP 1 begins:

> Through our service, we continue the heritage of American Soldiers stretching back to the minutemen at Lexington and Concord. We stand with the continental line at Yorktown, charge with the Union regiments at Missionary Ridge, and go over the top at the Argonne Forest with the doughboys. We dig in with GIs to stop German armor in the Ardennes; board Huey helicopters with the grunts in Southeast Asia, and sweat in our body armor and kevlar helmets while patrolling the hills of Afghanistan. […] Today, as in 1775, we are the strength of our Nation and its force of decisive action.[93]

Army culture is further shaped by the character of warfare in the land domain, described in ADP 1 as "the most complex of all the domains, because it addresses humanity — its cultures, ethnicities, religions, and politics."[94] In describing the nature of the land domain, ADP 1 continues:

> The distinguishing characteristic of the land domain is the presence of humans in large numbers. Humans are interlopers in the air, on the sea, and in space; temporary occupants, maintained there through various technologies. Cyberspace is a technological repository and means of transit for information, but its content originates with people on land. Humans live on the land and affect almost every aspect of land operations. Soldiers operate among populations, not adjacent to them or above them. They accomplish missions face-to-face with people, in the midst of environmental, societal, religious, and political tumult. Winning battles and engagements is important but alone is usually insufficient to produce lasting change in the conditions that spawned conflict. Our effectiveness depends on our ability to manage populations and civilian authorities as much as it does on technical competence employing equipment. Managing populations before, during, and after all phases of the campaign normally determines its success or failure. Soldiers often cooperate, shape, influence, assist, and coerce according to the situation, varying their actions to make permanent the otherwise temporary gains achieved through combat.[95]

---

[92] Headquarters, Department of the Army, *Army Doctrine Reference Publication 1: The Army Profession* (Washington D.C.: Headquarters, Department of the Army, June 2015). See also R. Zimmerman, K. Jackson, N. Lander, C. Roberts, D. Madden, R. Orrie, "Movement and Maneuver: Culture and Competition for Influence Among the U.S. Military Services" (Santa Monica, CA: RAND Corporation, 2019), 22.

[93] Headquarters, Department of the Army, *Army Doctrine Publication 1: The Army* (Washington D.C.: Headquarters, Department of the Army, September 2012), vi.

[94] *Army Doctrine Reference Publication 1*, 1-1

[95] Ibid.

The land domain is considered the ultimate arbiter of the outcome of conflict.[96] While actions in air and at sea can affect strategic outcomes, "no major conflict has ever been won without boots on the ground."[97] Having established the importance of land combat, ADP 1 goes on to describe its nature:

> Land combat against an armed adversary is an intense, lethal human activity. Its conditions include complexity, chaos, fear, violence, fatigue, and uncertainty. The battlefield often teems with noncombatants and is crowded with infrastructure. […] Because the land environment is so complex, the potential for unintended consequences remains quite high. In the end, it is not the quality of weapons, but the quality of Soldiers employing them that determines mission success.[98]

This brutal nature of land warfare, and the deterministic character of the land domain to the outcome of international conflict, means that the Army is often the service that must commit the greatest number of personnel to any given military endeavor, and that must also suffer the greatest number of casualties.[99] Accordingly, two of the Army's three strategic roles have to do with the prevention of war rather than the conduct of it. The Army's roles are described in terms of prevent, shape, and win: prevent conflict through the creation and sustainment of a credible land force; shape the international environment through strategic military-to-military cooperation and partnerships; and win when called upon to engage in land warfare.[100]

---

[96] General Mark Milley, Army Chief of Staff, stated at his swearing in: "War is an act of politics, where one side tries to impose its political will on the other. And politics is all about people. And people live on the ground. We may wish it were otherwise, but it is not. Wars are ultimately decided on the ground, where people live, and it is on the ground where the U.S. Army, the U.S. Marine Corps, and the U.S. special operations forces must never, ever fail." Quoted in C. Todd Lopez, "Ground Forces 'Must Never, Ever Fail,' New Army Chief Says," DoD News, August 14, 2015, https://dod.defense.gov/News/Article/Article/613672/.

[97] *Army Doctrine Reference Publication 1*, 1-4. Consider also the oft-used quote by T.R. Fehrenbach: "You may fly over a land forever; you may bomb it, atomize it, pulverize it and wipe it clean of life — but if you desire to defend it, protect it, and keep it for civilization, you must do this on the ground, the way the Roman legions did, by putting your young men into the mud." From T.R. Fehrenbach, *This Kind of War: The Classic Korean War History*, 50th anniversary ed. (Dulles, VA: Potomac Books, 2001), 290.

[98] *Army Doctrine Reference Publication 1*, 1-2.

[99] Thomas G. Mahnken and James R. Fitzsimonds, "Tread-heads or Technophiles? Army Officer Attitudes Toward Transformation," *Parameters* (Summer 2004): 57-72.

[100] *Army Doctrine Reference Publication 1*, 1-5.

CULTURAL IMPLICATIONS

One can derive several conclusions about Army culture from the descriptions given above. First, the Army has a special relationship with war that is both visceral and intellectual.[101] While one could argue that the Air Force and Navy are singularly enamored with their individual domains, "the Army believes that it alone understands the true and full nature of war."[102] To the Army, war is something eternal, a fundamental, unchanging aspect of human nature whose essence lies in ground combat. Because of its perceived special relationship with war, the Army places significant value on the development of operating concepts to guide it in war.[103] This is evident in both the emergence of overarching strategic concepts such as the AirLand Battle theory of the post-Vietnam era as well as the extent to which the Army has embraced its own internal doctrine and doctrine development.[104]

Second, the Army is a service which values the human component above all.[105] The land domain is a domain of human engagement, and land combat requires extreme human resilience.[106] Accordingly, the Army's historical identity is described not in terms of its victories, but of its shared hardships, from the perspectives of the soldiers who endured them. Training and maintaining the service is described as a process of strengthening the individual soldier rather than building the things he uses. As it has been said, "the Army equips the man" rather than mans the equipment.[107] It thus follows that the Army places a greater emphasis on its people than on its machines, a sentiment that is also echoed in Carl Builder's analysis. "Toys" for the Army, as Builder calls them, as well as technology in general, exist to augment the

---

[101] Zimmerman, et al, *Movement and Manuever*, 36

[102] Ibid., 22

[103] Zimmerman, et al, *Movement and Manuever*, 36

[104] It is not fair to attribute the Army's embrace of doctrine to purely the nature of the land domain, since not all Armies around the globe (Israel being one noteworthy example) exhibit similar doctrinally-minded tendencies.

[105] Zimmerman, et al, *Movement and Manuever*, 25: "While each of the services values its people, in the Army, the 'grunt' or 'Joe' is elevated in the imagination."

[106] Ibid., 26: "But for the Army, the timeless pursuit of battlefield victory is an inherently human endeavor — every battle is won or lost by the accumulated successes or failures of the individuals on the battlefield."

[107] Ibid., 49; this sentiment was echoed in an author interview with former Secretary of the Air Force Michael Wynne.

power of the individual soldier rather than to replace it.[108] The primacy of the individual soldier, and the reality of ground combat as an intimate human endeavor, has left the Army with a healthy institutional skepticism toward the promises of new technology.[109] The Army is alone among the three major services in this perception.

While strategic considerations affect how the Army prevents conflict and shapes the international system, it cannot achieve its core purpose of winning at land combat without sound tactical decision-making on the ground. This emphasis on individual decision-making at various echelons of command is seen as the antidote to the sprawling chaos of ground warfare. It is doctrinally encapsulated in the Army's concept of mission command, or an intent-based method of leadership designed to encourage the exercise of disciplined initiative in subordinates.[110] Importantly, mission command acknowledges that subordinates may err in taking aggressive action, but ultimately accepts that the pursuit of such action within the scope of a commander's operational intent is preferable to trepidation.

Furthermore, land warfare takes place in a bounded domain that is defined by clearly delineated pieces of terrain.[111] Whereas warfare in the air domain is naturally unbounded both temporally and terrestrially, and warfare at sea cannot end with decisive territorial ownership, warfare in the land domain is driven by the imperative to seize and hold key terrain until one has incrementally subdued the desired amount of territory and the enemy who inhabits it. One need not destroy the enemy provided one exercises this territorial control — a game of decidedly tactical decisions that must be played by those who

---

[108] Builder, *The Masks of War*, 22.

[109] Mahnken, Fitzsimonds, "Tread-heads and Technophiles."

[110] For more on mission command, see Army Doctrine Publication 6-0: *Mission Command* (Washington, D.C.: Headquarters, Department of the Army, 2012). As a methodology, mission command traces its roots back to Prussia. An 1837 update to the Prussian field service regulation states: "If an execution of an order was rendered impossible, an officer should seek to act in line with the intention behind it." Mistakes were "preferable to hesitancy to enable decisive bold action." Taken from James D. Sharpe Jr. and Thomas E. Creviston, "Understanding Mission Command," Army.mil, July 10, 2013, https://www.army.mil/article/106872/Understanding_mission_command/.

[111] Military theorist J.C. Wylie describes the effect of terrain well in his book *Military Strategy*: Terrain "is the fixed field within which [the soldier] operates. It is the limitation within which he must function. It is the opponent that he must always face no matter who may be his enemy. It is the fact of terrain that establishes the field within which the soldier's professional intellect must generate his plans. Where the sailor and the airman are almost forced, by the nature of the sea and the air, to think in terms of a total world or, at the least, to look outside the physical limits of their immediate concerns, the soldier is almost literally hemmed in by his terrain." From J.C. Wylie, *Military Strategy: A General Theory of Power Control* (Naval Institute Press, 1989), 42.

are closest to the action.[112] Thus, the dominant service function is the infantry, and the dominant decision-making level is the small unit.[113]

The complexity of the land domain creates necessary intra-service distinctions in which subcultures are defined by their relationship to the forward infantry. The infantry require a number of supporting functions in order to close with and destroy the enemy, from communications to intelligence, supporting artillery to logistics. Soldiers readily identify with their specific subculture, based less upon a perception of institutional superiority than to a pride in the role that they play in an interdependent fight.[114] This pride in the role that one plays is reflected in many branch mottos — Army Aviation, for example, is "above the best," while the Military Police strives to "assist, protect, defend." Each of these functions acknowledges the critical supporting role it plays in the fight to gain territory, destroy the enemy, and pacify populations. Thus, the infantry is the dominant subculture of the Army, for it is the only subculture that can decisively conclude combat on land. The infantry's motto of "follow me" emphasizes both this forward presence at the tip of the figurative spear as well as the aforementioned imperative of individual leadership and initiative.

Tension between the infantry and other supporting subcultures, or among the supporting subcultures themselves, arises not out of a competition for institutional prestige, but out of each subculture's perceived contribution to the forward fight. It follows that the greatest subcultural distinction in the Army is the distinction between combat arms — those who do the fighting — and combat

---

[112] The Army places nearly all of its personnel emphasis on the experience of command, and as a result tends to view staff tours away from operational units with suspicion. The resultant institutional and cultural focus on tactics over strategy was pointed out in Builder's study, which sprung from an initial research inquiry as to why the Army was so bad at long-term strategy, and has been reaffirmed by numerous studies and thinkers since. This tactical focus can tend to lead to a culture of "presentism," in which the Army struggles to see beyond the immediate tactical situation or operational problem (Zimmerman et al, *Movement and Maneuver*, 43). See, for example, MG (R) Robert Scales' article, "Are You a Strategic Genius? Not Likely, Given the Army's System for Selecting, Educating Leaders," *Association of the United States Army*, October 13, 2016.

[113] The traditional three combat arms have been infantry, armor, and artillery, with further distinctions between mechanized and light infantry. However, in terms of earning the cultural heart of the service, the infantry is the undisputed leader of the three. See Zimmerman, et al, *Movement and Maneuver*.

[114] Robert Zirkle of the Institute for Defense Analysis argues that the Army is best seen as an oligarchy. This description stands in contrast to an organization like the Air Force, which has the "monarchial" dominance of a single community. From Robert Allen Zirkle, "Communities Rule: Intra-Service Politics in the United States Army" (PhD diss., Massachusetts Institute of Technology, 2008), 63-67.

support.[115] The nature of the work performed by these different functions demands different attributes in their personnel and leadership. Leadership in combat arms is about motivating soldiers to do difficult things under adverse conditions. This requires an immense physical toughness and an unwavering mental resolve. It also requires a fundamental willingness to do the hard things oneself in order to inspire the execution of the same in others — the "follow me" mentality of the infantry or the iconic, officer-led bayonet charge of Hal Moore at Ia Drang.

Combat arms leaders are thus seen as leaders of soldiers first, and managers of capabilities second.[116] As managers of capabilities, they must have intimate knowledge of the weapon systems under their charge in order to employ them to maximal effect on the battlefield. As leaders of soldiers, they must have intimate knowledge of the soldiers behind the weapon systems to inspire them to perform the challenging tasks of which they are asked. As one study on service culture writes,

> In most of the other services, officers atop their service hierarchies are technicians of a sort: Air Force officers fly planes, Navy officers guide ships. For Army officers, their technical specialty is leadership. An Armor officer does not drive the tank; he leads his men, who drive the tank.[117]

Organizational culture in combat arms units tend to be more hierarchical than those of non-combat units in order to foster a type of instinctive obedience in the junior soldiers whose sole mission purpose is to do what they are told. While combat arms leaders remain generalists in the sense that they will never be experts on any particular weapon system, they are expected to be tactical specialists, and as such are seen as the repository of expert knowledge on the employment of troops within their given formation. In this

---

[115] Zimmerman, et al., *Movement and Maneuver,* 23-24.

[116] Ibid., 26: "The Joes are at the heart of the Army, and the true measure of an officer is in his or her ability to lead the troops."

[117] Ibid., 36.

world, combat credentials are valued; valor and grit are praised; patience and intellect are often seen as secondary.[118]

Contrast this with the Army's combat support functions — the logisticians, personnel officers, communicators, intelligence professionals, and others, who provide the massive support structure necessary to enable the forward troops to close with and destroy the enemy. The importance of these support structures is not lost on the institutional Army,[119] but the nature of their work is such that they nevertheless remain at the cultural periphery of the Army's warfighting soul. Combat support leaders manage assets in order to provide a service. They are leaders in the sense that all officers are leaders, but their work is fundamentally managerial in nature. Because combat support functions tend to take place at a distance from hard fighting, the cult of the mythical super human combat leader that so often animates combat units is far less important to the support culture. Rare is the occasion when a combat support leader must motivate his or her soldiers to advance into a hail of enemy fire.[120] Thus, the managerial function of leadership becomes far more important to combat support branches than the aspect of motivating soldiers to do difficult things under adverse conditions.

Furthermore, combat support branches tend to be immensely diverse and immensely dispersed, with a large variety of different formation types oriented around specific capabilities. Officers tend to learn about these capabilities after they arrive to their units, not before, and as such they are not expected or intended to be technical experts.[121] Support officers are thus groomed less for the depth of their

---

[118] This is not to say that patience and intellect are not valued attributes of a combat leader. Along with "character" and "presence," intellect is one of the attributes assessed on an Army officers annual evaluation form. However, culturally, these two traits tend to hold less of an influence than things like physical fitness, toughness, and an intangible fighting spirit. See "You Can Lead, But Can You Fight? Leadership as a Conduit to the Real Mission," The Company Leader, February 21, 2019, http://companyleader.themilitaryleader.com/2019/02/21/you-can-lead-but-can-you-fight/?fbclid=IwAR2RJykTMmOZ7CYo1pqjW5XZXs4YUYgti6vAYte9q7IWO-YF9PDbaRjtr2s.

[119] Nor have they been throughout history. Alexander the Great once famously said: "My logisticians are a humorless lot…they know if my campaign fails, they are the first ones I will slay." Quote taken from Joe Lynch, "The Logistics of Logistics," October 12, 2014, https://www.thelogisticsoflogistics.com/my-logisticians-are-a-humorless-lot/.

[120] I recognize that the past 17 plus years of counterinsurgency have complicated this distinction, and have led to many non-combat functions having to endure combat experiences. However, the Army's efforts to instill a "warrior first" mindset in its support branches throughout these wars did little to fundamentally change the fact that support branches do not generally attract the type of warriors who volunteer to do the bulk of the Army's killing in the combat arms branches.

[121] Specializations like explosive ordinance disposal (EOD), lawyers, and doctors are the exceptions to the rule.

expertise than for the breadth of their managerial experience. They are generalists in the true sense, able to apply their broad knowledge of diverse operating systems to the administrative and logistical problems that they are hired to overcome. The administrative and logistical skill sets of support officers are far more valuable than tactical prowess.

ARMY SUBCULTURES

The Army is comprised of a number of functional subcultures, each with its own purpose, mission, and culture. As described above, the broadest distinction is between the combat arms and combat support communities. This distinction is less salient in the Army than it is in the other services in that it does not erode the fundamental acknowledgement of interdependency that lies at the heart of Army branch rivalries, nor has it resulted in the type of fights for prestige that have characterized similar tribal rivalries in the Air Force and Navy.[122] Nevertheless, characteristics of this combat and combat support distinction have implications for everything from individual unit culture — with combat arms tending to be more hierarchical in order to foster stronger norms of instinctive obedience — to personnel practices and resourcing priorities.[123] Both combat arms and combat support officers are trained to be generalists and managers of capabilities. However, combat arms officers are also expected to be tactical experts grounded in the art of employing their assigned combat capability. As such, they tend to possess a level of specific tactical expertise that is naturally difficult to cultivate in the support branches.

In addition to this combat and non-combat distinction, there are five primary subcommunities which have interacted over time to influence the trajectory of Army cyberspace operations: military intelligence, electronic warfare, signal (communications), information operations, and space.

---

[122] Builder, *Masks of War*, 27: " To a degree significantly beyond that exhibited by the Navy and Air Force, the Army branches acknowledge their interdependency and pay tribute to their siblings. […] The Army branches of infantry, artillery, and armor see themselves as inextricably dependent upon their brother branches if they are to wage war effectively." This point is also affirmed in Zimmerman, et al., *Movement and Maneuver*.

[123] Zimmerman, et al., *Movement and Maneuver*, 26.

Military Intelligence

Army military intelligence (MI) exists to make sense of the battlefield, understand the enemy, and enable commander decisions. It is the sole sub community in the Army that is dedicated to thinking like the enemy. Military intelligence collects, processes, analyzes, and disseminates intelligence to the broader force at echelons tactical to strategic. The most salient distinction within this subculture is that between individual collection disciplines.[124] The second most salient distinction is that between the tactical and strategic components of these disciplines.[125] The culture embraces technology more so than other portions of the Army, but only insofar as it supports the judgment of the individual analyst.

The intelligence culture can be described as analytical, one that praises intellectual acumen over physical strength or combat experience. There is an ingrained instinct to protect assets and capabilities while simultaneously pushing the boundaries of what is able to be collected. The necessity of relying upon the individual intellect, as well as the generally high cognitive capacity of its personnel, contributes to a flatter and more collegial managerial style than that found within the broader force, even while operational decisions remain hierarchical in order to mitigate risk. It is an environment dominated by analytical assessments rather than by decisions, by thought and the presentation of information rather than by action. Officers within the intelligence community are trained to be generalists whose fundamental purpose is to advise the commander on the current state of the enemy. Officers have limited ability to specialize in particular collection disciplines; true intelligence expertise more often resides with warrant officers and non-commissioned officers as a result.

Within the intelligence community, the field of signals intelligence played an instrumental role in the development of cyberspace operations, and thus deserves its own separate analysis. The purpose of signals intelligence is to intercept and analyze enemy communications signals. The execution of these

---

[124] Human intelligence, signals intelligence, imagery intelligence, all-source intelligence, counter-intelligence, etc.

[125] Tactical military intelligence works at the level of the Army maneuver unit, or division and below. Strategic military intelligence works at the strategic echelon, often away from the battlefield and not in direct support of conventional troops. The strategic intel community tends to have more of an inter-agency "IC" (intelligence community) flavor, while the tactical intelligence community much more readily identifies with the culture of the maneuver units they support.

duties requires a combination of sophisticated technological equipment and rigorous analytical methods. Signals intelligence places a premium on the individual cognitive capacity of its soldiers, which means that these soldiers tend to be independent-minded and of high intellectual caliber. In addition, the evolving technological demands of intercepting signals in the digital area require most soldiers to have a high technological aptitude, as well as a comfort with the high stakes of operating in enemy technological space.

Expertise resides within the enlisted corps: the enlisted are trusted to make consequential analytical decisions while the officers are trained to be generalists. While the Army has an additional skill designation to help identify officers with proficiency in signals intelligence, it does not have a dedicated career field or separate career path for its officers who possess this proficiency. Regarding risk, the community can be said to have a high tolerance of risk in all areas save the exposure of collection assets and capabilities. In other words, soldiers are willing to push the boundaries of what can be collected, but will stop short of action which could reveal their precise collection methods or risk sacrificing collection capability. In order to avoid disclosing sources and methods, the field shrouds its operations in layers of additional classification designed to keep all but the final analytic product out of the hands of the unqualified.[126] The Army signals intelligence community is therefore moderately tolerant of risk, delegates analytic decisions to low levels, has a relatively flat organizational culture led by generalist officers, and places a high emphasis on technical aptitude among its enlisted population.

These cultural attributes can lead us to a few predictions regarding the intelligence community's approach to cyberspace. We can expect the community to approach cyberspace as a platform for strategic intelligence collection, akin to those which already exist within the signals intelligence community. We can expect a risk-averse mindset and an embrace of operational secrecy, with decisions made in procedural fashion by upper levels of leadership. Actions will be offensive in nature, for the purpose of intruding

[126] These layers of secrecy also serve to protect the 4th Amendment rights of U.S. citizens: the potential for raw signals intelligence traffic to incidentally or accidentally include U.S. person information is such that only those who receive specific training are allowed to see the unfinished product. Signals intelligence personnel must exercise their due diligence in ensuring that U.S. person information is sanitized or removed before disseminating an intelligence report to the broader community.

inside networks, while retaining espionage and intelligence collection — rather than disruption or attack — as their final purpose. The enemy-centric focus of intelligence as a discipline will ensure that technical wizardry does not eclipse an appreciation for the need to gain a holistic understanding of the enemy. We can therefore expect, in total, a strategically-oriented, moderately risk-averse, yet offensively-minded approach with an appreciation for the end user and a high need for secrecy.

Electronic Warfare

Comprising the reverse function of signals intelligence is the field of electronic warfare (EW): rather than collecting enemy signals, electronic warfare seeks to interrupt them. Electronic warfare is defined as any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy.[127] Electronic warfare comprises both offensive and defensive elements, described as electronic attack and electronic protect, with offensive elements tending to be in greater operational demand among supported units. The preeminence of offense over defense in this community was the result of two influences: the attack mindset of the primary electronic warfare customer — ground combat units — and the attack mindset of the artillery community into which electronic warfare was eventually embedded.[128] It is tactically focused, systems-based, and procedural in management style. Electronic warfare personnel are expected to be experts on the function and employment of their given systems; they are not expected to be technical experts on the physics of the electromagnetic spectrum itself.

Army electronic warfare capabilities were contained in intelligence units during the Cold War, fell into atrophy and disuse in the post-war period of the 1990s, and were not resurrected as either a set of capabilities or a separate career management field until the radio-controlled improvised explosive device

---

[127] Department of Defense, *Joint Publication 3-13.1: Electronic Warfare* (Washington, D.C.: Department of Defense, 2007), GL 10.

[128] As we shall see, the Army treated EW as a subset of military intelligence for a number of years before the practice died out at the end of the Cold War. It was resurrected as a subset of fires in response to the remote-controlled IED threat in Iraq in the mid-2000s. From a functional standpoint, Army artillery is referred to as "fires."

threat emerged in Iraq in the mid-2000s. This inconsistent history affected the amount of institutional influence that electronic warfare was able to leverage during the growth of cyberspace operations. Based on its culture and history, one can expect an electronic warfare approach to cyber that is tactically-focused, offensively-minded, risk-acceptant, and oriented fundamentally at technological systems rather than human psychology.

Signal Corps

The third subcommunity of interest is the Army signal corps, which manages communications systems for the broader force. Signaleers are the Army's communicators. They are responsible for building, maintaining, defending, and restoring networks of all kinds at levels tactical to strategic. The culture embraces technology as what enables communication, and thus, as the foundation for their existence as a field. However, this embrace of technology tends to be static rather than innovative. The source of individual and collective signal competence lies in a type of technical expertise that is centered around maintenance and trouble-shooting. Above all, signaleers are driven by the imperative to keep the networks working, leading to a customer service mindset in which all is good if nothing is wrong. Understanding specific types of threats to a network is considered irrelevant to the fact of whether or not the network is functioning properly. Thus, signal personnel have a threat-agnostic approach to network management that is less concerned with enemy efforts to disrupt network function than it is with the inner workings of the network itself.

The complexity of network management, as well as the risks of network compromise, creates a culture that is risk averse, hierarchical, and procedural, and in which initiative is generally discouraged. Officers serve as managers and gatekeepers, while the enlisted serve as network technicians trained to ensure continuous network service. One can thus expect that the signal corps' approach to cyberspace will be risk averse, technical, procedural, and overwhelmingly defensively oriented at both the tactical and the strategic levels. Moreover, given that signal officers think in terms of service provision rather than

operations, we can expect the signal community to struggle with the operational orientation of cyberspace.

Information Operations

The field of information operations is more difficult to categorize, given its emergence from a concept of information warfare that eluded a firm definition for years. Information operations as a concept emerged in the wake of the first Gulf War, and centered around the notion of attacking enemy communication systems as a way to inhibit the enemy's exercise of battlefield command and control.[129] Over time, it evolved into a staff managerial function directed towards the management of diverse information-related capabilities. Information operations as a career field did not arise until 1999, several years after the creation of the Army's first IO organization. Today, information operations is not a traditional branch within the Army; instead, it is a functional area, open to officers through an application process that is made available only after a minimum period of time in service. Information operations officers all have several years of traditional Army experience as a result.

Outside of select command positions within the Army's 1st IO Command, IO officers typically do not lead units or soldiers. Instead, they are trained to be staff officers who integrate information operations capabilities into the supported commander's campaign plan. Importantly, IO officers rarely have specialized expertise in any of the capabilities they steward — in other words, they are not experts on electronic warfare or psychological operations, but instead act to synchronize these and other functions to provide informational support to the maneuver operation. IO officers work on maneuver staffs from brigade to corps level and higher. Outside of 1st IO Command, the Army does not have any IO-specific units.

The fundamentally integrating purpose of information operations, combined with the fact that it does not actually own any of the capabilities it champions, has led to a weakened community culture that

[129] As I describe in a later section, this concept was originally called command and control warfare rather than information operations.

has struggled to wield significant institutional influence. This struggle is exacerbated by IO's status as a functional area and the attendant structural disadvantages that such an arrangement provides.[130] As a functional area, the IO community has few command billets, few promotion opportunities past the rank of colonel, and thus few potential community champions who have commensurate rank and stature to advocate for IO needs at the general officer level. During the later years of the global war on terror, these structural deficiencies combined with a doctrinal confusion over how the IO mission could be best fulfilled to produce an Army community that struggled to achieve any significant institutional influence throughout the most pressing period of cyberspace growth. One can therefore expect the information operations approach to cyberspace to follow an inconsistent trajectory in which cyber capabilities are initially championed as a potential tool to affect decision-making, and then forgotten in tandem with the IO community itself.

Space

The Army's small space community is comprised of around 300 functional area officers organized into a single Army space brigade. Individual liaisons deploy from this brigade to provide space support to division and higher commands. Unlike the Air Force, the Army space community is not in the business of building or launching satellites. Rather, Army space officers are responsible for leveraging space-based capabilities to support the needs of ground forces. As the single largest beneficiary of space-based capabilities, the Army's reliance on space for communication and navigation has lent the community a

[130] An Army functional area is a grouping of officers by technical specialty or skill which usually requires significant education, training, or experience. Officers may apply to transfer into functional areas around their fifth year of service. If accepted, they are removed from the traditional Army career trajectory in order to become specialists in a particular field, where they are managed for the remainder of their careers. Functional area officers continue to wear the colors and insignia of their original base branch even while they fulfill the exclusive duties of their new career field. In addition to space and information operations, examples of Army functional areas include: Foreign Area Officer, Nuclear Medical Scientist, Environmental Scientist and Engineering, Explosive Ordinance Disposal, Public Affairs, Systems Automation Management Officer, Army Strategist, Strategic Intelligence, and Operations Research.

unique type of operational importance that is not diminished by its relative size or anonymity.[131] However, this operational importance does not correspond with institutional renown, as the average conventional Army soldier is unlikely to know that his service has a space brigade. Nevertheless, as a functional area, space officers' origin in the conventional Army has allowed the community to remain in tune with conventional Army needs. The fact that these personnel must have several years of traditional operational experience before joining the space community means that Army space officers come from the regular Army, understand how the regular Army works, and are conditioned to think in terms of service to the end user on the ground. In addition, space officers tend to be technically proficient and comfortable around technologically advanced systems and concepts.

Contrast this with the Air Force, where officers commission into the space branch as lieutenants and spend their entire careers in this community. The Air Force space community is also much larger, and as one of the Air Force's three major operating domains, it competes with air and cyberspace for budget, resources, manpower, and the cultural claim to the heart and soul of the Air Force.[132] Air Force space also serves a different purpose than Army space. Whereas the Army is concerned with coordinating for and using space assets to provide services to the troops on the ground, the Air Force has to design, acquire, develop, and then launch the satellites that enable those services. The Air Force's responsibility for satellite launch, acquisition, and development means that they operate on a fundamentally different time horizon and use a fundamentally different plane of risk than the Army community with the same name. The Air Force space community works with big things and long timelines, and as a result tends to be more risk averse and less agile in its thinking. These necessary attributes did not help the development of Air Force

[131] By this I mean that the average officer in the operational Army is unlikely to know that the Army even has a space brigade. Institutional importance taken from author interview with Jeff Harley. Largest user of space-based assets from "The Army Space Cadre: Space Professionals (FA40) and Space Enablers," Army.mil, September 27, 2010, https://www.army.mil/article/45767/the_army_space_cadre_space_professionals_fa40_and_space_enablers.

[132] Jeffrey S. Harley, telephonic interview with the author, October 26, 2018.

cyberspace operations when they were placed under Air Force Space Command in 2009, as we shall see in the next chapter.[133]

However, while the Army space community is more tactically-focused than its Air Force corollary, it still abides by the slower operational timeline and lower acceptance of operational risk than is characteristic of the joint space community. Furthermore, the sensitive nature of space-based capabilities results in a culture that is accustomed to operating behind multiple layers of classification and compartmentalization. One can thus expect the community's approach to cyberspace to be similar to the community's approach to space: focused on leveraging existing capability to provide uninterrupted service to the ground user, for whatever purpose is in greatest need, yet shrouded beneath a veil of compartmentalization that increases the difficulty of cooperation across disciplines.

Computer Technologists

In addition to the five formal subcultures defined above, a sixth, informal subculture of computer technologists — the hackers, software developers, and computer scientists who comprise the intellectual core of the cyberspace operations field today — wielded significant influence on the development of the Army's cyber branch. Prior to the creation of a defined career field, the epicenter of this culture in the Army was best represented by faculty within the Electrical Engineering and Computer Science Department (EECS) at West Point. This culture values intellectual creativity, flat organizational constructs, and individual autonomy to a far greater degree than any other subset of the institutional Army, which is one of the reasons why the Army has struggled to understand how to approach it. Many of these personnel subscribe to the "hacker" mindset, which in the broadest sense describes one who is passionate about technology and enjoys creatively overcoming or circumventing limitations in pursuit of a solution to a problem.[134] Manipulation and deception of both computer systems and the humans who operate them

[133] Harley, interview.

[134] Gregory Conti and Jen Easterly, "Recruiting, Development, and Retention of Cyber Warriors Despite an Inhospitable Culture," Small Wars Journal, 2010.

are embraced as legitimate methods to achieve the ultimate aim of outsmarting one's opponent. Given these characteristics, any doctrinal influence from within the smaller subgroup of computer programmers is likely to encourage autonomy at lower echelons, risk-acceptant offensive operations, an embrace of technical expertise, and an emphasis on both technical and psychological elements.

CULTURAL SUMMARY

What does the above study tell us about Army culture, and what might that culture tell us about the Army's subsequent approach to cyberspace? The Army is a people-centric organization whose primary purpose is to fight and win land wars. This terrestrial focus lends itself to a tactically-oriented mindset, in which the micro details of terrain demand an intrinsic deference to the decision-making capabilities of small-unit leaders who are best positioned to understand what is needed in the midst of the chaos of ground combat. The Army's valuation of combat arms, combined with the fundamentally human nature of land warfare, creates an institutional skepticism toward any technology or technological development that is not oriented toward supporting the individual soldier at the lowest level of tactical maneuver.

Given these cultural proclivities, we can expect the Army to struggle early in its integration of cyberspace concepts and capabilities due to the technological expertise required to succeed in the domain and the difficulties of qualitatively measuring success. Eventually, cyberspace will have to be assimilated into the Army's dominant maneuver culture in order to enjoy widespread institutional acceptance. Conceptually, this assimilation will occur through the development of doctrine. Practically, it will occur through the development of capabilities which are increasingly relevant at the tactical level. Cyberspace personnel management practices will also have to be carefully tailored in order to balance the technical demands of the medium with the cultural demands of the institution, such that cyberspace personnel are equally capable of communicating with Army maneuver audiences as they are with the technologists of

broader hacker culture. Careful analysis of the Army's history in cyberspace will demonstrate how this development actually took place.

The Influence of Information Operations

DOCTRINE

The U.S. Army's intellectual engagement in cyberspace began with the concept of command and control warfare (C2W) in the early 1990s.[135] Command and control warfare officially entered into the joint lexicon in 1993 as a replacement for the previous term of command, control, and communication countermeasures (C3M), which had emerged from revolution-in-military-affairs theorizing of the 1970s and 1980s as a result of the proliferation of new information systems on the battlefield.[136] C2W was described as "the military strategy that implements information warfare on the battlefield and integrates physical destruction" to "decapitate the enemy's command structure from its body of combat forces."[137] In other words, C2W was about attacking the adversary's ability to make timely decisions by attacking the systems he uses to communicate.[138] The Gulf War of 1991 was the first decisive demonstration of this central idea that attacking adversary command and control systems would be the key to success in future combat.[139]

---

[135] The deep strike premise of C2W — the intention to strike at high-value targets in reserve, reinforcing, and second-echelon forces, to include critical C2 nodes — was first codified in the emphasis on depth and synchronization that was a critical tenet of AirLand Battle doctrine in 1986. See *Field Manual 100-6: Information Operations* (Washington D.C.: Headquarters, Department of the Army, 1996), ch 3.

[136] Chairman of the Joint Chiefs of Staff Memorandum of Policy 30, "Command and Control Warfare" (Issued July 17, 1990, 1st Revision March 8, 1993); as a product of revolution-in-military-affairs theorizing, see Zimmerman, et al., *Movement and Maneuver*, 195

[137] Chairman of the Joint Chiefs of Staff Memorandum of Policy 30, "Command and Control Warfare," Issued July 17, 1990, 1st Revision March 8, 1993. Department of Defense Directive TS-3600.1, "Information Warfare," December 21, 1992, describes the original DoD guidance on information warfare.

[138] A critical distinction between the original conception of command and control warfare and how we pursue cyberspace operations today is that C2W was wholly focused on enemy command and control systems, and was thus wholly focused on preventing the opposing commander from effectively controlling his forces. Modern cyberspace operations are less explicitly focused on affecting enemy command and control.

[139] *Field Manual 100-6*, ch 3. See also Edward Mann, "Desert Storm: The First Information War," *Air Power*, Vol 8 No 4 (1994): 4-14.

While the Gulf War largely proved the effectiveness of the command and control warfare concept in theory, it revealed several challenges to how this theory was implemented in practice. The Army in particular noted a number of incidents of information fratricide due to the lack of proper deconfliction mechanisms between competing methods of information dissemination — OPSEC efforts conflicting with military deception campaigns, for example, or public affairs messages unintentionally countering those put forth by psychological operations.[140] As a result, a number of active and retired Army officers convened to develop ideas on how the Army could better synchronize, coordinate, and integrate its various information efforts in future conflict.[141] This theorizing provided the intellectual foundation for the Army's first information operations Field Manual published in August 1996, FM 100-6, *Information Operations*.[142]

Shortly before the publication of FM 100-6, the Department of Defense released JP 3-13.1, *Joint Doctrine for Command and Control Warfare.*[143] The publication concentrated on command and control warfare rather than information warfare based on the assertion that "the full dimensions of IW policy and its implementation are still emerging."[144] The ambiguity of JP 3-13.1 reinforced the notion that the DoD had yet to develop a coherent vision for what information warfare was or how it should be practically implemented. JP 3-13.1 described IW "as a whole-of-government affair that could support national interests but had to work in cooperation with a broad range of stakeholders."[145] Notably, JP 3-13.1 contained no mention of the concept of information operations, a concept which would play a significant role in the Army's own doctrinal development, and which would eventually come to replace the more militarized-sounding "information warfare."[146]

---

[140] Michael Muztafago, telephonic interview with the author, October 30, 2018.

[141] The origins of both the Land Information Warfare Activity and later 1st Information Operations Command were tied to lessons learned from the 1991 Gulf War in regards to the need to provide information warfare support to Army commands ("1st IO Command (Land) History — Information Paper," May 7, 2014).

[142] Muztafago, interview.

[143] Field Manual 100-6 was released in August 1996 and Joint Publication 3-13.1 in February 1996.

[144] Warner, "Notes on Doctrine."

[145] Ibid.

[146] Warner, "Notes on Doctrine."

In spite of the lack of doctrinal clarity at the joint level, the Army pressed ahead with its own theories of conflict in the information space. FM 100-6 was the first doctrinal publication on information operations among the military services, preceding both Air Force and Joint doctrine on the same topic by two years.[147] FM 100-6 also heavily influenced the development of JP 3-13, *Information Operations,* released in 1998.[148] FM 100-6 articulated the distinction between the overlapping concepts of information warfare, information operations, and command and control warfare. Information warfare was defined according to the joint definition as "actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own."[149] Fundamentally, it was about protecting and attacking the mechanisms that enabled commanders to make sound battlefield decisions.

However, because the joint definition for information warfare was narrowly focused on the impact of information during a state of conflict, the Army adopted the specific term information operations to recognize the role of information issues across the entire spectrum of military operations from peace through global war.[150] This represented a broader perspective on the role of information to conflict than that taken by the DoD.[151] Concurrently, the Army defined command and control warfare as the specific application of information warfare in military operations: "the integrated use of operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW), and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy

---

[147] Both Joint Publication 3-13, Information Operations, and Air Force Doctrine Document 2-5, Information Operations, were published in 1998.

[148] Muztafago, interview

[149] Chairman of the Joint Chiefs of Staff Instruction 3210.03, "Joint Command and Control Warfare Policy," March 31, 1996.

[150] FM 100-6; this point was reiterated by John Mahoney, telephonic interview with the author, October 12, 2018.

[151] John Mahoney and FM 100-6; note also that the Air Force attempted to make a similar distinction in its 1998 publication AFDD 2-5 by introducing the dual concepts of information warfare and information-in-war. While this did not differentiate between information-related activities inside war and those outside war, it did attempt to distinguish adversary-focused information activities from those intended mainly to provide friendly situational awareness. This micro-evolution in the service's understanding of information was part of a broader effort to add specificity to the larger question of the general relevance of information to conflict.

adversary C2 capabilities, while protecting friendly C2 capabilities" against similar efforts.[152] The manual noted that C2W contained both offensive and defensive functions. FM 100-6 also contained the first use of the words "computer" and "computer network" in an Army doctrinal publication, and discussed the threat that malicious software posed to Army information systems.

It is important to note that neither C2W, nor information warfare, nor information operations were considered by the Army to be capabilities in and of themselves. One could not request C2W in the same way one could request close air support. Rather, they were terms used to describe the integration of multiple individual capabilities in order to achieve the unified purpose of attacking enemy decision-making. C2W, and later IO, contained five core elements, each of which offered a way to affect one component of the adversary decision-making process. C2W involved the holistic use of all five together for maximal effect. It was this integrating function that allowed the idea to work, rather than the singular execution of any individual capability it contained.[153]

ORGANIZATIONS

Land Information Warfare Activity

The Army's organizational effort to address command and control warfare began nearly a decade before the doctrine for it solidified. In the mid-1980s, the Army staff created a small planning element called the Studies and Analysis Activity (SAA) in order to determine how the Army should fight doctrinally and technologically under the C2W construct.[154] The specific nature of the SAA remains classified. However, it is generally known that the organization sought to find ways inside adversary command and control systems, and that it worked with other intelligence agencies to do so.[155] The SAA

---

[152] Chairman of the Joint Chiefs of Staff Instruction 3210.03, March 1996.

[153] Austin Branch pointed out this critical distinction in a telephonic interview with the author, November 9, 2018.

[154] Details of this activity remain classified. Estimates place its activation around 1984. William J. Thompkins, interview with the author, September 27, 2018.

[155] Harley, interview.

was comprised of around forty intelligence and signal personnel who were organized into four divisions: plans, intelligence, combat development, and acquisitions.[156] While the organization originally had the ability to both identify requirements and build capability to meet those requirements, it eventually lost the latter function due to federal law which prohibited the placement of development and acquisitions in the same organization.[157]

On 8 May 1995, the Army activated the Land Information Warfare Activity to serve as the service focal point for land-based information operations.[158] LIWA's purpose was to provide information operations support to Army land component commanders, a task which was as much about educating commanders on the relevance of the information space as it was about driving the development of substantive information-related capabilities.[159] This mission entailed the defense of Army automated communications and data systems from intrusion as well as the eventual pursuit of capabilities in the defensive and offensive aspects of any future conflict in cyberspace.[160] LIWA also had broad authority to coordinate with Army, joint, and DoD-wide organizations on the topic of IO. As such, it worked with the special operations community, the Joint Command and Control Warfare Center (JC2WC), and both the

---

[156] Thompkins, interview.

[157] In part due to federal law, and in part due to the fact that the O5 in charge of acquisitions wanted to work for the Assistant Secretary of the Army for Acquisitions and Technology (ASALT), acquisitions eventually split off from SAA to become the INSCOM project manager (PM) for IW. This organization, PMIW, still exists today, and is still the INSCOM program of record with full acquisition authorities for information warfare. (Thompkins, interview).

[158] Memorandum from DA Washington DC to ARSTAF, Subject: "Activation of US Army Land Information Warfare Activity," May 8, 1995. See also INSCOM Command History Office, "The INSCOM Story," INSCOM.mil, updated May 2, 2019, https://www.inscom.army.mil/organization/History.aspx.; and Richard A. Sizer, "Land Information Warfare Activity," *The Military Intelligence Professional Bulletin*, https://fas.org/irp/agency/army/mipb/1997-1/sizer.htm.

[159] Memorandum of Understanding Among Deputy Chief of Staff for Operations and Plans and Deputy Chief of Staff for Intelligence and Director of Information Systems for Command, Control, Communications, and Computers and Commander U.S. Army Intelligence and Securities Command. Subject: "The U.S. Army Intelligence and Security Command's Land Information Warfare Activity. March 24, 1995; this purpose was reiterated in nearly all interviews with former LIWA personnel.

[160] "1st IO Command (Land) History — Information Paper," May 7, 2014, and INSCOM Command History Office, "The INSCOM Story." In October 2000, the commander of LIWA was officially directed by HQDA to assume responsibility as the deputy commander for Army computer network defense and attack in support of SPACECOM.

Air Force and Navy's respective information warfare centers.[161] Concurrent to the creation of LIWA, the SAA dissolved, and its C2W efforts were subsumed under LIWA's charter to engage in information operations.[162]

While LIWA was administratively attached to INSCOM, it was operationally controlled by the Army G3.[163] This command and control relationship reflected two realities. First, as an operational function, information operations would need to be controlled by an operational directorate. Intelligence, as a supporting function to operations, was deemed ill-suited to execute this type of command and control. Second, there was an assumption that operationally assigning LIWA to INSCOM would turn it into an intelligence organization by default, thus requiring LIWA to follow the restrictive procedures of intelligence oversight. While these procedures are a necessary safeguard against intelligence overreach, they were considered an unnecessary handicap on non-intelligence operations that could potentially hinder the much-needed intellectual and practical experimentation that was implied in LIWA's charter.[164] LIWA's direct reporting channel to the Army G3 contributed to the wide operational latitude that the organization enjoyed.

As an activity, rather than a traditional command, LIWA was directed by a colonel with two lieutenant colonels in charge of its respective operations and intelligence directorates.[165] It reported directly to the Army G3. This relationship provided a tremendous amount of flexibility and high level visibility for an organization that otherwise risked falling into operational obscurity. LIWA began with 55

---

[161] Paul E. Blackwell, Trent N. Thomas, Paul E. Menoher, and Otto J. Guenther, Memorandum of Understanding Among Deputy Chief of Staff for Operations and Plans and Deputy Chief of Staff for Intelligence and Director of Information Systems for Command, Control, Communications, and Computers and Commander U.S. Army Intelligence and Securities Command, "The U.S. Army Intelligence and Security Command's Land Information Warfare Activity," March 24, 1995, para. 9a. On JC2WC, telephonic interview with Patrick J. Scribner, November 8, 2018.

[162] Blackwell, et al. Memorandum of Understanding, para. 9b; Thompkins, interview.

[163] The direct lieutenant-general-to-colonel tasking chain that this relationship entailed led to the creation of Department of the Army Management Office, Information Operations Division (DAMO-ODI), which later became DAMO-CY for cyberspace operations. (Muztafago, interview).

[164] Ibid.

[165] Ibid.

people, eleven of whom were enlisted and around a dozen of whom were government civilians.[166] These numbers eventually grew to 230 authorized personnel by October 1997.[167] LIWA was extraordinarily officer-heavy for an Army organization, a fact that is unsurprising given that the bulk of its job was to liaise with division- and corp-level planners. The majority of these officers were field grades and above with an intelligence or signal background.

As LIWA grew in size, the type of expertise it collected expanded through a deliberate effort to incorporate more operationally-minded personnel.[168] These operational personnel were often recruited to provide field support teams with an understanding of how divisions and corps functioned. Even with this growth, intelligence and signal soldiers continued to represent the dominant population. Contractor personnel with additional qualifications would augment the unit as required, with one former unit member stating that half the force was contractors at one point in its history.[169]

LIWA was designed to work itself out of a job by changing how the Army thought about the information environment.[170] It accomplished this through two primary operational efforts: deployable field support teams (FSTs) which assisted corps and division staffs in information operations planning, and vulnerability assessment teams (VATs) that would help units identify how they might be vulnerable to similar enemy efforts.[171] FSTs were small teams of up to ten uniformed military personnel, civilians, and contractors who would deploy for one to six months to provide planning capability to Army unit staffs during overseas deployments and pre-deployment readiness exercises. Team personnel were deliberately selected for their diverse background experiences. The first deployable FST, for example, had an

---

[166] Muztafago, interview.

[167] "1st IO Command (Land) History — Information Paper," May 7, 2014.

[168] LIWA was an operational organization that reported to the G3 of the Army. The organization's senior enlisted leader, for example, was coded for a Special Forces senior non-commissioned officer. (Muztafago, interview).

[169] John Mahoney, telephonic interview with the author, October 12, 2018.

[170] Scribner, interview.

[171] 1st IO Command (Land) History — Information Paper, May 7, 2014; Memorandum from DA Washington DC to All Army Commanders, "Information Operations Support from LIWA," January 8, 1999.

intelligence planner, signal soldier, Air Force electronic warfare expert, an intel analyst with a counterintelligence background, and a contracted military deception planner.[172] These backgrounds spoke to the type of capabilities that FSTs were expected to help units integrate.

As the de facto information operations planners for corps and division level Army staffs, FSTs did not bring organic IO capability across any of the five dimensions of IO.[173] Instead, they provided planning expertise to units that were unaccustomed to thinking about the information environment. Teams also provided an otherwise unavailable level of technological reach back into the national intelligence picture that allowed supported units to engage in proper information systems targeting.[174] Team personnel received extensive training on the supported unit's mission and operational standard operating procedures prior to integration. FST support often culminated in the publication of an IO annex to the unit's base operations order.[175]

As a compliment to the planning efforts of FSTs, vulnerability assessment teams helped units identify their own vulnerabilities to enemy information operations efforts. Units could later request to test their fixes through attacks by LIWA red teams.[176] Individual vulnerability assessment teams soon expanded into a vulnerability assessment division. This division was comprised mostly of signal personnel and it contained two programs: the Information Operations Vulnerability Assessments Program (IOVAP) and the C2W opposing force (OPFOR).[177] The former consisted of the aforementioned vulnerability assessment teams, while the latter existed to replicate these adversary C2W methods in order to condition

---

[172] Tammy Heath, telephonic interview with the author, November 6, 2018; Scribner, interview; Austin Branch, interview.

[173] Teams eventually started to bring along electronic warfare tools, but these were largely discarded by units who lacked the organic understanding of how to employ them. (Mahoney, interview). As an echelon-above-corps unit, LIWA was originally intended to provide IO support at the Army Service Component Command (ASCC) level; lack of adequate staff support at the ASCC level caused LIWA to quickly adjust its support model to focus on corps and division level staffs (Muztafago, interview). FSTs wore the shoulder patch of the unit they supported to enhance integration efforts.

[174] Teams would bring a briefcase with a laptop, battery, and satellite terminal to provide connectivity to INSCOM intelligence worldwide. (Heath, interview).

[175] Mahoney, interview.

[176] Muztafago, interview.

[177] *Field Manual 34-37*, preliminary draft, ch 3.

Army units during training exercises. Over time, this effort expanded to include network vulnerability assessments, setting the precedent for what would eventually become the Army's World Class Cyber OPFOR.[178] The dual combination of FSTs and VATs allowed units to identify how they could attack enemy communication systems, and where their own systems were vulnerable to attack.

From 1996 to 1999, the international peacekeeping mission in Bosnia served as the proving ground for Army information operations.[179] Field support teams in Bosnia were able to test many of the concepts developed through FM 100-6, culminating in the publication of the Draft IO Handbook in 1998.[180] The standard operating procedures developed over years of FST deployments to the Balkans later became the templates for the 2003 version of FM 3-13, *Information Operations*, which provided far more guidance on the practical implementation of IO than its largely theoretical predecessor.[181] One of the practical challenges identified through LIWA's Bosnia experience was how to conduct distributed command and control over geographically dispersed teams. To solve this problem, LIWA used a mix of military and commercial communications platforms to create a robust reach-back capability that would electronically tether its FSTs to the LIWA support center.[182] This effort eventually turned into the Information Dominance Center, which would be important to future Army computer network operations.

Success in the Balkans helped to demonstrate the value of information operations to maneuver commanders. This demonstration of value was critical to normalizing information operations throughout the Army, as few commanders would be willing to risk operational success on a largely unproven

---

[178] Mahoney, interview.

[179] Muztafago, interview; 1st IO Command (Land) History — Information Paper, May 7, 2014. After the 1995 signing of the Dalton Peace Accords, the Army recognized that the Balkans would be an informational conflict rather than a kinetic one. The first LIWA FST hit the ground in Bosnia January 1996.

[180] Though the handbook contained more or less definitive guidance for LIWA operations, it had to be called a draft publication because only U.S. Army Training and Doctrine Command (TRADOC) is authorized to publish doctrine. (Muztafago, interview).

[181] Mahoney, A. Branch, interviews

[182] *Field Manual 34-37*, preliminary draft, ch 3; this point was corroborated by Tammy Heath, interview — as FST team lead her equipment consisted of a suitcase with a laptop, battery, printer, and satellite terminal to provide the most the team with its most important capability: reach back to the intelligence enterprise.

theoretical concept.[183] Observations from the Balkans also drove changes stateside: IO integration soon became a core criteria for passing the Army's large-scale warfighter exercises, which served as validation tests for the proficiency of division and corps commanders.[184]

While much of the early theorizing and experimentation on information operations were offensive in nature, LIWA soon expanded into the realm of network defense.[185] In September 1996, the Army stood up its first Computer Emergency Response Team (ACERT) to improve the management of daily command and control protection and to provide continuous handling of Army computer incidents worldwide.[186] The ACERT was created in response to the Army's efforts to digitize the force in the late 1990s, when the introduction of new tactical communication platforms to maneuver brigades resulted in the introduction of new battlefield vulnerabilities.[187] The ACERT had the ability to conduct limited incident response in the event of a network intrusion through a level of network defense that exceeded the ability of the Army's tactical communicators. The ACERT's success inspired the creation of six regional CERTs that were geographically aligned with combatant commands and were co-located with the theater signal brigades.[188] Both regional CERTs and the ACERT were populated by a mix of signal personnel, civilians, and contractors, and would report incidents through the Theater Network Operations Support Centers (TNOSC) to the Army CERTs.

---

[183] The lack of demonstration of value through the middle years of the Global War on Terror contributed to the IO community's decline.

[184] Muztafago, interview.

[185] Scribner, Branch, Heath, Mahoney, interviews.

[186] 1st IO Command (Land) History — Information Paper, May 7, 2014.

[187] The Army's Force XXI initiative sought to transform the post Cold War Army into a digitized force for the 21st century. It did this through a three-fold effort to redesign the operational Army, redesign the institutional Army, and to integrate information age technologies into the force. LIWA's vulnerability assessment division conducted the network penetration testing for Force XXI. Their success led to the realization of widespread network vulnerabilities that then drove the creation of the ACERT and RCERTs. (Matthew Stern, telephonic interview with the author, Nov 26, 2018). See Susan Bryant and Heidi A. Urben, "Reconnecting Athens and Sparta: A Review of OPMS XXI at 20 Years," *The Land Warfare Papers,* no. 114 (October 2017); and Mark Hanna, "Task Force XXI: The Army's Digital Experiment," *Strategic Forum*, no. 119 (July 1997).

[188] Thompkins, interview.

The expansion of information operations efforts in the late 1990s exacerbated the increasingly complex problem of information management. In 1999, LIWA attempted to solve this problem through the creation of the Information Dominance Center (IDC). The IDC was originally intended to function as a tactical operations center to synchronize plans, operations, and intelligence functionality.[189] As such, it served three purposes: to improve capabilities for network defense and attack, to improve real-time situational awareness and command and control for deployed field support teams, and to expand capability for the production of unique operational intelligence through new methods of data collection and management.[190] As part of its function of network attack and defense, the IDC enabled command and control to the ACERT and RCERTs, which allowed for the streamlined reporting of and rapid response to network incidents worldwide. The IDC also contained a section to coordinate computer network operations (CNO), as well as an attack, sensing, and warning cell which conducted triage analysis on potential intrusions.[191]

LIWA's expansion throughout the late 1990s occurred concurrently with a change in joint terminology. In December 1996, DoDD S-3600.1 formally adopted the term "information operations" to replace information warfare and command and control warfare.[192] This replacement was not a product of a genuine change in military thinking so much as it was a reflection of the government's new sensitivity to foreign and domestic concerns about the militarization of the internet.[193] However, the document did make one notable change through its introduction of the phrase "computer network attack," described as

---

[189] Scribner, interview. The futuristic IDC was designed by DARPA engineers who served as Hollywood set design consultants (Stern, interview).

[190] James E. Heath and Alexander E.R. Woodcock, "The Challenge of New and Emerging Information Operations," unclassified paper released by INSCOM, LIWA (Fort Belvoir, VA: June 1999).

[191] Thompkins, interview. The CNO section mostly served a coordinating function (Scribner, interview).

[192] Department of Defense Directive TS-3600.1, "Information Warfare."

[193] Warner, "Notes on Doctrine."

"operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks or the computers and networks themselves."[194]

In October 1998, JP 3-13 expanded upon the notion of information operations outlined in DoDD 3600.1. Heavily influenced by the Army authors of FM 100-6, this document depicted information operations as a broadening of information warfare, and information warfare as primarily a wartime tool.[195] The five capabilities of information operations were identical to the five capabilities of command and control warfare, with the exception that IO could now include computer network attack.[196] The definition for CNA was identical to its definition of two years prior, although the nature of its application remained ambiguous. The publication made no mention of the term computer network defense, referring only to the offensive potential of computer-based activity.

In 2003, the Army replaced FM 100-6 with FM 3-13, *Information Operations*. This new publication added the practical lessons learned from seven years of LIWA experience to the strong theoretical foundation of its predecessor. Neither command and control warfare nor information warfare made an appearance in this document. Rather, both had been subsumed under a more robust definition of information operations which included computer network operations as one of its five core capabilities. The document described CNO as consisting of three parts: computer network defense, computer network attack, and computer network exploitation, which marks the first such appearance of these terms in any DoD doctrinal publication to date.[197] FM 3-13 suggests that, by 2003, thanks largely to the experimental efforts of LIWA, the Army information operations community had developed a robust understanding of computer network operations as a tripartite orchestration of attack, defense, and exploitative functions.

Given this evolution in doctrine, what form did actual CNO capabilities take in LIWA operations throughout this time period? How was this activity seen by the nascent information warfare community

---

[194] Warner, "Notes on Doctrine."

[195] Ibid. That the joint pub was influenced by Army doctrine: Muztafago, interview.

[196] Warner, "Notes on Doctrine."

[197] The first use of these terms in a joint doctrinal publication was JP 3-13 released in 2006.

that LIWA represented?[198] During LIWA's early years, the experimentation on C2W and the latent CNO concepts it contained were primarily offensive in nature. Over time, LIWA also began to develop its own defensive capability through the expansion of the vulnerability assessment concept. In addition to the creation of CERTs in 1997, LIWA developed blue and red network penetration testing teams, as well as a team which identified changes in worldwide signature information that required the reprogramming of Army software.[199] Called the Army Reprogramming and Analysis Team-Threat Analysis (ARAT-TA). the purpose of the ARAT-TA was to identify and report changes in worldwide signature information that required the reprograming of Army Target Sensing Systems (ATSS) software.[200] Identified threat signature changes were then pushed out to tactical units through the ARAT project office electronic bulletin board.[201]

In tandem with the growth in LIWA's defensive cyberspace capability came the growth of the signal community's involvement in this capability, so much so that the defensive component of LIWA's computer network operations mission had become a default function of the signal community by the early 2000s.[202] This change was the product of two factors. First was the natural territorial claim that signaleers had to the defense of networks through their role as network maintainers. CERTs were attached to NETCOM, for example, because NETCOM and the broader signal community were the ones who owned and operated the Army's networks. To be sure, there was an adjustment period associated with this mission expansion, since signaleers were unaccustomed to thinking in enemy-centric terms. However,

---

[198] It is important to note that LIWA did not provide actual capabilities to supported units, as it did not have a directorate or the requisite authorities to develop them — capability development at the time came from the INSCOM G3 staff for information operations, called the G3IO and led by a civilian (Thompkins, interview). Instead, LIWA's purpose was to drive experimentation on future capabilities based on the ideas and requirements of deployed commanders — particularly in the realm of both attacking and defending electronic communications. The fruits of this theoretical labor were realized through partnership with other organizations, ranging from the special operations community, to special access programs within INSCOM, to research centers such as Lincoln Labs and Johns Hopkins Applied Physics Lab. LIWA funded and built an IO test range to enable this experimentation as early as 1998 (Branch, interview).

[199] Heath, interview.

[200] 1st IO Command (Land) History — Information Paper, 7 May 2014. ATSS included smart munitions, sensors, processors, and aviation electronic combat survivability equipment.

[201] FM 34-37, preliminary draft, ch 3.

[202] Scribner, interview.

network defense eventually became a natural outgrowth of network maintenance at this intersection of signal and IO.

The second factor that contributed to increased signal involvement was the composition of LIWA itself. LIWA was originally designed to have six field support teams of ten people each. Two of those ten people were signaleers.[203] The problem with fielding teams of ten, however, is that operational units are inherently limited in the number of additional people that they are able to absorb. FSTs adapted to this challenge over time by deploying fewer people, which meant that the bulk of their signal personnel stayed behind.[204] Simultaneous to these changes was the creation of the information dominance center in 1999. While the IDC was originally intended as an operations center, over time it became more focused on providing analytic and intelligence support to deployed teams. As the IDC grew in size and scope, so did the complexity of its networks. The signaleers who were no longer rotating out on deployments eventually began to take over stewardship of this functionality in tandem with the FA53s and FA24s whose purpose was the management of information systems.[205] By the time of the transition of LIWA to 1st IO command, signal branch had assumed an implicit stewardship of much of the IO community's network defense mission.

1st Information Operations Command

By 2002, LIWA had grown to an organization of over 500 people. As a reflection of its increase in both size and importance, LIWA was renamed and elevated into the 1st Information Operations Command. This elevation occurred a few years after — and was no doubt influenced by — the creation

[203] Scribner, Interview.

[204] A. Branch, interview.

[205] A. Branch, interview. FA53 is Information Systems Management functional area and FA24 is Information Systems Engineer. Both career fields are trained by the U.S. Army Signal School.

of the Army's first information operations career field, FA30.[206] 1st IO command split its previous LIWA functionality into two battalions: 1st battalion contained the FSTs and VATs, and 2nd battalion contained the CERTs and all related computer network efforts.[207]

Second battalion was organized into two detachments. Detachment A contained the CERTs. Detachment B contained mission support teams that provided CNO planning capability to deployed commanders, conducted independent validation and verification of security for army networks, and created experimental solutions to security problems that could be rapidly deployed across the Army.[208] As part of its mission to support CNO planning, 2nd battalion developed a liaison relationship with the computer network personnel in the Army's 704th Military Intelligence Brigade at Fort Meade, Maryland. CNO planners in the detachment were familiarized with the 704th's network warfare capabilities — in addition to all other network warfare capabilities across the DoD — prior to deployment, so that they could request said capabilities in support of the deployed commander. In addition, the battalion kept a small element of personnel on temporary duty at Fort Meade, where they received additional computer network training and provided technical support to 704th computer network operations.[209]

The consolidation of computer-related capabilities into a single battalion led to a flourishing of computer network expertise within 1st IO Command. It further allowed 1st IO to help synchronize computer network operations across the Army.[210] Two factors contributed to the development of this expertise. First, the battalion's composition — eight active duty, 190 contractors, 33 civilians, and around 60 reservists — and an enormous contractor budget allowed it to recruit an extraordinarily high caliber of

---

[206] How did the creation of a career field influence the transformation of LIWA? In the Army, officers need command to get promoted. The elevation of the Army's IO organization from an activity to a command resulted in the creation of companies and battalions that could be commanded rather than detachments and divisions that could merely be led or supervised. (A. Branch, interview).

[207] 1st battalion today also includes OPSEC support and training teams, as well as a number of other capabilities to include social media analysis and engagement for Army and Joint forces

[208] Stern, interview.

[209] Ibid.

[210] Ibid. Colonel John Davis, 1st IO commander from 2006-2008, drove the synchronizing mission for 2nd battalion.

personnel.[211] Second, the battalion's unique charter and wide operational latitude allowed it to pursue a virtually unlimited number of professional development opportunities that would be otherwise unavailable to an ordinary army unit.[212] Battalion personnel traveled to hacker conventions around the world, where they interacted with hackers of all stripes to learn about cutting edge exploits, vulnerabilities, and penetration methods. This exposure had the effect of increasing the battalion's computer network expertise while normalizing Army computer network operations across a wide variety of audiences.[213] Exposure to Army, joint, and interagency capabilities as well as cutting-edge private sector technology ensured that 2nd battalion's CNO planners could provide adequate CNO support to deployed commanders.

Ownership of the Army CERTs also meant that the 2nd battalion commander had responsibility for the security of all networks in the Army.[214] This responsibility meant that command of the battalion usually fell to an FA53 or FA24 network technician.[215] The battalion was responsible for reporting intrusions to the Army Chief of Staff within four hours of detection.[216] However, it had little authority to implement the reforms necessary to fix the underlying network vulnerabilities the intrusions in the first place.[217] In the event of an intrusion, second battalion would send teams of technical experts called

---

[211] Stern, interview.

[212] Ibid.

[213] Matt Stern, who was the commander of 2nd battalion from 2006-2008, described the beneficial secondary effects of these interactions through one such event where his personnel went head-to-head against hackers. They were told they'd be attacking Windows systems only to find out that they'd have to attack Linux machines instead. Since these 2nd battalion personnel were unprepared to attack Linux, they focused all of their energy on defense. Their systems went uncompromised as a result. Witnesses spread the results of the competition across online hacker forums with a warning that Army systems were impenetrable and Army defenders were too good. Army network compromises deceased by 55% that year, while compromises into the rest of the DoD went up.

[214] Stern, interview.

[215] That second battalion was usually commanded by an FA53 or FA24 meant that it was not available for command by an FA30 IO officer, thus leading to the further, gradual marginalization of the FA30 community even within the 1st IO Command.

[216] Stern, interview.

[217] A classified memorandum written by the Chief Information Officer for the Secretary of Defense, John P. Stenbit, outlined the different tiers of response actions that the battalion had to follow upon detection of a network intrusion. These response actions ranged from local coordination with installation commanders, to coordination with JTF-GNO for action across the DoD, to even higher response actions that required presidential approval. (Stern, interview).

network damage assessment teams to conduct local analysis. More often than not, the CERTs would have to send their network remediation recommendations to NETCOM. Populated by Army signaleers who were more concerned with network availability than network security, NETCOM had an inconsistent record of following through with these recommendations. The battalion commander often relied upon his direct reporting line to the Army G3 in order to gain leverage to get higher ranking installation commanders to acquiesce to unfamiliar remediation measures.[218]

After the stand-up of Army Cyber Command in 2010, 2nd battalion grew to include the Army's World Class Cyber Opposition Forces (WCCO), which was created to replicate adversary cyber capabilities to test Army networks during major training exercises.[219] The Cyber OPFOR was originally intended to provide full-spectrum information operations capability to replicate a sophisticated adversary threat during Army training rotations, to include electronic warfare and on- and off-net cyberspace operations. However, a lack of resources and manpower combined with organizational discord over the allocation of responsibilities resulted in the WCCO defaulting to scripted on-net operations — thus falling short of their original vision.[220] 1st IO Command continued to house the Army's CERTs until the activation of Army Cyber Command in 2010, at which point the CERTs were renamed to Regional Cyber Centers (RCCs) and transferred to ARCYBER upon the activation of that command in 2010.[221] As of 2019, 1st IO's only cyber capability consists of the World Class Cyber OPFOR. All other cyber-related

[218] Stern, interview.

[219] Of note, the original vision for the WCCO was akin to what the Army would later achieve with CSCB. However, 1st IO Command lacked the vision, resources, or cultural unity to make this original vision a reality (Matthew D. Giovanni, telephonic interview with the author, December 14, 2018.

[220] While the different components internal to 1st IO, such as the VATs or red teams, could have provided all the desired capabilities to achieve the WCCO's original intent, many of these components were reluctant to participate, just as the WCCO was reluctant to include them out of original guidance that the WCCO would provide all necessary cyber capabilities by itself. (Giovanni, interview).

[221] Richard D. Moore and Anthony F. Portare, telephonic interview with the author, October 18, 2018.

efforts were subsumed by ARCYBER, until eventually the entire 1st IO was placed underneath the new command.[222]

The history of the Army information operations community suggests that computer network operations had both their conceptual and practical origins in the command and control warfare concepts of the early 1990s. While the technology and the terminology to enable these ideas had yet to develop, much of the experimentation required to realize them took place within the Army's nascent information operations community from 1995 to roughly the mid-2000s. Many of the offensive CNO capabilities that were subsequently developed came directly from requirements identified through FST deployments in support of Army operational units. Furthermore, the entirety of the Army's defensive computer network mission originated within LIWA and remained in the IO community until the creation of ARCYBER and the cyber branch in 2010 and 2014 respectively. The amount of early cyber expertise within the IO community was such that the Army's first cyber planner course was created and run by 1st IO command.[223] This course later became a standard requirement for Army officers in a cyber planning role, regardless of branch affiliation.

---

[222] On the movement of 1st IO to ARCYBER, see John M. McHugh, Secretary of the Army Memorandum, "Army Directive 2011-03 (Change of Operational Control for 1st Information Operations Command (Land) and Direction for U.S. Army Cyber Command to Conduct the Information Operations Missions for the Army)," February 2, 2011. The transformation of LIWA into 1st IO Command paralleled the release of a series of joint declarations that sought to elevate information operations into a core capability of future military forces. The first was the 2001 Quadrennial Defense Review, which required the Department of Defense to treat IO, intelligence, and space assets as core defense competencies on par with air, ground, maritime, and special operations rather than simply enablers for military forces. The second publication was the 2003 Information Operations Roadmap, a then-secret document authorized by Defense Secretary Donald Rumsfeld which has since been declassified. The 2003 IO Roadmap outlined three critical tasks required to make IO into a core military capability for combatant commanders: network defense, network attack, and psychological operations. The five core capabilities of IO — electronic warfare, psychological operations, operational security, military deception, and computer network operations — remained the same as in previous joint doctrine. Importantly, the roadmap advocated the need for a common understanding of IO among the services that was focused explicitly on the degradation of adversary decision-making and the protection of friendly decision-making capabilities. This understanding of IO would guide joint doctrine for several years to come, and would make the Army's later doctrinal departure all the more consequential.The roadmap also argued for the development of IO planners and capability specialists to remediate the existing deficiency of qualified IO personnel. In conjunction, it stated a need to devote substantial energy to the expansion of both computer network defense and attack capability across the joint enterprise. Several pages of discussion devoted to computer network operations emphasized the growing importance of the digital battlefield to future military engagement. Practically, however, the IO Roadmap had the effect of encouraging a split between the technical and cognitive portions of information operations (this point came from Michael Dominque, telephonic interview with the author, Nov 13, 2018). The different IO capabilities then began to fight over resources in an effort to fulfill the vision put forth in the joint roadmap.

[223] Mahoney, interview.

What accounts for the strong cyber expertise in these early IO organizations from roughly 1995-2008? For the first portion of LIWA's existence, the fact that the Army did not have an information operations career field proved an innovation advantage. Absent a cadre of officers who had received standardized IO training, the Army deliberately populated LIWA with officers from a variety of operational backgrounds and experiences — albeit with a heavy emphasis on signal and military intelligence. The flexibility LIWA received by virtue of its relationship with the Army G3 allowed it to pursue training in a similarly ad hoc manner, with the result that personnel were extensively trained in a variety of operational modalities in order to build up a broad base of subject-matter expertise. Moreover, the fact that much of this training came from either the private sector or contractors due to a lack of equivalent instruction within the institutional Army meant that LIWA personnel were not only well trained, but were well trained in the most cutting-edge concepts and capabilities that existed across government and industry. Finally, the high number of LIWA civilians and contractors allowed the organization to attract a level of talent and creative thinking that did not exist and could not be easily reproduced within its cohort of uniformed personnel. Thus, unburdened by the operational proclivities of a uniform subculture, LIWA was able to experiment both technologically and conceptually in a way that more traditional Army organizations were not.

DOCTRINAL CHANGES AND A NEW PERSONNEL FIELD

However, in spite of this extensive early involvement in the development of the concept of computer network operations, the information operations community's later influence on the creation of ARCYBER and the Army cyber branch was comparatively small. Why was this so? The community's eventual slip from relevance was the result of two primary factors: a change in the definition of information operations, and a change in the management of information operations personnel. In the mid-2000s, at the behest of the Army Combined Arms Center (CAC) and in defiance of protestations from both the information operations community and Army maneuver commanders, IO was redefined

from an integrating function that enabled the disruption of enemy decision-making to "inform and influence activities:" "the integration of designated information-related capabilities in order to synchronize themes, messages, and actions with operations to inform United States and global audiences, influence foreign audiences, and affect adversary and enemy decision-making."[224] While this redefinition was not formally codified until the 2008 release of the Army's seminal operations manual, Field Manual 3-0, the ideas behind the redefinition first began to circulate around 2005.[225] FM 3-13, retitled *Inform and Influence Activities*, was updated to reflect this change in 2013.[226]

The new definition of information operations that began to circulate in the mid-2000s and was codified doctrinally in 2008 led to ambiguity in the Army's understanding of what IO could actually provide.[227] Inform and influence activities as then defined seemed to be more the purview of psychological operations than information operations, which meant that it became more difficult to justify the purpose of having a separate information operations staff function. The redefinition of IO away from its original five elements also meant that these five elements now had room to elevate themselves as individual capabilities which were distinct from any unified whole. Thus, the fields of EW, PSYOP, MILDEC, OPSEC, and CNO began to split away, and to lobby for resources and prestige independently of the mechanism which formerly held them together.[228]

---

[224] Headquarters, Department of the Army, *Field Manual 3-0: Operations* (Washington, D.C.: Headquarters, Department of the Army, February 27, 2008). Many former LIWA and 1st IO members I interviewed referenced this redefinition and the widespread opposition to it by all but a few senior Army leaders. Why the redefinition? Interview feedback suggested that the 2003 IO Roadmap had the effect of encouraging a split between the technical and cognitive portions of information operations, such that the different IO capabilities began to fight over resources in an effort to fulfill the vision put forth in the joint roadmap. Others traced the decision to the influence of a few senior leaders who were heavily shaped by their experience in the "hearts and minds fight" of Iraq. Regardless of the source of the redefinition, it was met with widespread resistance within the IO community as a substantial departure from both Army and joint doctrine.

[225] Scribner, interview. Of note, CAC attempted to release an updated FM 3-13 in 2008 with the new inform and influence definition, but this effort narrowly failed.

[226] In a tribute to the insufficiency of the new definition, the 2013 edition of FM 3-13, titled *Inform and Influence Activities*, was one of the shortest-lived doctrinal publications the Army has ever issued. Three years in the making, it lasted nine months in print before the Chief of Staff directed the Army to change it. (Scribner, interview).

[227] Matthew J. Sheiffer, "U.S. Army Information Operations and Cyber-Electromagnetic Activities: Lessons from Atlantic Resolve," Military Review online exclusive, March 19, 2018, https://www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2018-OLE/Mar/Army-Info-Ops/.

[228] A. Branch, interview.

Furthermore, the ground conditions of the global war on terror had replaced the simple enemy-centric model of conventional conflicts with the necessary yet far more complex population-centric model of counterinsurgency. These changes to the conditions of conflict from an enemy-centric conventional battle to a largely ideological counterinsurgency meant that the spirit of C2W which had invigorated the Army's earlier understanding of IO — inhibiting adversary decision-making by attacking his methods of communication and the underlying availability of information — became increasingly difficult for commanders to either understand or apply. The ideological battleground of the counterinsurgency in Iraq, and the related discovery that the Army was poorly equipped to conduct the necessary ideological messaging, likely had a substantial influence on the small handful of senior Army leaders who pushed the doctrinal change, to the widespread disagreement of the IO community itself.[229]

Problems with the creation of the FA30 functional area in the early 2000s exacerbated the effects of this IO doctrinal ambiguity. First, the career field had a tendency to attract mediocre officers who lacked the professional attributes required to successfully integrate into maneuver staffs.[230] While there were a number of good, qualified officers who were driven into the field by a particular passion or skill, an even larger number did not voluntarily transfer into IO so much as they fled their own base branches and the diminished career prospects contained therein.[231] The influx of this mediocre officer talent into the IO community occurred at the exact time that the Army decided to adopt a new definition for IO, one which was more confusing, harder to sell, and whose consequences were more difficult to measure.

Second, the creation of an information operations career field was not followed by the creation of an adequate training program. Prior to the creation of the FA30 functional area, LIWA's IO personnel were seen as a combination of staff planners and informal technical experts.[232] They alone possessed the

---

[229] This point was suggested by many former LIWA and 1st IO Command members in interviews.

[230] Heath, Branch, interviews.

[231] I do not mean to demean the many high-performing FA30s that have existed over the years, a number of whom were interviewed for my dissertation. However, the phenomenon of underperforming officers transferring into IO had a very real effect on the quality of IO support throughout the mid-2000s that was noticed both inside and outside of the IO community.

[232] Dominque, interview.

expertise necessary to find the complex technical solutions to forward operational problems. In order to cultivate this expertise, LIWA personnel attended whatever contractor and interagency training was necessary to familiarize with new and emergent technologies.[233] The lack of a standard IO training program had the paradoxical effect of ensuring that LIWA soldiers were extensively well trained. Moreover, the lack of an integrated IO career field prevented the performance of the IO from being unduly influenced by homogenous behavioral and cultural practices, even while it remained procedurally standardized. With the creation of the FA30 information operations functional area, IO officer identity began to lean heavily towards the role of staff integrator at the expense of the development of any particular subject-matter expertise. The unlimited specialized training courses that were available under LIWA were eventually replaced with a single twelve-week course at Fort Leavenworth on the basics of information operations and Army staff work.[234] This abbreviated training was insufficient to either cultivate intellectual ingenuity, or to create the type of expertise necessary to convince maneuver unit staffs that information operations was worth their time. In other words, IO officers became more beholden to the staff processes in which they were trained rather than to the type of independent critical thinking that had previously marked information operations as a field.

Just as training opportunities for information operations officers fell in tandem with the quality of the average FA30, demand for IO support rose in multiple theaters of conflict. However, because 1st IO Command had limited resources with which to satisfy this demand, they prioritized the support of the special operations and strategic communities rather than the conventional army. To fill the conventional support gap, 1st IO began to mobilize teams comprised of national guard and reserve personnel.[235] These teams were organized into theater information operations groups that were modeled after 1st IO command, but that consisted of personnel who had inferior training and insufficient operational

---

[233] Heath, Scribner, Gray, interviews.

[234] Dominique, interview. The 12 week course was finalized around 2008, which meant that there was no formalized IO training for FA30s for the first several years of their existence.

[235] Dominique, interview.

experience. The resultant poor quality of support decreased the expectations of conventional maneuver commanders as to IO's operational relevance. In contrast to the Army's positive experience in the Balkans, information operations support to conventional operations during the middle years of the global war on terror had the effect of delegitimizing IO as a relevant combat capability.

The insufficient levels of expertise displayed by IO personnel only exacerbated the desires of its constituent parts — EW, PSYOP, MILDEC, OPSEC, and CNO — to further distance themselves from the center, thus hastening the centrifugal demise of a once unified community.[236] The structural absence of a general officer billet within the FA30 career field then made it increasingly difficult for the community to advocate for itself as its members began to split apart.[237] As a result, the IO community lacked the institutional influence to push its vision for the future of cyberspace operations — a future in which cyberspace was doctrinally subordinate to information operations, with the community having an increased say in the deconfliction and employment of cyberspace capability.[238] From 2009-2011, the FA30 career field had to fend off multiple efforts by other Army communities to absorb it, to include military intelligence, cyberspace, special operations, psychological operations, and fires.[239] All of this happened at exactly the time that ideas of cyberspace and cyberspace operations began to gain increased attention in the world of signals intelligence.

---

[236] Dominique, interview.

[237] Scribner, Dominique, interviews.

[238] 1st IO command wanted cyber to be doctrinally underneath IO, but it lacked the necessary institutional influence to advocate for this position. The cyber community, meanwhile, argued that they had their our own integration responsibility in the form of the Cyber-Electromagnetic Activities (CEMA) cell. This disagreement led to the question of how to give cyber autonomy while still affording the information operations officer some authority to ensure that cyber and IO activities will not conflict (Dominique, interview).

[239] Dominique, interview. These communities did not want the IO mission so much as they wanted the billets that went along with it. Specifically, ARCYBER wanted to create two more cyber battalions, PSYOP wanted to create a second group, MI would train the IO people to be military intelligence, and FA just wanted to backfill vacant billets.

SUMMARY: THE INFLUENCE OF INFORMATION OPERATIONS

Cyberspace operations emerged within the information operations community as an outgrowth of command and control warfare concepts of the 1990s. While the technology and the terminology to enable these ideas had yet to develop, much of the experimentation required to realize them took place within the Army's nascent information operations organizations from 1995 to roughly the mid-2000s. Many of the offensive CNO capabilities that were subsequently developed came directly from requirements identified through field support team deployments in support of Army operational units. Furthermore, the entirety of the Army's defensive computer network mission originated within LIWA and remained in the IO community until the creation of ARCYBER and the cyber branch in 2010 and 2014 respectively.

The initial ingenuity, flexibility, and creativity that was demonstrated by LIWA and 1st IO Command in response to operational IO requirements was product of both the organization's wide mission charter and its unique personnel composition. The absence of a dedicated IO career field for the first two-thirds of LIWA's existence meant that was not beholden to a single way of thinking or to a single set of standardized training constraints. On the contrary, LIWA deliberately sought a mix of uniformed and non-uniformed personnel from a variety of operational backgrounds in order to adequately respond to the unstructured challenges the organization faced. These personnel received private sector and industry training commensurate with the operational and technological requirements of a mission whose contours had yet to be firmly established.

In spite of LIWA's early successes, changes in both doctrine and personnel management practices came to have a detrimental effect on the community's lasting cyberspace influence. The Army's mid-2000s shift in IO doctrine — from a largely technical focus on disrupting enemy decision-making to the amorphous concept of inform and influence — was driven by a small handful of senior service whose recent experience on the ideological battlegrounds of Iraq had convinced them that the Army needed to deviate from both joint consensus on IO and from its own doctrinal heritage. These changes were

universally opposed by members of the information operations community, and had the effect of increasing the difficulty of IO integration into Army operations.

Changes in personnel management practices took the form of creating an information operations career field with its own standardized training. This resulted in a cadre of officers who were insufficiently trained to provide adequate subject matter expertise in the components of IO, yet who were perhaps too sufficiently acculturated in an unwavering set of processes and procedures that precluded the type of creative theorizing that had defined previous IO practice. The result was a field without direction, without strong senior leadership, and with a poor institutional reputation at precisely the time that the larger Army's interest in cyberspace operations — once both a functional and doctrinal component of IO — began to intensify.

The Influence of Signals Intelligence

While much of the conceptual development for cyberspace operations took place under the guise of information operations, the Army intelligence community played a dominant role in the formation of deployable cyberspace capability.[240] Army intelligence eventually ended up as one of the largest bill payers for the creation of cyber branch. A brief history of how this community formed will provide insight into some of the key factors that influenced its approach to cyberspace through the late 1990s and 2000s.

[240] I will briefly discuss the nature of these capabilities in a later section. However, offensive cyberspace capabilities of the sort created by the intelligence community before the advent of Army Cyber Command (in other words, from 1998-2010) consisted largely of a type of "active SIGINT" against digital and cellular targets that would be largely underwhelming if presented as cyberspace capabilities today. Nevertheless, they represented an important stepping stone from electronic attack, which was largely a blunt instrument of denial across the electromagnetic spectrum, into today's world of offensive cyberspace operations, which tend to be a more carefully tailored application of denial and disruption through digital networks.

HISTORY

The shape of Army military intelligence as it is known today began with lessons learned from the latter stages of the Vietnam War.[241] During the Vietnam War, Army signals intelligence fell under the purview of the Army Security Agency (ASA).[242] The ASA deployed about one-fifth of its total population to Southeast Asia through radio research battalions, ground collection stations, and airborne collection assets. It also attached specially tailored companies and detachments to American divisions and brigades in order to provide direct SIGINT support to tactical commanders.[243] These teams provided valuable SIGINT information on enemy dispositions and movements through both airborne and ground-based direction-finding platforms. However, while most ASA teams fell under the operational control of the in-country intelligence unit to which they were attached, the ASA exercised centralized direction of these teams from its own separate headquarters.[244] This arrangement denied local ground commanders operational control of a key component of their intelligence collection.

Troop drawdowns after the Vietnam War, combined with a lingering sense within the Army that intelligence collection and analysis in theater could have been done better, created pressure to reorganize the Army intelligence structure.[245] Army Chief of Staff General Frederick C. Weyand commissioned the Intelligence Organization and Stationing Study (IOSS), under the direction of Major General James

---

[241] The Army intelligence community effectively began on 1 July 1962, when the Army Chief of Staff signed an order creating the Army Intelligence and Security Branch. Limited to about 4,000 officers, the branch encompassed all existing fields of intelligence, including signals, strategic, imagery, combat, human, and CI. It was re-designated the Military Intelligence Branch on 1 July 1967, by which point Army intelligence was involved in the conflict in Vietnam. From Michael E. Bigelow, "A Short History of Army Intelligence," INSCOM Command Historian, 41. https://fas.org/irp/agency/army/short.pdf.

[242] Alfred Price, *The History of U.S. Electronic Warfare Vol III: Rolling Thunder Through Allied Force, 1964-2000,* (Association of Old Crows, 2000), 300-303. The Army Security Agency was established on September 6, 1945, to encompass all signals intelligence and communications security establishments, units, and personnel. (Memorandum from the War Department, "Establishment of the Army Security Agency," Washington D.C. September 6, 1945, http://armysecurityagencyveterans.net/history-of-the-army-security-agency/.) The ASA assumed SIGINT responsibilities from the SSA (Signal Security Agency) on September 15, 1945. It had a number of fixed field stations supplemented by semi-fixed mobile formations. Through large regional headquarters in Germany and the Pacific, the ASA exercised tight control over these overseas elements, but it centralized direction and processing at its Arlington Hall headquarters in Washington DC. (Bigelow, "A Short History," 39).

[243] Bigelow, "A Short History," 43.

[244] Price, *History Vol. III*, 301.

[245] Ibid.

Ursano, to explore alternatives.[246] The Ursano Report, released in 1975, was highly critical of the state of affairs within Army intelligence. It found that Army intelligence was fragmented among too many agencies, with the ASA in particular accused of being too functionally independent from the broader Army it served. This independence led to a "stovepipe" of SIGINT that prevented the effective development of all-source intelligence.[247] As one historian wrote:

> In the panel's opinion, the ASA pattern of organization had actually impeded the development of an efficient mechanism for carrying out intelligence and electronic warfare. The monopoly of signals intelligence and electronic warfare by an organization operating under compartmented secrecy had artificially kept signals intelligence out of the general intelligence flow and had largely excluded the rest of the Army from involvement in the vital electronic warfare field. At the same time, ASA's preoccupation with the cryptologic aspects of its mission had prevented it from keeping up with new trends in electronic warfare, despite the emphasis which the Army now had given to the latter function.[248]

The report made a series of far-reaching recommendations which were approved in August 1976. These recommendations resulted in the most sweeping changes to Army intelligence since World War II, and made the Army intelligence apparatus more deliberately integrative in both its structure and its personnel practices.

Central to this reorganization was the dismembering of the ASA to bring SIGINT operations more in line with the rest of the Army. The agency's training structure and research and development arms were integrated with Army Training and Doctrine Command (TRADOC) and Army Material Command, respectively. Its tactical units were subordinated to field commanders at corps and divisional level through the creation of Combat Electronic Warfare and Intelligence (CEWI) battalions.[249] Those parts of the ASA that remained were merged with the Army Intelligence Agency and several intelligence

---

[246] Bigelow, "A Short History," 46.

[247] Ibid.

[248] Price, *History Vol III*, 302.

[249] Ibid, 302-304. See also Ruth Quinn, "522nd MI (CEWI) Battalion Passes Tactical Intelligence Test, April 7 1977," Army.mil, https://www.army.mil/article/123363/522nd_mi_cewi_battalion_passes_tactical_intelligence_test_april_7_1977.

production elements to become the Army Intelligence and Security Command (INSCOM) on 1 January, 1977. INSCOM thus emerged as the Army's single instrument to conduct and coordinate multi-disciplinary intelligence operations at levels above corps.[250] INSCOM remains the Army's most powerful intelligence organization today.

A series of additional studies throughout the 1980s were meant to further improve the Army's ability to deliver intelligence by addressing the breakdown between the strategic and tactical components of the intelligence community.[251] Combined with the Ursano-driven reorganization of 1977, these efforts attempted to answer the question of how to organize battlefield surveillance and electronic warfare in a way that was most responsive to ground units.[252] As such, the studies built out the current MI force and provided the foundation for differences in how the tactical and strategic Army thinks about intelligence support. Of foremost concern were the contrasting roles of communication versus exploitation, as well as the challenges posed by classification differences between echelons above and echelons below corps. Echelons above corps tended to operate at the TS//SCI level, while echelons below corps tended to operate at the secret level, with limited access to TS//SCI.[253] This bifurcation would pose challenges to the introduction of tactical SIGINT, and would later challenge the efforts of Detachment Meade to provide meaningful cyber capability to ground units.

What are the implications of this history for the future development of cyberspace operations? First, the creation of CEWIs and the merger of electronic warfare with military intelligence contributed to the erosion of electronic warfare capability and a loss of electronic warfare expertise throughout the 1990s and early 2000s. By placing its electronic warfare capabilities within tactical signals intelligence

---

[250] Bigelow, "A Short History," 46.

[251] Content of paragraph taken from the author's interview with GEN (R) Keith Alexander, Sep 24, 2018. The Intelligence and Electronic Warfare (IEW) Mission Area Analysis of 1980-1981 looked at Army intelligence activities at corps level and above; this study was followed by a series of discussions for the Vice Chief of Staff of the Army from 1983-1985 called the IEW Tech Laydown: The MI Story. Following on the heels of this study, the 1988 Army Intelligence Master Plan created a vision for Army intelligence through 2004.

[252] Alexander, interview.

[253] GEN (R) Keith Alexander, who was heavily involved in the aforementioned studies as a young officer, provided this insight.

units who saw jamming as counterproductive to their primary practice of intelligence collection, the Army unwittingly assured that electronic warfare — and the skills required to engage in it — would receive a lower prioritization. This decline would limit the ability of the electronic warfare community to influence the later development of cyberspace operations.

Second, the dissolution of the ASA and subsequent move of SIGINT capabilities under Intelligence and Securities Command reflected the Army's belief that SIGINT must be structurally integrated with other intelligence capabilities in order to provide the most effective support to ground commanders. While the various legal restrictions and oversight procedures surrounding the practice of signals intelligence meant that this integration would never be total, integration — along with the associated need to make intelligence more responsive to tactical commanders — nevertheless became an important driving principle over the next several decades. However, this reorganization and the integration it imposed had consequences for the development of Army intelligence officers, in that an integrated command structure incentivized the development of generalist intelligence officers. Officers were bred to have a broad familiarity with all intelligence disciplines yet little to no specialized expertise in any of them in order to prepare them for command of multi-faceted intelligence organizations.[254] This generalizing tendency precluded the future emergence of a highly technical cadre of SIGINT-capable officers upon whom the Army could later rely for its cyber expertise.[255]

ORGANIZATIONS

Detachment Meade

Nevertheless, it was from this signals intelligence community that the Army's earliest dedicated cyberspace organization would emerge. In June of 1998, the 704th Military Intelligence Brigade — the

[254] Officers have a limited ability to specialize through multi-week long courses and immersion programs that culminate in receipt of an additional skill identifier; however, this specialization does not guarantee a career track in any particular field. The only way for officers to become experts in any particular discipline is to leave the conventional military entirely through an excepted career program. Understandably few officers chose to do this.

[255] The Navy's experience offers a contrasting model: their maintenance of a separate cryptologic community at the officer level meant that they had a stronger pool of expertise to draw upon when the time came to build out cyber capability. See chapter 4.

Army's signals intelligence brigade within INSCOM — was tasked to develop a computer network operations force for the Army.[256] This task fell to B Co of the 742nd Military Intelligence Battalion, which dedicated a small platoon of soldiers to the problem.[257] The intelligence community's exploration of computer network operations emerged as the natural response to a technological migration from analogue to digital communications. At the time, most CNO was performed by the National Security Agency under the auspices of signals intelligence collection, with the service CNO elements providing support to the joint intelligence community.

In June of 2000, this small effort grew into Detachment Meade, a small outfit of approximately three dozen soldiers that was established to sustain the growing need for an Army computer network operations force.[258] Both Detachment Meade and its predecessors maintained a close relationship with LIWA, and later 1st IO Command: Det Meade provided capabilities while LIWA worked to integrate them into Army operations.[259] However, the detachment faced a number of challenges to its task of growing the Army's cyber capability. First, the organization was small and shrouded in secrecy, a by-product of its origins in the strategic SIGINT community.[260] Efforts to increase awareness of the detachment's capability and potential were complicated by the lack of any unclassified doctrine on computer network operations, which did not arrive until the 2003 edition of FM 3-13.[261]

---

[256] "History, 780th Military Intelligence Brigade," INSCOM.mil, accessed Sep 9, 2018, https://www.inscom.army.mil/MSC/780MIB/history.html. Beginning in 1995, the 704th had a small element, approximately 25 person element that supported the National Security Agency's information warfare product manager and related development products. However, the lack of an unclassified doctrine for computer network operations hindered the element's ability to inspire a larger conversation. The inclusion of computer network operations in the 2003 edition of FM 3-13 finally sparked a broader, unclassified conversation on the subject of cyberspace and its relevance to the Army. (Alfred Monteiro, telephonic interview with the author, Dec 7, 2018).

[257] Monteiro, interview.

[258] "History," 780th Military Intelligence Brigade. Monteiro placed the initial estimate between 36 and 39 personnel, only around half of whom had the necessary skill set to engage in the detachment's mission.

[259] Monteiro, interview. Det Meade was also reliant on LIWA for its special technical operations (STO) capability.

[260] One 742nd BN CDR who took command in mid-2003 didn't even know about Det Meade until a month into her command. In this, Det Meade was as much of an unknown quantity to its own parent organization as it was to the larger Army. (Lisa Bennett, telephonic interview with the author, Oct 23, 2018).

[261] Monteiro, interview.

Additionally, the lack of a dedicated computer network operations career field meant that the detachment had a hard time finding qualified soldiers to fill its ranks. Only around half of the detachment's initial cohort had the requisite skill set to engage in the assigned mission.[262] In the absence of a clear accessions pipeline, the only way for Det Meade to find the right talent was to send a recruiting team out to look for it.[263] This method resulted in a cadre of 89 soldiers by the early 2000s, the majority of whom had a signals intelligence background with a small minority coming from the signal community.[264] Soldiers received sporadic technical and tactical training from the NSA and associated agency vendors on an as-needed and as-available basis.[265] Absent a formal training progression, consistent course availability, or even a large training budget, Det Meade soldiers had to rely heavily on individual self-study to rectify gaps in their technical knowledge.[266]

The lack of an appropriate career field also caused retention challenges: because detachment soldiers were managed from within their traditional field of signals intelligence, regardless of the specialized computer expertise they may have possessed, the soldiers faced a real threat of being forced into a more conventional assignment by the Army personnel system. To protect against this tendency, the unit invested in a special management program that effectively kept its soldiers hidden from conventional Army human resources.[267] This program allowed those with the appropriate talent to avoid the Army's three-year unit rotation cycle, and thereby remain in Det Meade indefinitely. However, the special management status that this program conferred complicated the unit's efforts to interface with the regular Army or to deploy in support of it.[268] When coupled with the fact that most of the Army's CNO

---

[262] Monteiro, interview.

[263] The recruitment team, as of late 2003, was comprised of an E8 and a warrant officer. The traveling recruitment model was formally adopted by the 742nd battalion commander in late 2003. (Bennett, interview).

[264] Bennett, Minnick, Monteiro, interviews.

[265] Bennett, interview.

[266] Minnick, interview.

[267] Monteiro, interview.

[268] Bennett, interview.

capabilities were heavily protected by compartmentalized special access programs — many of which were legacies of the strategic SIGINT system and were not seen as operationally necessary by unit members — deployed units would often find it easier to ignore the small CNO teams they received rather than find a way to integrate them into their operations.[269] Partially as a result of these difficulties in supporting the conventional force, Det Meade shifted its focus to the special operations community in the mid-2000s.[270]

Det Meade's unique recruitment, training, and management model had resulted in the creation of a highly specialized and highly skilled force of just under 200 soldiers by the mid-2000s.[271] However, this force lacked both the capability to demonstrate its operational worth and the vision to articulate why such capability was worth pursuing. Inconsistent chain of command support and a lack of centralized direction resulted in a more or less ad hoc approach to the pursuit of computer network operations from 2000-2006.[272] As one former unit member described, Det Meade was a small core group of people trying to figure out what could be done with limited resources in an area that did not have much guidance.[273] Much of this organizational confusion stemmed from the fact that computer network operations were neither well-defined nor well-understood in the early- to mid-2000s.

Though the phrase "computer network attack" first appeared in the joint lexicon with the publication of JP 3-13 in October 1998, it was only vaguely described as a subcomponent of information operations with little guidance as to how it could be practically implemented.[274] While the Army's release of FM 3-13 in 2003 provided a slightly more detailed articulation of the concepts of computer network defense, attack, and exploitation, the fact that this was an IO manual rather than an intelligence one likely kept these more detailed explanations from having much of an impact on the intelligence community.

---

[269] Bennett, interview. On SAPS, Monteiro, interview.

[270] Bennett, interview. This shift was also no doubt due to the lack of adequate authorities to employ CNO through conventional channels; JSOC, on the other hand, operated in a more permissive environment.

[271] Monteiro, interview.

[272] Minnick, interview.

[273] Monteiro, interview.

[274] Warner, "Notes on Doctrine."

What FM 3-13 did do, however, was push discussion of computer network operations into an open, unclassified setting. At the joint level, computer network operations were not specifically articulated as one of the five core components of IO until the updated release of JP 3-13 in 2006.[275] Absent sound doctrinal guidance, the signals intelligence community developed their own understanding of CNO as simply another form of SIGINT.[276] As such, it was expected to deliver in the same way that SIGINT delivered during the heyday of the global war on terror: by providing an increased understanding of how threat actors were using the internet to perpetrate violence.[277]

The Army's extensive involvement in the global war on terror provided an additional challenge to the early growth of Det Meade. The high demand for SIGINT support during the wars in Iraq and Afghanistan made the dozens of skilled detachment personnel a tempting target for brigade leaders who wanted to augment the unit's SIGINT production.[278] These temptations were exacerbated by the detachment's lack of demonstrable operational output. The popularity and perceived utility of Det Meade would therefore ebb and flow according to the predilections of rotating brigade and battalion leadership. Whereas one command team might see potential value in the unit and consequently attempted to grow and normalize it, the next would think it useless and try to end the experiment entirely.[279] During these early years, there were a number of conversations over whether the unit should keep its unique personnel management system or come more in line with that of the regular Army, with the former enabling longer soldier tenure and the latter more able to facilitate conventional deployments and better interactions with the regular Army.

---

[275] Warner, "Notes on Doctrine."

[276] Much of what we call "cyber" today or "CNO" in the 2000s was long classified by the SIGINT community as "Digital Network Intelligence," or DNI. This contrasted with DNR, the analogue counterpart.

[277] Jen Easterly, telephonic interview with the author, Nov 6, 2018.

[278] Bennett, interview.

[279] Lisa Bennett's efforts to develop an ASI and bring the unit into the open were followed by a commander who wanted to shut the unit down.

Consistent personnel turmoil combined with confusion over the role of computer network operations made it difficult for the detachment to generate a demand signal for CNO capabilities, and likewise made it difficult to envision what those capabilities should look like in order to provide maximum benefit. Much of the detachment's early methods of computer network attack were indistinguishable from active SIGINT, electronic warfare, or close range electronic attack.[280] Without any marketable capability to speak of or justification as to why that capability should be treated differently, and with a personnel management structure that made it difficult to integrate with conventional military units, Det Meade began to develop a reputation as a high talent organization that nevertheless struggled to make substantive warfighting contributions.[281]

In part to rectify this dysfunction, a number of the detachment's early key leaders tried to push for better talent management and a more normalized force. The push for an additional skill identifier (ASI) for computer network operations soldiers that began in 2003 culminated with the declaration of the D6 ASI for enlisted personnel and the E4 ASI to identify officer CNO planners.[282] In the absence of a coherent vision for what Army cyber should be, and without much capability to drive the creation of such a vision, the detachment also began to invest heavily in NSA work centers to build key relationships and to keep cyber-savvy soldiers gainfully employed.[283] This strategy of inter-agency investment helped to build relationships and cultivate a deep bench of skill, but the pseudo-reliance it created inhibited the pursuit of an independent conceptual framework for Army cyberspace operations.

---

[280] Minnick, Monteiro, interviews.

[281] Easterly, Minnick, interviews.

[282] Lisa Bennett began the effort to establish a CNO ASI but ran into resistance from her brigade commander. The D6 ASI specifically referred to soldiers who had completed the Basic Digital Network Analyst (BDNA) course. Memorandum from GEN Petraues, 26 July 2008, discusses need for a CNO planner ASI in addition to the D6. Technically, the E4 ASI requires a minimum of 12 months of service in the Cyber Mission Force.

[283] Investment in Agency work centers: Minnick, interview. Integration under TAO: Bennett, interview.

Army Network Warfare Battalion and the 780th Military Intelligence Brigade

These years of languid growth for the intelligence community's cyberspace operations began to shift around 2005 in conjunction with the appointment of Lieutenant General Keith Alexander as director of the National Security Agency. In 2007, Detachment Meade was renamed the Army Network Warfare Detachment.[284] In 2008, this detachment became part of the Computer Network Operations Task Force. On 2 July, 2008, the CNO-TF became the Army Network Warfare Battalion (Provisional) (ANWB). The ANWB was redesignated as the 744th Military Intelligence Battalion in October 2009. On 1 December 2011, the 780th Military Intelligence Brigade (Cyber) was activated under INSCOM.[285] Shortly thereafter, the 744th became the 781st Military Intelligence Battalion, and the 782nd Military Intelligence Battalion was activated at Fort Gordon, Georgia. In a span of five years, the Army had gone from having a secretive, under-manned, and poorly understood computer network operations detachment to a full cyber brigade that contained the bulk of the Army's operational cyberspace activity. What explains this rapid growth?

First, while this dissertation is not intended to be a study of individuals, the role of Keith Alexander in building both the Army's and the nation's cyber apparatus cannot be overstated. As the director of INSCOM from 2001-2003, then-Major General Alexander drove the expansion of two organizations which would be critical to the Army's early involvement in CNO: the Information Dominance Center (IDC), which had previously been established under LIWA, and the Intelligence Operations Center (IOC).[286] The IOC contained a signals intelligence organization called the SIGINT Technical Development Activity (STDA), which provided SIGINT support to the NSA's computer

---

[284] "History," 780th Military Intelligence Brigade.

[285] "Army Cyber Chronology," no date, received from Scott Anderson via email. The brigade was originally going to be called the 1st Army Cyber Brigade, but then fell into line with the INSCOM unit naming series. All INSCOM units are intelligence units in the 100/500/700 series range. Since the 700 series are strategic assets, and INSCOM believed the cyber brigade would be a strategic asset, it was decided to call it the 780th MI Brigade. (Thompkins, interview).

[286] Thompkins, interview.

network operations efforts.[287] Alexander's efforts increased INSCOM support to computer network operations and planted the seeds for its future development in subordinate units. As the Army G2 from 2003-2005, Lieutenant General Alexander also influenced INSCOM's later decision to create a cyber battalion.[288]

The second factor that affected this rapid growth was the increasing demand signal for cyber effects in support of overseas counterinsurgency operations.[289] As enemy forces migrated from analogue to digital communication platforms, the need to follow their communications was accompanied by the realization that those communications could be actively manipulated. Thus, demand grew for not only cyber-savvy SIGINT soldiers who were proficient in this new form of digital network intelligence, but for a force and authority structure which would allow those soldiers to switch from Title 50 intelligence collection to Title 10 military effects. However, the fact that these nascent computer network operations were seen as an offshoot of traditional signals intelligence contributed to the difficulty of either envisioning or articulating what an independent cyberspace operational framework might look like.[290]

The final piece of the cyber puzzle, and the piece which most directly led to the cyber organizational structure of today, was the discovery of a substantial, DoD-wide network intrusion. Codenamed Buckshot Yankee, the intrusion affected classified military networks in the Central Command area of responsibility. Though the substantive effects of the intrusion were debatable,[291] both its fact and

---

[287] Thompkins, interview.

[288] Minnick, interview.

[289] Easterly, interview. David H. Petraeus, Memorandum from Headquarters: Multi-National Force-Iraq to the Vice Chief of Staff, United States Army, "Computer Network Operations," July 26, 2008.

[290] The creation of Joint Forces Component Command-Network Warfare (JFCC-NW) in 2005 was intended to serve as a partial solution to this problem. Services were expected to support JFCC-NW through service information warfare centers — though there was little rhyme or reason as to how these centers were built, who served in them, or how they operated. The JFCC-NW years were very much a time of "winging it" as the joint services and the intelligence community attempted to figure out how joint cyberspace operations were going to work. Through JFCC-NW, the NSA effectively split its pursuit of CNO operations into two components: the Title 50 support to strategic intelligence collection through TAO, and the Title 10 support to military operations through the JFCC-NW and affiliated service operations centers. (Easterly, Thompkins, interviews; Michael Lanham, interview with the author, October 30, 2018).

[291] Lanham, interview.

its scope created the sense that the DoD did not have an adequate method for tackling cyber defense.[292] In 2008, Defense Secretary Bob Gates directed the director of the NSA, Lieutenant General Alexander to take operational control of cyber defense in addition to the cyber offense that he already oversaw through JFCC-NW and TAO.[293] This consolidation directive was the foundation for what would later become Cyber Command. It also invigorated the cyber efforts of each military service in anticipation of a future need to provide expanded service support to the joint cyber command. The rapid growth of Detachment Meade into the 780th occurred in partial response to these joint level demand signals.

However, this growth period was not without its challenges. For one, it exacerbated the growing divide between SIGINT, represented by Army Cryptologic Operations (ACO) within the INSCOM G3, and cyber over whether cyber actually represented anything new.[294] ACO believed then, and still believes today, that cyber was simply SIGINT with a different name. As a result, they attempted to treat it like SIGINT in terms of operational practices, with an enforcement of heavy classification schemes and limited independent experimental authority. In contrast, those who had been engaged in the field of computer network operations throughout the early and mid-2000s, and who were thus less beholden to the influence of classic signals intelligence, were increasingly of the opinion that cyber was something different, and as such deserved its own rules, authorities, personnel, and organizations.[295]

The squabble between SIGINT and cyber fit into a much larger discussion over who in the Army should own this new capability. Members of the intelligence community were adamant that cyber should remain where its most significant capabilities were first developed and where the vast majority of its most

---

[292] Alexander, interview.

[293] Ibid.

[294] See "Army Cryptologic Operations," U.S. INSCOM website, last updated May 2, 2019, https://www.inscom.army.mil/MSC/ACO.aspx, and Headquarters, Department of the Army, *Field Manual 2-0*, *Intelligence* (Washington D.C.: Headquarters, Department of the Army, March 2010), section 12-8.

[295] The ACO perspective came from McNeill, William and Wetzel, Thomas, interview with the author, Fort Meade, M.D., Sep 24, 2018. The cyber perspective came from Minnick, interview, and George G. Franz, email correspondence with the author, Aug 12, 2018.

skilled practitioners had originated.[296] Meanwhile, the signal corps argued that the cyber realm belonged to them, given their stated purpose of building and maintaining the Army's communication networks and the support they provided to intrusion detection, mitigation, and remediation through NETCOM.

Discussions of the potential for cyberspace effects led to involvement from the Army's Combined Arms Center, which saw cyber as a form of fires that naturally fell under their purview.[297] Information operations involvement stemmed from the fact that cyberspace owed much of its conceptual origins to early IO experimentation, as well as to 1st IO Command's near-total ownership of Army computer network defense efforts.[298] These disagreements were only partially resolved through the creation of Army Cyber Command in 2010, and were more fully resolved through Army Chief of Staff General Raymond Odierno's direction to create a cyber branch in 2014, both of which will be discussed in a later section.

PERSONNEL CHALLENGES

A second challenge the Army faced during this 2006-2010 period was where to find personnel for the mission. As with the early years of Det Meade, the Army still did not have a career path for soldiers with the right cyber skills, nor was there much of an idea of what those right skills were. Success in getting an enlisted ASI had improved Army-level visibility of cyber talent, but it had not resulted in improved personnel management practices. On the officer side, the expansion of the detachment into a more conventionally-styled unit had the effect of attracting increasingly conventional officer talent — in other words, the detachment began to attract officers who were raised within the SIGINT system, with all its attendant intellectual and operational influences. The opportunity to send the detachment unconventional officers who were capable of driving change in a new operational paradigm was overruled by the institutional need to get generic officers qualified for their next promotion. Thus, for an officer, service in

[296] Minnick, interview.

[297] Ibid.

[298] Moore, Portare, interview.

Det Meade became like service in any other organization: in which one's ability to serve in a managerial position was more important than the presence or absence of any specialized expertise.[299] The difficulty of attracting officers with the appropriate skill sets contributed to the detachment's struggle to develop a conceptual framework for cyberspace operations that was independent of the signals intelligence experience that animated more long-standing detachment leadership.

The rapid expansion of the cyber detachment also meant that an increasing number of soldiers would not have the career protection of the special management program that protected soldiers from conventional reassignment. Without the protection of this program, which was originally intended as a stop-gap measure and had only a limited number of billets, cyber soldiers were seen by the big Army as nothing more than highly qualified SIGINTers. The increasing demand for on-the-ground SIGINT support to the conflicts in Iraq and Afghanistan made it difficult to justify why these personnel should be allowed to stay at Fort Meade rather than deploy forward. The resultant cyclical loss of trained unit members only increased the difficulty of creating a coherent vision for what the Army's cyberspace capabilities should look like independent of the inclination to default to a SIGINT-based solution. It thus became increasingly clear that the Army would not be able to grow its cyber unit without a mechanism in place to retain cyber personnel. This mechanism eventually took the shape of the 35Q military occupation specialty in 2012 before it was decided that cyberspace would have its own career management field in 2014.

The question of where to get cyber soldiers was soon followed by the question of where to get the billets in which they would serve.[300] The push for growth of Det Meade and the creation of a cyber battalion had been largely internal to the intelligence community up to this point. In other words, it neither resulted from nor resulted in the type of large-scale force restructuring that would have allowed

[299] Monteiro, interview.

[300] Minnick, interview.

the Army to formally reallocate billets from one mission to another.[301] Thus, all billets for the Army Network Warfare Battalion would have to come out of hide from INSCOM at the potential expense of INSCOM's other intelligence missions. The lack of a dedicated organizational infrastructure in which to place the cyber mission is why the 704th had to sacrifice SIGINT billets in support of it, from the earliest days of Detachment Meade to the activation of the 780th Military Intelligence Brigade.[302] The sunk costs associated with the intelligence community's ongoing sacrifice of billets and personnel only increased their interest in not losing cyberspace to another branch.

The final hurdle in the cyber puzzle was training. What critical knowledge, skills, and abilities would so-called cyber soldiers need to have? What tasks and functions would they need to perform? As previously stated, much of the training that took place in the detachment's early years was through self-study. Courses were available intermittently through the NSA, but there was neither consistency in who attended nor reliability in when they were offered. The push for a sustainable training program was due in large part to the arrival of Lieutenant General Alexander as the DIRNSA in 2005. General Alexander had been cultivating a vision for cyberspace operations over his time in service, and his background in the Army gave him a vested interest in ensuring that the Army would be well-prepared for whenever this vision came to materialize. When the 704th received a new brigade commander in 2006, intimations that there would be an increased demand for the CNO mission led to a new initiative to establish a sustainable recruitment and training model to identify qualified soldiers within the brigade.[303] Soldiers who had computer skills were identified and set aside for future work in the CNO detachment. These prospective personnel were screened according to their knowledge of several technical content areas: proficiency in

[301] After the Army's decision to create a cyber branch, some of this force restructuring took place through the deactivation of Long Range Surveillance and Pathfinder companies.

[302] Thompkins, interview.

[303] Minnick, interview.

Windows and Linux; networking; information assurance; penetration testing; and system hardware and architecture.[304] Those who passed the screening were then recruited into the detachment.

The soldiers then followed a loose training program that was a mix of NSA-affiliated courses, external vendor courses, and the Navy's digital network analysis courses for which the Army got around eight slots per year. The detachment's primary source of operational experience came from its investment in NSA work centers, which meant that soldiers would have to pass high NSA technical standards in order to become gainfully employed. This loose training program did not provide the competence necessary to interview with the agency, so the 704th MI brigade's S3-Network Warfare (S3-NW) shop contracted its own training program through the University of Maryland Baltimore County (UMBC).[305] The detachment sent eight to ten soldiers at a time through a twelve to thirteen week block of training, which was followed by assessments to determine placement by workrole.[306] The unit also began to get officers on temporary assignment through the Junior Officers Career Cryptologic Program (JOCCP), as well as analytic augmentation from a reserve information operations unit located in New England.[307]

Concurrent to the Army's internal effort to figure out how to train its cyber soldiers, the National Security Agency formed a CNO working group to determine what roles at the national level would be defined as CNO.[308] This agency's effort to more carefully define CNO was part of a larger paradigm shift that had been years in the making, as the primary methods of communication moved from radio to cellular to digital. While the NSA had a number of people working with computers already, there was no standard training pipeline to get into the agency from any of the individual services. The working group was an effort to both discipline the NSA's internal approach to CNO and to help standardize the

---

[304] Minnick, interview. Internal brigade recruiting efforts resulted in the identification of perhaps 20 qualified personnel in a 1600 person brigade.

[305] Ibid. This partnership provided the core skills necessary for soldiers to embed with the NSA (malware triage, packet analysis, penetration testing, etc.) and was augmented by additional outside training as necessary.

[306] Ibid. All activity was focused on Title 50 at this point, and all through the NSA's Signals Intelligence Directorate.

[307] Ibid. Officers only had 2-3 year rotations before they were gone; reserve soldiers provided analytic support

[308] Ibid.

procedure by which the services could provide workforce augmentation. They spent six months narrowing the field of CNO to thirteen total workroles, then another six months defining the specific skills and abilities required of each workrole.[309]

The services used these two lists — of workroles and abilities — as the basis for the creation of a joint course that would provide graduates with the majority of training necessary to fill these thirteen workroles. This effort, called the critical task advisory group (CTAG) sought to answer a question that had been plaguing the Army's cyber efforts for years: what is the standard baseline of training required in order to conduct CNO at the national level?[310] The fruits of the critical task advisory group led to the content for what would become, in the fall of 2010, the Joint Cyber Analysis and Attack Course (JCAC), which was the standard joint course for cyberspace operations.[311] All Army JCAC graduates were automatically routed to what eventually became the 780th Military Intelligence Brigade, thus helping to alleviate the talent problem in the short term. However, the Army would adopt a different approach to solve this problem in the long term.

SUMMARY: THE INFLUENCE OF SIGNALS INTELLIGENCE

Cyberspace operations emerged within the signals intelligence community in response to adversary migration from analogue to digital communications. While the structure of this response changed over time — from a small signals intelligence group that supported the NSA's information warfare directorate to an operational brigade — its initial character mimicked that of the National Security Agency upon whose authorities and expertise it relied: highly secretive, risk-averse, and compartmentalized. These characteristics persisted through a period of increased operational demand for

[309] Minnick, interview. The CNO working group was comprised of stakeholders from the agency and each of the five services.

[310] Ibid.

[311] JCAC replaced the DNA series of courses that the Navy would run. JCAC piloted fall 2010. Had attendees from each of four services. 24 week 3 day course to advise on curriculum etc. ensure getting the right content at the right level. JCAC now producing roughly a thousand people a year across the services. (Ibid).

cyberspace effects in support of the global war on terror, thus complicating efforts to effectively integrate into conventional Army operations or to satisfactorily meet the Army's needs.

As Detachment Meade began to expand in the early-2000s, an influx of officers with conventional intelligence backgrounds contributed to the widespread assumption that computer network operations were simply another form of signals intelligence. Absent a more expansive conceptual framework to guide the development and employment of cyberspace capabilities, what limited capabilities did exist often took the rather unremarkable form of active SIGINT or close range electronic attack. This CNO-as-SIGINT assumption, and the lack of either senior leader or staff officer momentum to challenge it, ultimately hampered the detachment's ability to innovate offensively. The erection of structural safeguards around the community's cyber talent — which allowed for the retention of a cadre of technically competent and intellectually innovative cyberspace personnel — combined with an increased awareness of the importance of cyberspace operations among Army senior leadership — which ultimately increased the appetite for innovative solutions — helped to liberate cyberspace both conceptually and operationally from its signals intelligence influence.

The Influence of Army Space

SPACE AND CYBER AT THE JOINT LEVEL

The organizational relationship between the space and cyber communities began on 1 December 1998, when the Department of Defense created Joint Task Force Computer Network Defense (JTF-CND) and assigned it to U.S. Space Command (SPACECOM).[312] On October 1, 2000, responsibility for computer network attack functionality was also moved from the Joint Staff into space command, and later

[312] JTF-CND evolved into JTF Computer Network Operations (JTF-CNO) by late 1999 to reflect its incorporation of computer network attack.

consolidated with computer network defense under a single operational headquarters within the Joint Task Force Computer Network Operations (JTF-CNO).[313]

The decision to place cyberspace capabilities under the purview of space command was due in part to a lack of viable alternatives, and in part to a natural synergy between cyber and space that was first recognized in the seminal planning document *Joint Vision 2010*. Written in 1996, Joint Vision 2010 described information superiority as the cornerstone of future warfare.[314] Since so much of the U.S. military's ability to transmit and receive information depended on space platforms, the ability to delay or deny information from space systems was seen as the basis for future information dominance.[315] The space community in general, and U.S. Army space officers in particular, emerged as integral to the conduct of successful information operations.[316]

The series of reorganizations which resulted in placing JTF-CNO into Space Command had repercussions for command and control of Army cyberspace operations. The most important of these repercussions was the designation of the Army service component for space operations, Army Space Command (ARSPACE), as the de facto higher headquarters for Army cyberspace activity.[317] ARSPACE worked with Space Command and the joint services to translate cyberspace needs and requirements into a

---

[313] "U.S. Cyber Command History," from U.S. Cyber Command webpage, accessed Oct 14, 2018, https://www.cybercom.mil/About/History/. In 2001, Space Command adopted the following mission statement for computer network operations: "JTF-CNO will, in conjunction with the CINCs, Services and Agencies, coordinate and direct the defense of DoD computer systems and networks; coordinate and, when directed, conduct computer network operations (less CNE) in support of CINCs and national objectives." The vision was to operationalize CND and CNA to be fully integrated with air, land, sea, and space across the full spectrum of conflict. JTF-CNO consisted of 101 military and civilian personnel billets. (Headquarters, U.S. Space Command, "USCINCSPACE Implementation Plan for Computer Network Warfare," Peterson Air Force Base, CO: Headquarters, U.S. Space Command, May 13, 2001).

[314] Joint Chiefs of Staff, *Joint Vision 2010*, 1996. Specifically, JV2010 describes a "system of systems [that] will integrate intelligence collection and assessment, command and control, weapon systems, and support elements. It will connect the commanders to the shooters and suppliers and make available the full range of information to both decision makers in the rear and the forces at the point of the spear." From William Cohen, "Report of the Quadrennial Defense Review," *Joint Forces Quarterly*, (Summer 1997), 11.

[315] Jeff Harley, "Space and Information Operations," *Army Space Journal*, 2002.

[316] FM 3-13 lists the Space Operations Officer as a member of the command IO cell, with duties that include: including IO requirements in the space operations appendix of the operations annex; coordinating IO requirements with US Army Space Command; coordinating with adversary targeting to include enemy space systems in the targeting process; supporting OPSEC and MILDEC by maintaining enemy space order of battle, to include monitoring orbital paths and satellite coverage areas. Harley, "Space and Information Operations," 38.

[317] ARSPACE was not an operational headquarters; instead, it served coordination and facilitation functions for the synchronization of Army cyberspace capability with joint cyberspace requirements.

request for capability, and then to see who within the Army had the capability to meet that requirement. Through its capacity as a coordinating headquarters, ARSPACE built a number of relationships with the various Army components that operated in cyberspace, namely INSCOM, NETCOM, and 1st IO, as well as the Army staff.[318] The nascent concepts of computer network attack that were developed by ARSPACE planners gradually affected the trajectory of INSCOM capability development.[319]

Following 9/11, a demand for space and information operations support in U.S. Central Command led to the creation of the joint Space and Information Operations Element (SIOE). The SIOE was a team of space and IO experts created to augment the CENTCOM space and IO staff for operations in Afghanistan and later Iraq.[320] Each service fed the SIOE through their component IO centers, which for the Army was the Land Information Warfare Activity and later the 1st IO Command.[321]

In 2002, the SPACECOM merger with U.S. Strategic Command (STRATCOM) gave STRATCOM responsibility for all military cyberspace activity.[322] The service components reorganized accordingly, and U.S. Army Space Command became Space and Missile Defense Command/Army Strategic Command (SMDC/ARSTRAT). In 2003, the Secretary of Defense tasked each service to stand up an element to conduct planning and capabilities development for computer network operations.[323] This task naturally fell to SMDC/ARSTRAT for the Army given its previous experience coordinating Army cyberspace activity. Concurrently, the SIOE transitioned into a larger organization called the Information Operations Task Force (IOTF). Comprised of 108 personnel and led by a brigadier

---

[318] Jeff Harley, telephonic interview with the author, Oct 26, 2018.

[319] Ibid.

[320] Randall L. White, "Command and Control Structures for Space and Information Operations in a Joint Command" (Masters Thesis, Air Command and Staff College, Air University, 2002), 12. Estimates place the team size at 65 people (Gray, interview).

[321] White, "Command and Control."

[322] "History," Stratcom.mil, accessed Oct 14, 2018, http://www.stratcom.mil/About/History/.

[323] Gray, interview.

general,[324] the IOTF was created to provide oversight to all IO activities within the DoD.[325] As a joint organization, the IOTF was supported by all military services, with an approximately 30/30/30/10 distribution of billets between the Army, Navy, Air Force, and Marines. The IOTF had a separate cyber division that was managed by the J39 joint staff planner for information operations. From 2003 to 2005, the IOTF provided direct support to over 100 different operations in CENTCOM.[326]

In 2005, STRATCOM was reorganized into a series of joint functional component commands. JTF-CNO — which in 2004 had been renamed JTF Global Network Operations (GNO) — became an exclusively defensive organization and was moved under the Defense Information Systems Agency (DISA). Concurrently, STRATCOM created the Joint Functional Component Command for Network Warfare (JFCC-NW) to handle all computer network attack under the authority and direction of the Director of the NSA.[327] Each of the services was directed to provide support to JFCC-NW.

SPACE AND CYBER IN THE ARMY

Throughout the creation of these joint cyber warfare organizations — SIOE, the IOTF, and JFCC-NW — the Army had two different organizations that engaged in computer network operations: LIWA/1st IO and Detachment Meade. Although possessed of an offensive conceptual orientation in its early years, LIWA evolved to focus primarily on the defense of friendly networks and the integration of joint and national capabilities through IO and CNO planners. Detachment Meade, meanwhile, conducted computer network exploitation in support of intelligence operations, with limited opportunity for offensive computer network attack due to restrictive authorities and insufficient capability

[324] Gray, interview.

[325] White, "Command and Control."

[326] Gray, interview.

[327] "U.S. Cyber Command History," U.S. Cyber Command.

development. Cross-talk between the two organizations was facilitated by the INSCOM G3IO, particularly in reference to the special access capabilities that existed within the 704th at the time.[328]

However, in spite of the existence of two separate Army organizations with cyberspace functionality, two problems confronted SMDC/ARSTRAT's ability to redirect cyber talent toward the aforementioned joint requirements: a lack of adequate personnel, and a lack of command support for redirecting these personnel from their existing missions. When ARSTRAT sent out a request for forces to support the IOTF in the early 2000s, Army headquarters identified exactly 18 personnel with the necessary training to fulfill the requirement. None of these people were considered taskable, however, because they were all working under Title 50 intelligence authority under the auspices of the National Security Agency.[329] SIGINT support to the global war on terror was an understandably high priority at the time, and INSCOM leadership did not want to redirect these personnel to something else that seemed of limited relevance to the tactical fight.[330]

Absent the ability to pull what limited talent existed within the active Army, the planners at ARSTRAT improvised by turning to the space community and the national guard. The Army's main cyber planner for JFCC-NW, for example, was not a cyber soldier but a space control officer who had a good enough understanding of network diagrams to conduct offensive cyber targeting. The bulk of the Army's cyber attack team consisted 14 members of the National Guard who were recruited on the basis of the tech jobs they held as civilians. ARSTRAT also developed their own cyber training program based off of the NSA's, and rewrote the code for a new tool suite. This team of part-time soldiers became the Army's first substantive contribution to JFCC-NW, and has since served as the organization's longest-running offensive cyber team.[331]

---

[328] Heath, interview.

[329] Gray, interview.

[330] Lisa Bennett, former 741st CDR, stated an ongoing desire to take the 200+ people in Det Meade and redirect them to the Army Cryptologic Office in support of Operations Iraqi and Enduring Freedom, but resisted the urge based on a suspicion that cyber was going to become something big.

[331] Gray, interview.

In 2008, Secretary of Defense Robert Gates directed the services to stand up service cyber commands. While the Secretary of Defense's order made it clear that the Army would have to create a new cyber command, what was not clear was where it would go or who should own it.[332] The Army designated SMDC/ARSTRAT as the interim headquarters for Army Cyber. The adoption of this "third hat" in addition to its responsibilities for space/missile defense and in support of U.S. Strategic Command was a reflection of two realities. First, that SMDC/ARSTRAT already had a relationship with existing STRATCOM, Army, and joint cyber machinery through its work in support of computer network operations over the previous decade. Second, and perhaps less evidently, that SMDC/ARSTRAT had earned a reputation as an honest broker by remaining outside the grind of beltway politics, and thus could transcend the increasingly vocal disagreements between the signal and intelligence communities over who should own the Army's cyber command.[333]

SMDC/ARSTRAT's designation as the official interim headquarters for the establishment of Army cyber entailed the creation of three separate organizations. The first was Headquarters, Army Forces Cyber Command (ARFORCYBER), a three-star headquarters that was administratively assigned to SMDC/ARSTRAT and served as the interim ASCC for U.S. Strategic Command. ARFORCYBER was responsible for command and control of global Army cyberspace operations. In fulfillment of this responsibility, the command had to maintain working relationships with the four separate headquarters that contained operational components of the cyberspace mission: INSCOM, NETCOM, 1st IO Command, and SMDC/ARSTRAT. ARFORCYBER reached initial operating capacity on 1 October 2009.[334]

---

[332] Gray, interview. The Army staff did not have a strong sense of urgency to fulfill this tasker.

[333] Both points came from Harley, interview.

[334] Anthony J. Naples, "Concept Plan: Establish Headquarters, Army Forces Cyber Command (ARFORCYBER) & Army Cyber Operations and Integration Center (ACOIC)," U.S. Army Space and Missile Defense Command/Army Forces Strategic Command, June 4, 2010.

In addition to ARFORCYBER, SMDC/ARSTRAT created the Army Cyber Operations and Integration Center (ACOIC), located in the INSCOM headquarters building at Fort Belvoir, Virginia.[335] The ACOIC was designed to direct, coordinate, integrate, and synchronize cyberspace operations; maintain a common operational picture of all Army networks; conduct cyberspace operations in support of full spectrum operations; and fulfill all planning functions that these activities required.[336] The final requirement was the creation of the Army cyber proponent. The proponent was responsible for the administrative requirements of standing up a new command, to include issues of doctrine, organization, training, material, leadership and education, personnel, and facilities.

SUMMARY: THE INFLUENCE OF ARMY SPACE

In total, Army Space Command and SMDC/ARSTRAT spent a decade as the higher headquarters for Army cyberspace operations, a relationship which ended upon the activation of Army Cyber Command on 1 October 2010.[337] Given this long tenure, how did the space community impact the development of Army cyber, and what elements of space culture proved most salient in this relationship?

The demands of Operations Iraqi and Enduring Freedom lent an operational focus and an added sense of on-the-ground urgency to the conduct of Army space operations throughout the 2000s. Army space command liaisons were embedded in combatant commands down to corps level, which gave the otherwise strategically-oriented command a level of tactical awareness that the Air Force's space command understandably lacked. This deliberate exposure of space personnel to ground operations fed how the Army thought about space support, and it fed how the Army would later think about computer

[335] The ACOIC's footprint later became the basis for Army Cyber Command headquarters (Gray, interview).

[336] "Concept Plan."

[337] John M. McHugh, General Order No. 2010-26, "Establishment of the United States Army Cyber Command," Headquarters, Department of the Army, October 1, 2010.

network and information operations. The result was a less risk averse, more agile, and more tactically-focused organization than what would otherwise be expected for a space headquarters.[338]

However, while the Army space community maintained a stronger tactical focus than its Air Force corollary, it still remained beholden to certain requirements of space culture writ large. This was especially true with regards to classification and compartmentalization. The necessarily high classifications and compartmentalizations that surround space operations created additional operational demands that went above and beyond what the SIGINT community required, and went far beyond what cyber-savvy SIGINTers believed was necessary for cyberspace innovation.[339]

For the first several years of its cyberspace mission ownership, ARSPACE, and later SMDC/ARSTRAT, persisted in doing things according to the norms of their community despite pushback from leadership in the Army's operational cyberspace organizations.[340] The resultant tension between the two communities contributed to the SIGINT reluctance to cede personnel to space command's cyberspace missions, which — due to their operation at the joint level in support of strategic requirements — were seen as too far removed to support Army warfighting needs.[341] Thus, while SMDC/ARSTRAT provided an important managerial function for the integration of Army cyberspace capability at the joint level, the highly classified and compartmented nature of space culture in the Army challenged initial efforts to effectively develop or employ cyberspace capability beyond the joint strategic environment. Tensions between the space and SIGINT communities over mission prioritization further exacerbated these challenges.

---

[338] Gray, Harley, interviews.

[339] Monteiro, interview.

[340] Ibid.

[341] Ibid.

The Influence of the Signal Corps

One of ARFORCYBER's main preoccupations as an interim headquarters was to plan for the creation of a more permanent organizational solution to the question of who should own Army cyber. This planning and analysis culminated in the presentation of four courses of action to the Army Chief of Staff: (1) give the command to SMDC/ARSTRAT as a third hat (2) give the command to INSCOM (3) give it to NETCOM (4) or create something new.[342] INSCOM and NETCOM both lobbied hard to adopt the cyber mission as their own, knowing that it would come with command elevation from 2 to 3 stars and a significant increase in funding.[343]

The two commands also had an operational justification for their lobbying efforts. At the time, defense comprised the bulk of the cyberspace mission even while offense earned the most attention. This fact gave the signaleers of NETCOM the opportunity to lobby for a mission over which they already had sway through their ownership of Army networks and their support to the Army CERTs. The signal community also reasoned that their intimate knowledge of the Army's network terrain made them eminently qualified to defend those networks, in the same way that a maneuver commander would never cede defense of his area of operations to the commander of another battlespace.[344]

The problem with this argument, however was that network defense was never the cultural or operational priority for signal branch. Culturally, signaleers are administrative service providers whose sole concern is that their networks are functioning properly and the data resident on them is readily available.[345] Signaleers' exist to ensure that the commander can talk — they do not conduct operations of their own, they are not innovative technologists, and they have little incentive to understand the nature of external network threats so long as the network itself is on line. While signaleers certainly possessed the

[342] Thompkins, Gray, interviews.

[343] Gray, interview.

[344] John A. Davis, telephonic interview with the author, Nov 29, 2018.

[345] Carmine Cicalese, telephonic interview with the author, Oct 18, 2018. Giovanni, interview.

technical aptitude, and in many cases possessed the technical expertise, to conduct network defense — recall their substantial involvement in the defensive portions of both LIWA and 1st IO Command's computer network operations efforts — their cultural predisposition as service providers was such that effective defensive measures were often seen as a hindrance to what they considered the more important mission of ensuring that the network was available and accessible.[346] In other words, the community's cultural proclivities were shaped by the operational reality that network defense and network maintenance are two different tasks that can have competing sets of priorities. These proclivities persisted despite mounting evidence that cyberspace attacks would negatively effect network functionality, and in spite of a clearly increasing demand signal that the practice of network maintenance would need to incorporate aspects of network defense.

The debate over the distinction between network maintenance and defense was ultimately a question of where cyber ended and signal began. From a resourcing perspective, the signal community had a vested interest in maintaining a clear distinction between these two activities: the farther cyberspace encroached into the tactical signal community, the more likely it was that signal billets would be lost to a future cyber branch over which it was not guaranteed that they would have any direct control.[347] Thus, while the signal community may have nominally supported the Army's network defense activities, they did not do so from the type of holistic, threat-centric operational perspective that had grown to define the Army and the joint vision for the future of cyberspace.[348]

It was not until the creation of Cyber Command in 2010, and the later Cyber Protection Brigade in 2014, that signal branch began to take steps toward a more holistic defensive strategy, first through the creation of the 255S information protection technician career field, and second through the rotation of

---

[346] Observation by MG (R) John Davis, former J3 of JTF-GNO, which had the defensive mission and worked heavily with DISA. Reinforced by LTC Matt Giovanni, a signal officer and former 2nd BN 1st IO S3.

[347] Harley, interview.

[348] Chavez, Gray, Bennett, interviews.

these 255S warrant officers into cyber command assignments.[349] Exposure to the integrated operations of cyber command — where intelligence, defense, offense, and law enforcement functions all mutually supported one another — helped shift the signal perspective into a more threat-centric, operational mindset.[350] Signal branch followed these efforts with the creation of the 25D network defender MOS in 2014, comprised of enlisted personnel who were exclusively trained in the tools of network defense as opposed to network maintenance or administration.

In contrast, INSCOM's argument stemmed from their historical ownership of the computer network operations mission through both the 704th Military Intelligence Brigade and LIWA. The SIGINT community had the resources, the expertise, and over a decade of computer network operations experience that other communities did not. However, an INSCOM takeover of the complete cyber mission would inevitably have required them to take over NETCOM as well — something that the INSCOM commander desired but which the signal community did not. Furthermore, there was an expectation that the compartmentalized nature of the intelligence community would negatively affect its approach to cyberspace, as happened during the Det Meade years in a way that inhibited cyber mission growth. While the intelligence community had a more operational mindset than its signal counterparts, fear of a continuation of intelligence tribal politics ultimately trumped whatever operational suitability for cyberspace the branch may otherwise have had.

Meanwhile, ARSTRAT did not have a preference either way: it was already a three-star command that had few delusions about expanding its own prestige through the addition of another mission set.[351] The information operations community also played a small role in these discussions based on their historical role in cyberspace through LIWA and 1st IO, but the lack of a general officer champion

---

[349] Abel Chavez, telephonic interview with the author, Sep 13, 2018. Chavez was the first 255S to rotate into USCC in 2011.

[350] Ibid.

[351] Harley, interview.

combined with ongoing doctrinal confusion over the definition and role of IO softened the community's voice.[352]

SUMMARY: THE INFLUENCE OF THE SIGNAL CORPS

The signal community helped to shape cyberspace development through its early involvement in network defense within LIWA and 1st IO Command. The community's role as network maintainers, and the technological skills required therein, lent them a natural claim to the computer network defense mission during the early years of cyberspace experimentation and discovery. This claim resulted in a preponderance of signal personnel on the Army ACERTs, on LIWA and 1st IO vulnerability assessment teams, and in the later cyber missions of 1st IO's 2nd Battalion.

However, as a more coherent theory of cyberspace operations began to develop, it became clear that the signal community's predisposition to focus on network accessibility and availability rather than on network security, combined with a mentality of service provision rather than operations, was less ideally suited to the defensive cyberspace mission than it was originally assumed. While possessed of the requisite technical skill to perform network defense, the signal community perspective was such that the network defense mission was not seen as wholly necessary. This cultural incompatibility was first made evident in the internecine squabbles between NETCOM and the ACERTs over the implementation of recommended network remediation strategies from the late 1990s into the 2000s, and came to a head during later discussions over who should own the new Army Cyber Command. The fact that the signal community was unable to adapt to the operational realities of cyberspace ultimately contributed to the Army's decision to place the command elsewhere.

[352] This point was reinforced through multiple interviews with IO personnel.

Table 2. Army Cyberspace Organizations, 1995-2019

Unit	Year Formed	Purpose	Subordinate To
Land Information Warfare Activity	1995	Provide IW/C2W operational support to land component and separate Army commands, active and reserve components, to facilitate planning and execution of IO.	Intelligence and Securities Command (INSCOM), with operational control under Army G3
B/742nd MI BN	1998	Develop an Army computer network operations force	704th MI Brigade
Detachment Meade, 742nd MI BN	2000	Expand the Army's computer network operations capability	704th MI Brigade
1st Information Operations Command	2002	Provide IO support through deployable support teams, reach back planning and analysis, resident and mobile IO and cyberspace training, and synchronization and conduct of CNO, in coordination with other stakeholders to integrate IO, reinforce forward IO capabilities, and defend cyberspace.	INSCOM/Army G3
Army Network Warfare Detachment	2007	Conduct computer network operations and signals intelligence	704th MI Brigade
Computer Network Operations Task Force	2008 (Jan)	Conduct computer network operations and signals intelligence	704th MI Brigade
Army Network Warfare Battalion (Provisional)	2008 (Jul)	Conduct computer network operations and signals intelligence	704th MI Brigade
ARFORCYBER	2009	Plans, coordinates, integrates, synchronizes, directs, and conducts network operations and defense of all Army networks; when directed, conducts cyberspace operations	SMDC/ARSTRAT, with operational control under USCYBERCOM
744th MI BN	2009	Conduct computer network operations and signals intelligence	704th MI Brigade
Army Cyber Command (ARCYBER)	2010	Integrates and conducts cyberspace operations, EW, and IO, to ensure freedom of action for friendly forces in and through the cyber domain and information environment while denying the same to our adversaries	HQDA
780th MI BDE	2011	Conducts SIGINT and cyberspace operations to create effects in and through the cyberspace domain to gain freedom of action while denying the same to our adversaries.	INSCOM, with operational control under ARCYBER
Cyber Protection Brigade	2014	Conduct cyberspace defense	ARCYBER
Cyber Warfare Support Battalion	2019	Provide expeditionary cyber support to maneuver units	ARCYBER
I2CEWS	2019	Provide cyber, space, and electronic warfare support to maneuver units	ARCYBER

The Development of an Independent Cyberspace Framework

CONCEPTUAL DEVELOPMENT

The intractability of these different perspectives on who should own the Army's Cyber Command was exacerbated by the fact that the Army did not have a unified central vision for what the future of cyber would need to look like.[353] Individual community perspectives — with intel pushing for full ownership based on its historic ties to the Title 50 computer network exploitation enterprise and signal pushing for the same thing based on its responsibility for the Army's networks — were thus not mediated or tempered by strategic direction from senior leadership. Add to that the lack of a sense of urgency among Army staff planners, and the result was a long process of community in-fighting that eventually culminated in the decision to give the new command to neither of the players who wanted it most.[354]

However, the Army's lack of strategic direction on the future of cyberspace operations did not correspond to a lack of critical thought or analysis. On the contrary, a number of publications released between 2007 and 2010 indicate that portions of the Army were hard at work trying to grapple with what cyberspace would mean for the future of land warfare. In August of 2007, TRADOC Pamphlet 525-7-6 *U.S. Army Concept Capability Plan for Electronic Warfare Operations 2015-2024,* identified the Army's lack of capability or organization in the field of electronic warfare as a crippling deficiency in the pursuit of information dominance across the electromagnetic spectrum.[355] A few months later, the Army released an updated version of its seminal operating document, FM 3-0 *Operations*, that reflected both post-Cold War modernization efforts and lessons learned from six years of war. The document heavily emphasized the importance of information and the information environment to future conflict, with a full chapter

---

[353] General Keith Alexander, impressed by what the Navy had done with its N2N6 merger (see chapter 4), wanted to merge the signal and MI branches into a new cyber branch, but as the NSA Director and CYBERCOM commander, he did not have much direct influence into Army structural conversations. (John "Buck" Surdu, telephonic interview with the author, Nov 28, 2018, and Jennifer Buckner, telephonic interview with the author, Dec 7, 2018).

[354] Gray, interview.

[355] U.S. Army Training and Doctrine Command, *TRADOC Pam 525-7-6: United States Army Concept Capability Plan for Army Electronic Warfare Operations for the Future Modular Force, 2015-2024*, U.S. Army Training and Doctrine Command, August 16, 2007.

dedicated to the idea of information superiority. This emphasis culminated in an expanded definition of the operational environment to include cyberspace:

> The operational environment will probably include areas not defined by geography, such as cyberspace. Computer network attacks will span borders and will be able to hit anywhere, anytime. With the exception of cyberspace, all operations will be conducted 'among the people' and outcomes will be measured in terms of effects on populations.[356]

Future Army forces would thus be expected to operate in complex terrain "and in cyberspace."[357] Cyber capabilities were described as a critical component of a nation's strategic reach, or the distance across which a nation can project its decisive military power.

However, in an indication of the doctrinal confusion that surrounded cyberspace across the entire joint force, as well as the identity crisis that had begun to infect the information operations community, the 2008 release of FM 3-0 could not disambiguate a strategy for cyberspace from the more general idea of "information engagement." The document listed computer network attack and exploitation as subtasks of command and control warfare, thus indicating a narrow application of cyberspace capability toward communication platforms rather than toward the ideas those platforms might contain or disseminate. In an indication of the ambiguous transformation of Army information operations, FM 3-0 also defined five separate information tasks which combine to form information superiority: information engagement, command and control warfare, information protection, operations security, and military deception.[358]

A series of pamphlets from Army Training and Doctrine Command called *Army 2020* offers additional insight into the conceptual development of the Army cyberspace operations from 2008-2010. TRADOC Pam 525-3-0, *The U.S. Army in Joint Operations*, published in December of 2009 and frequently referred to as the Army Capstone Concept (ACC), marked the beginning of a major revision to the

---

[356] Field Manual 3-0 (2008), 1-3.

[357] Ibid., 1-18.

[358] These tasks formerly comprised information operations; the retirement of the term in 2008 required the creation of the new term of information superiority.

Army's conceptual framework for future warfare. It argued that conflict in the information age would require an expansion of the concept of combined arms to include the information realm. The addition of the information environment as an added layer to the maneuver space meant that the future Army will require forces able to "fight and win on an emerging cyber-electromagnetic battleground."[359] In other words, no longer would forces have to simply contend with cyberspace as a component of their operating environment — now they must develop the ability to maneuver through that space in tandem with maneuver on land.

TRADOC Pam 525-3-1, *The Army Operating Concept for Operational Maneuver*, further developed this idea of combined cyber-physical maneuver in August of 2010. It explicitly mentioned the cyber-electromagnetic contest as a dimension of future conflict before going on to state that "military cyberspace operations employ a combined arms approach integrated across the war fighting functions."[360] In other words, cyberspace operations must be part and parcel of the Army's future operating construct, and not merely a supporting component.

Building upon these conceptual foundations, two documents published in 2010 provided additional detail as to what it might look like to have a cyber-capable Army force. The first, TRADOC Pam 525-7-8, the *Cyberspace Operations Concept Capability Plan* of February 2010, was a response to the fact that the Army did not have a holistic vision, concept, or doctrine to guide its capability development efforts in cyberspace. As opposed to previous publications which were largely theoretical, this document offered a practical take on how to integrate cyberspace operations into land warfare. It addressed how leaders must think about cyberspace operations, how they should integrate cyberspace into their overall operations, and which cyberspace capabilities will be needed. The publication further argued that the Army must make cyberspace and the EMS central and routine components to its operations in order to

---

[359] U.S. Army Training and Doctrine Command, *TRADOC Pam 525-3-0 The Army Capstone Concept. Operational Adaptability: Operating Under Conditions of Uncertainty and Complexity in an Era of Persistent Conflict, 2016-2028*, U.S. Army Training and Doctrine Command, December 21, 2009.

[360] U.S. Army Training and Doctrine Command, *TRADOC Pam 525-3-1 The United States Army Operating Concept, 2016-2028*, U.S. Army Training and Doctrine Command, August 19, 2010.

seize and maintain operational and tactical advantage against adaptive adversaries. While the terminology of this publication was never adopted, the spirit of its ideas can be seen in later doctrine.

The second influential document, the *Army Cyber/Electromagnetic Capabilities Based Assessment (C/EM CBA)* published in December 2010, provided the most explicit articulation to date of several years' worth of accumulated cyberspace thinking. The C/EM CBA was directed by the Army Chief of Staff and published by the Army Combined Arms Center (CAC), which at the time had proponency for both computer network operations and electronic warfare.[361] The CBA was inspired in part by the definitional challenges associated with the growing cyber and electromagnetic domains: namely, neither the proponent nor anyone else in the Army could satisfactorily delineate where electronic warfare ended and cyberspace began.[362] It was also inspired by the need to conclusively determine how the Army should be organized and manned to address the cyber-electromagnetic dimension of full spectrum operations, particularly in light of the impending establishment of U.S. Cyber Command.[363]

The C/EM CBA opened by stating that "the most prolific issue facing the Army today is the inability for Army forces to holistically include C/EM activities as an integrated part of FSO."[364] Building upon the previously developed expanded combined arms concept, the CBA stated unequivocally that the C/EM environment "must be thought of as maneuver space where positional advantage can be gained or lost."[365] The document argued that the natural technological convergence of cyber and electromagnetic activities would need to be matched by an operational convergence that integrates C/EM into all aspects

---

[361] Thompkins, interview. Every core function in the Army, from fires to intelligence, has a proponent. The proponent office provides guidance on what something is, on what it needs in order to properly function, and on what capability gaps currently inhibit the full realization of that function, from doctrine to equipment to type and size of unit. Until cyber gained a proponent office, it lacked both guidance on how it should develop or funding — hence its reliance on the ingenuity of individual organizations and extracurricular INSCOM funding. The C/EM CBA was CAC's effort to provide concrete guidance to the Army on what it would need in order to employ cyberspace and electronic warfare capability effectively. As such, it was a welcome departure from what to that point had been mostly theoretical speculation.

[362] Ibid.

[363] Martin E. Demspey, Memorandum for General Peter W. Chiarelli, "Posturing the Army for Cyber, EW, and IO as Dimensions of Full Spectrum Operations," October 16, 2009.

[364] Combined Arms Center, Capability Development Integration Directorate, "Army Cyber/Electromagnetic Contest Capabilities Based Assessment (C/EM CBA) Final Report," Fort Leavenworth, KS, March 30, 2011, 17.

[365] Ibid., EXSUM 1.

of Army operations. It also described how the Army's understanding of C/EM revolved around the primacy of network-enabled mission command to Army operations — maneuver forces must be able to communicate with each other reliably. Thus, the fundamental objective of the Army's C/EM contest was "to establish a network that enables effective mission command, then operate and defend it," a statement which hearkens back to previous doctrine on command and control warfare.[366] The number one recommendation to address the Army's C/EM discrepancies was the modification of doctrine "to internalize the C/EM contest from both an institutional and operational perspective" in order to "generate the necessary mindset within the force."[367]

As these discussions over how to organize for cyberspace took place, the Army was pursuing an equally important transformation in its information operations paradigm. This transformation made the concept of information operations increasingly irrelevant to the cyberspace discussion. Influenced by the conflicts in Iraq and Afghanistan, and in particular the sub-par quality of IO support received therein, a number of senior Army leaders began to push a paradigm shift in the Army's treatment of the information environment by the mid-2000s. This shift culminated with the release of FM 3-0 in 2008, which replaced the term "information operations" in the doctrinal lexicon with the idea of "information engagement."[368] Information operations as an integrating concept disappeared, and the five core capabilities which once comprised it were disaggregated into independent fiefdoms now free to secure resources and power on their own.[369] The arrival of the electronic warfare branch in 2012 helped to fill the staff integration gap left by an increasingly marginalized IO community, as the new brigade EW

---

[366] C/EM CBA Final Report., EXSUM 2.

[367] Ibid., 8.

[368] Information engagement would eventually be transformed into "inform and influence activities" by the time of the next release of FM 3-13 in 2013. The Army Combined Arms Center tried to release this updated version of FM 3-13 in 2008/2009, but the release was stymied by widespread opposition from both the IO communities and Army field commanders (this fact was mentioned in the "Posturing the Army for Cyber, EW, and IO" memorandum by General Martin E. Dempsey, as well as in several interviews with former IO personnel).

[369] Dominique, interview. Dominique served as the Army IO proponent from 2009-2011.

planner position assumed responsibility for cyber and electronic warfare integration that had previously fallen to the IO planner.[370]

A 2009 memo released by then-TRADOC commander General Martin Dempsey illuminates much of the thought process behind these definitional transformations.[371] Dempsey's memo summarized the findings of a series of CAC-led working groups that met in the summer of 2009 to establish a conceptual framework for how the Army should be organized for cyber, electronic warfare, and information operations. Specifically, Dempsey recommended a shift in the vocabulary of the cyber-EW-IO concept. Dempsey outlined three dimensions of the future operating environment to guide that shift: the psychological contest of wills, which required an acute understanding of human behavior in order to influence key battlefield actors; a dimension of strategic engagement with actors beyond the battlefield in both peace and war; and the cyber-electromagnetic contest, which included computer and telecommunication networks.[372] Because each dimension was seen to operate under different rules of causal logic, each would require its own doctrine and subject matter experts. As relates to cyberspace specifically, Dempsey did not recommend the creation of a new career field, but a continued reliance on those fields that already exist to perform the offensive, defensive, and exploitative functions required of the cyber-electromagnetic spectrum. This recommendation affirmed the idea of separation between the cyber-electromagnetic dimension from the broader cognitive space of those who use it.

---

[370] Headquarters, Department of the Army, *Field Manual 3-36 Electronic Warfare* (Washington D.C.: Headquarters, Department of the Army, November 2012).

[371] Dempsey, Memorandum "Posturing the Army for Cyber, EW, and IO."

[372] Ibid.

Table 3. Cyberspace in Army Doctrine, 1996-2019

Publication	Date	Contribution
FM 100-6, Information Operations	1996	The first Army doctrine on information operations. Took a broader approach to the DoD's guidance on information warfare by defining IO as something which spans the full range of military operations from peace through global war. Defined Command and control warfare as the warfighting application of IW in military operations. C2W is comprised of OPSEC, MILDEC, PSYOP, EW, and physical destruction.
FM 3-0, Operations	2001	The first iteration of the Army's operations manual to contain a chapter on information superiority.
FM 3-13, Information Operations	2003	Introduces computer network operations as a component of information operations.
FM 3-0, Operations	2008	Contains the first mention of cyberspace in a doctrinal publication. Emphasizes the importance of information to operations. Discusses information engagement as the integrated employment of information capabilities.
FM 3-36, Electronic Warfare Operations	2009	Introduced as "a key element in the Army's ongoing effort to rebuild and modernize its EW capability." Moves the Army's EW strategy into cyberspace and the electromagnetic environment. Provides guidance on how the electromagnetic spectrum and the cyberspace environment can be used to gain an advantage.
FM 3-13, Inform and Influence Activities	2013	Replaced the concept of IO with "inform and influence." A short-lived publication that contributed to the erosion of IO community influence.
FM 3-36, Electronic Warfare	2012	No significant changes from 2009 version, though with increased emphasis on cyber-electromagnetic activities as a doctrinal construct in Army operations.
FM 3-38, Cyber and Electromagnetic Activities	2014	Recognized as an interim solution to the cyber doctrine problem, and considered the "first of its kind to integrate cyber and EW." Replaced FM 3-36.
FM 3-12, Cyberspace Operations	2017	The Army's first dedicated manual for cyberspace operations.

ORGANIZATIONAL DEVELOPMENT

Army Cyber Command

The ideas contained within the aforementioned publications suggest that the problem within the Army was not a lack of analysis, but disagreement as to how the conclusions from that analysis should be pursued. The Army took steps to solving some of this disagreement on 1 October 2010, when general order 2010-26 established Army Cyber Command as an independent three-star command.[373] This new command would be functionally independent of, but supported by, INSCOM and NETCOM.[374] The first two ARCYBER commanders were neither intelligence nor signal officers, but were deliberately selected from combat arms backgrounds with the expectation that they would be able to transcend the entrenched political feud between the signal and intelligence communities, and that they would thus be able to look at the problem from an untarnished perspective.[375] Lieutenant General Rhett Hernandez, the first ARCYBER commander, was a field artillery officer whose recent experience commanding Human Resources Command made him ideally suited to the task of building a new organization. He was succeeded by Lieutenant General Edward Cardon, an engineer and former Army division commander.

The creation of Army Cyber Command in 2010 led to a period of rapid change in Army cyberspace development. For the first time, the Army cyber community had the institutional momentum it needed to solve some of the more pressing challenges that past patchwork efforts had revealed. It also had its own three star champion that was independent of the parochial interests and cultural influences of the various subcommunities that had given birth to it. From the beginning, ARCYBER was intent on fulfilling the chief of staff's vision to operationalize the domain — to develop cyberspace as something wholly distinct from the supporting missions from which it arose. Cyberspace operations would thus need to develop as a synergistic, threat-focused blend of offense, defense, and intelligence.

---

[373] McHugh, General Order No. 2010-26.

[374] Thompkins, interview.

[375] John D. Branch, telephonic interview with the author, October 19, 2018.

However, while the creation of ARCYBER signaled a sea change in the Army's institutional emphasis on cyberspace, there remained a great deal of confusion over the command's role for the first several years of its existence. Unity of command posed an especially difficult challenge, given early uncertainty surrounding which units would actually belong to ARCYBER and what sort of command and control relationships the organization would exercise.[376] LTG Hernandez initially lobbied for ownership of all of INSCOM and NETCOM, a move which would have effectively subsumed the intelligence and signal communities underneath the cyber umbrella.[377] This desire for ownership was due as much to the convoluted cyber authorities structure as it was to the natural command impulse to control one's own troops. Because ARCYBER lacked operational authorities of its own, the Army's main operational cyberspace units had to remain tethered to other institutions: for example, the 780th MI Brigade remained an intelligence organization in INSCOM even after it assumed full responsibility for the Army's operational cyberspace missions.[378] While ARCYBER eventually gained total control over NETCOM and 1st IO, INSCOM remained independent.[379]

ARCYBER also assumed force modernization proponency for cyberspace shortly after its activation, making it one of two operational commands in the Army — along with SMDC/ARSTRAT — that had responsibility for both force modernization and doctrine.[380] The recommendation for ARCYBER to assume proponency came directly from the space community, which believed that highly specialized, highly technical fields were best suited to make their own decisions on resources, training, and doctrine.[381] As the proponent, ARCYBER launched a second capabilities-based assessment to replace the

---

[376] "Cicalese, interview. "U.S. Army Cyber Command, Brief History," Powerpoint briefing, no date.

[377] Cicalese, interview.

[378] Ibid.; author experience.

[379] John M. McHugh, Secretary of the Army Memorandum, "Army Directive 2011-03 (Change of Operational Control for 1st Information Operations Command (Land) and Direction for U.S. Army Cyber Command to Conduct the Information Operations Missions for the Army)," February 2, 2011. This memorandum established ARCYBER as the operational headquarters and INSCOM as the administrative headquarters of 1st IO.

[380] Thompkins, interview. Ordinarily, the Army would have split these two functions between operational commands and training and doctrine commands.

[381] Frank Gray, interview. Gray authored the recommendation for ARCYBER proponency and designed the proponent shop.

cyber and electronic warfare CBA that had been completed the year prior. This second CBA focused on cyberspace only, since ARCYBER at the time was uninterested in assuming responsibility for the electromagnetic spectrum or electronic warfare.[382] Completed in summer 2013, the ARCYBER CBA concluded that the Army was not optimally organized to conduct cyberspace operations and electronic warfare.[383] The CBA recommended a number of significant changes to Army doctrine, training, and personnel management practices that would come to transpire over the next several years.

The Cyber Center of Excellence

The Army responded to the training deficit in October of 2014 through the wholesale conversion and reorganization of the Signal Center of Excellence into the Cyber Center of Excellence (CCoE).[384] The cyber center would be subordinate to Training and Doctrine Command, and would become the force modernization proponent for all cyberspace, signal, and electronic warfare functions — thus taking the proponency mission away from ARCYBER. The CCoE was directed to develop adaptive solutions for the aforementioned disciplines while coordinating with the Intelligence center of excellence for institutional intelligence support to cyberspace operations.[385] The cyber center of excellence managed separate signal and cyber schools with their own chains of command, overseen by separate one-star commandants.[386] The latter focused on communication, network management, and information services, and the former focused on defensive and offensive cyberspace operations and electronic warfare. In addition to the standard priorities of education, training, and force management, the CCoE's initial priorities stipulated a

---

[382] Thompkins, Hunter, interviews.

[383] Army Cyber Command/2nd Army Leavenworth Support Element, "Army Cyberspace Operations Capabilities Based Assessment (Cyber CBA) Executive Summary," Fort Leavenworth, KS, July 1, 2013, 1.

[384] Headquarters, Department of the Army Execution Order 057-14, "HQDA EXORD 057-14 Cyber Center of Excellence (COE) Establishment," January 24, 2014.

[385] Stephen G. Fogarty, "Cyber Center of Excellence (Cyber CoE)," Powerpoint briefing, AFCEA TechNet, September 10, 2014, https://www.afcea.org/events/augusta/14/documents/FogertyAFCEAv10.pdf.

[386] "Cyber Center of Excellence (Provisional): Offsite #2," Powerpoint briefing, March 24, 2014.

need to increase support to tactical forces at echelons below corps, in an indication of the Army's propensity to ground new ideas and new capabilities in the realities of ground warfare.[387]

The initial shape and purpose of the cyber school was driven by a combination of joint, national, and Army-level documents: the classified Cyber Forces Concept of Operations and Employment (CFCOE), which was the guiding document for the new Cyber National Mission Force (CNMF); the Cyber CBA; and the Army Cyberspace Leader Development, Education, and Training (LDE&T) Assessment and Implementation Strategy, approved December 2013, which addressed gaps and shortfalls in Army-wide cyber training, leader development, and education.[388] The impact of these documents is visible in three ways. First, the initial training focus for the CCoE was clearly and explicitly the task of building soldiers to populate the Cyber Mission Force (CMF), rather than to build soldiers who would be able to support independent Army requirements. This resulted in a mindset that was joint by necessity. The Army modeled its training progression on the Cyber Command joint training pipeline, with the intent to receive eventual joint accreditation and to assume a leadership role in training the joint cyber force.[389]

Second, the joint, inter-agency, and inter-industry nature of cyber training, as well as the realistic forecasts of Army cyber capacity within the capabilities-based assessment, led the CCoE to prioritize the leveraging of industry and joint partners in its training approach. The CCoE's stated goal was not the unilateral execution of all training requirements, but to provide management and oversight of federated training offered by distributed stakeholders — a model that stands in contrast to traditional Army way of doing business.[390] Third, the LDE&T assessment, as well as the repeated mantra that cyberspace was "commander's business," resulted in an Army-wide push to incorporate cyber training into all levels of

---

[387] "Cyber Center of Excellence (Provisional): Offsite #2," Powerpoint briefing, March 24, 2014.

[388] Ibid., slide 20.

[389] Ibid., slide 48.

[390] Ibid., slide 47.

professional military education. The effectiveness of this training has been subject to debate, but it represented an early effort to normalize cyberspace operations across the broader force.[391]

Third, the CCoE's vision for itself suggests the extent to which leadership understood that succeeding in cyberspace would require a culture shift within the Army. Notes from a 3 February 2014 off-site planning conference explicitly state that the CCoE "must embrace a culture shift in the Army" as part of its effort to be the "first choice" in all things cyber within the Department of Defense, across industry, and across academia — the latter two being particularly ambitious goals considering that most cyber expertise resides within industry and academia.[392]

Early documents also emphasized a need to "stay strategic," to think in terms of the joint force, and to look at things through the lens of a "combined arms approach."[393] These documents suggest that, while cyber had its origins within both the signal and intelligence communities, and while its most urgent requirements manifested themselves in the build of the cyber mission forces, Army leadership during the early phases of the CCoE intentionally sought to think beyond these original parameters in order to hypothesize what a post-CNMF future might look like.[394]

While the creation of the CCoE satisfied the need for a cyberspace training and doctrine headquarters, feedback from initial CCoE staff suggested that its close relationship with the signal community provided counterproductive cultural influences that ultimately hindered the center's early growth. These challenges ranged from the acquisition of classified workspace and workstations to encouragement of an operational mindset in the center's approach to soldier development.[395]

---

[391] For example, the Army's Command and General Staff College, which trains majors for field grade assignments, currently has only one day of instruction on cyberspace operations out of a year long course.

[392] "Cyber Center of Excellence (Provisional): Offsite #2."

[393] Ibid., slide 46.

[394] "Cyber Center of Excellence (Provisional): Offsite #2." The Cyber CoE CG stated "We need to develop a short and concise mission statement for the Cyber CoE. The new TRADOC CG likes Google's mission statement, 'To organize the world's information and make it universally accessible and useful.' The Cyber CoE's mission statement should be similar to Google's mission statement."

[395] Bennett, interview.

DOCTRINE DEVELOPMENT

The Army responded to the challenges outlined by the CBA with the creation of Field Manual 3-12, *Cyberspace Operations*. Initial work on the manual began shortly after ARCYBER became the cyber proponent, though the final draft was not published until roughly six years later.[396] Responsibility for the publication's development shifted to the Army's Signal Center of Excellence in early 2014 after General Odierno directed the wholesale conversion of the Signal Center to the Cyber Center, with subsequent responsibility for signal, electronic warfare, and cyberspace operations.

The multi-year process of creating FM 3-12 involved the input of over thirty five different organizations ranging from SMDC/ARSTRAT to Army Forces Command.[397] The process was also influenced by a number of older formal and informal publications, to include previous iterations of electronic warfare and information operations doctrine, previous concepts of computer network operations, concepts of employment for the incipient national mission force, and the ARCYBER CBA. Fundamentally, the publication sought to answer two questions: how should the Army fight in cyberspace, and how concepts of cyberspace should apply to traditional questions of how the Army operates as a force. Writers applied Army foundational doctrine on mission command, operations, and targeting to different aspects of cyberspace operations and electronic warfare to determine how the physical and virtual realms could seamlessly integrate.[398]

The most substantial debate, and the most significant pushback, centered around two issues. First was the question of how to treat electronic warfare. The question of where electronic warfare ended and cyberspace began was what prompted the analysis behind the first CBA, which began in 2008 and was completed in 2010. While that document advocated for the operational convergence of cyberspace and

---

[396] Hunter, interview.

[397] Ibid.

[398] Ibid.

electronic warfare based upon their technological convergence in the electromagnetic spectrum, the conclusions from it were largely ignored by an ARCYBER that remained uninterested in taking responsibility for electronic warfare. ARCYBER's own CBA released in 2013 focused on cyberspace operations explicitly, to the point where the command was reluctant to approve the inclusion of electronic warfare in the new FM 3-12 even as a subordinate component of cyberspace operations. ARCYBER's perspective was that electronic warfare operations should be treated as separate and distinct from cyberspace operations, regardless of what technological overlap the two realms might share. The final release of FM 3-12 included electronic warfare as a related but subordinate function to cyberspace operations.[399]

A second major point of disagreement concerned the concept of key terrain. The maneuver community especially pushed back on the notion that terrain in cyberspace could receive the same sense of doctrinal importance as an actual physical landmass. This community maintained the need for a distinction between physical key terrain, such as a hilltop or road junction, and so-called cyber key terrain, such as a router or server, regardless of how important that piece of cyber terrain might be to an overall operation.[400] This largely semantic debate proved less intractable than the debate over the status of electronic warfare. The final version of FM 3-12 was released on April 1st, 2017.

The deficit of institutional knowledge of what cyberspace was or how to integrate it into Army operations lent the manual a more instructional tone than what usually characterizes Army doctrine. As such, FM 3-12 contained more than just fundamental principles and definitions; it contained a number of

---

[399] Hunter, interview. It is worth noting that others disagreed with the inclusion of EW not based on disagreement with the operational principle, but due to the absence of a proper 2-3 year DOTMLPF assessment of what structural changes such a move would necessitate. Normally, significant changes in doctrine follow a multi-year process of change in organizations, training, personnel, and equipment. These changes had not taken place by the time the doctrine was being written.

[400] The lead doctrine writer for this publication stated that it took 3-4 weeks and a 4-5 hour online discussion to arrive at a consensus on the wording of the following paragraph: "1-75. In the context of traditional land operations, *key terrain* is any locality, or area, the seizure or retention of which affords a marked advantage to either combatant (JP 2-01.3). However, cyberspace operations uses the concept of key terrain as a model to identify key aspects of the cyberspace domain. Identified key terrain in cyberspace is subject to actions the controlling combatant (whether friendly, enemy, or adversary) deems advantageous such as defending, exploiting, and attacking. References to key terrain correspond to nodes, links, processes, or assets in cyberspace, whether part of the physical, logical, or cyber-persona layer. The marked advantage of key terrain in cyberspace may be for intelligence, to support network connectivity, a priority for defense, or to enable a key function or capability." From Field Manual 3-12, 1 April 2017, chapter 1, page 1-18.

prescriptive techniques for how units should approach cyberspace. For example, FM 3-12 drove the creation of a cyber and electromagnetic activities (CEMA) section in doctrine before such a section existed on Army unit staffs.[401] This sequence was backwards, but considered necessary at the time, since the majority of Army units did not know how to organize or how to task their electronic warfare personnel. Ultimately, FM 3-12 was published with the understanding that it was only a fifty to sixty percent doctrinal solution that left many topics unaddressed, but that even an unfinished document was necessary to aid in the education of the total Army force.[402]

FROM PERIPHERY TO CORE: CYBER SUPPORT TO CORPS AND BELOW

In 2014, General Odierno directed Army Cyber Command to assess the feasibility of integrating cyberspace operations into conventional maneuver at the tactical level.[403] Called Cyber and Electromagnetic Activities (CEMA) Support to Corps and Below (CSCB), the resultant initiative sought to determine three things: whether cyberspace operations could be useful to brigade combat teams; what balance of capability and expertise would need to reside at that level for successful cyber integration; and how the force would need to change to adapt to warfare in the digital age. Without billets to dedicate to tactical cyberspace operations, ARCYBER turned toward a small, piece of its 780th MI Brigade to execute the mission.[404] In late 2014, the 780th began the first of a series of sequential partnerships with conventional brigade combat teams (BCTs) by sending a team of expeditionary cyber operators to the

[401] Hunter, interview. The CEMA section of FM 3-12 differed from the CEMA cell described in FM 3-38, the Army's previous manual on cyber and electronic warfare. A cell is an informal portion of a unit that a commander can create out of any organic assets, whereas a section is a formal portion of a unit that a commander must create.

[402] Ibid. FM 3-12 excluded information on non-organic cyberspace capability, national-level cyberspace organizations like the CNMF, discussion on Army cyberspace organizations outside of the brigade level, and a proper explanation of the interaction between defensive and DODIN operations in cybersecurity.

[403] At a 2013 Senior Leader Seminar, General Odierno stated that "We have to focus on tactical cyber and EW capabilities immediately…we need to determine how do we use cyber capabilities at the tactical level." From "Tactical Offensive Cyberspace Operations in Army 2020," Powerpoint briefing, April 10, 2013.

[404] Author experience as commander of the executing unit.

25th Infantry Division in Hawaii.[405] Through this and subsequent efforts, CSCB would come to play a significant role in influencing how the broader maneuver Army would come to embrace cyberspace.

At the time the initiative was announced, and through a substantial portion of its execution, there was no Army doctrine on cyberspace operations at any level. Furthermore, the Army did not possess expeditionary cyber capabilities that would be relevant or useful to a maneuver brigade; brigade combat teams lacked the necessary staff knowledge to facilitate the proper integration of cyberspace into their planning; and the Combat Training Centers (CTCs) that served as the initiative's testing grounds were wary of allowing a new and poorly understood capability onto their closely guarded turf.[406] The cyber personnel assigned to the pilot thus had to create a conceptual integration framework for the inclusion of cyber at the tactical level, teach this framework to the maneuver community, gain buy-in from leadership at the CTCs and the approval to expand their training networks, rewrite portions of the training scenarios to allow for a realistic cyber component, and concurrently build a set of expeditionary capabilities without the proper acquisitions channels to buy them or research and development money to fund them.[407]

The bulk of CSCB concept and capability testing took place at the Army's Combat Training Centers in Fort Polk, Louisiana, and Fort Irwin, California.[408] The CTCs demonstrated varying levels of initial receptivity to the pilot. The Joint Readiness Training Center (JRTC) at Fort Polk proved initially less willing to invite cyber capabilities into its training rotations, due in part to a culture that revolved around the technology-averse light infantry community, and in part to a poorly developed network infrastructure that required a substantial amount of effort to improve. NTC was more receptive: the armor community

---

[405] Author experience as commander of the executing unit.

[406] Ibid.

[407] The lack of resources for capability development was an acute problem. One capability for the first NTC rotation of the pilot was built by lieutenants on their personal laptops on weekends.

[408] CTCs are massive collective training environments that serve the purpose of certifying the proficiency of Army brigades. They are run by a two-star general, have a dedicated battalion of opposition force, and an enormous supporting staff that handles everything from scenario scripting to observation and coaching of all echelons of brigade leadership. To give an understanding of scale, the training environment at the National Training Center (NTC) at Fort Irwin, California, is the size of Rhode Island. The training centers certify ten BCTs per year. A CTC rotation is the culminating event of a brigade's training cycle, and must be successfully executed prior to every deployment.

around which NTC was built has been historically more open to technological developments than its light infantry counterpart, and the network infrastructure within the training facility was more robust.[409] Over time — encouraged by reports of Russian electronic warfare from the Ukraine and small battlefield drones from Syria — both came to embrace the initiative.

The Army has conducted numerous CSCB rotations since General Odierno's initial directive. Several lessons learned from these rotations are worth further discussion.[410] First, because cyberspace is inseparable from either the electromagnetic spectrum or the broader information space it touches, the Army's embrace of CSCB has resulted in a resurrection of the oft-neglected capabilities of electronic warfare and information operations at the tactical level. The Army's decision to combine electronic warfare, information operations, and cyber into the functional category of information dominance — an arrangement inspired by the need to more coherently situate cyberspace operations within the Army's broader warfighting concept — has thus lent the historically marginalized functions of EW and IO a degree of tactical staying power that they could not otherwise gain on their own. In an indication of the service's commitment to expanding the availability of these resources to maneuver units, the pilot resulted in the creation of two new expeditionary cyberspace organizations, with substantial funding allocated for their capability development: a 171-person Cyber Warfare Support Battalion to provide dedicated expeditionary electronic warfare and cyber capability for the conventional force, and a 191-person Intelligence, Information, Cyber, Electronic Warfare, and Space (I2CEWS) Detachment, both of which were activated in early 2019.[411]

---

[409] Author experience as commander of the executing unit.

[410] Wayne Sanders, "Expectations Management of Cyberspace Effects at the Tactical Level," white paper. Lessons learned also taken from the author's own experience with the first three CSCB rotations 2015-2016.

[411] Department of the Army Memorandum, "Addendum 1 to Army Structure (ARSTRUC) Memorandum 2020-2024, Dated 08 December 2017," April 3, 2018. See also Caleb Minor, "New Space, Cyber Battalion Activates at JBLM," Army.mil, January 16, 2019, https://www.army.mil/article/216236/new_space_cyber_battalion_activates_at_jblm; and Mark Pomerleau, "The Army is Willing to Spend Big to Support the Cyber Mission," Fifth Domain, April 3, 2019, https://www.fifthdomain.com/dod/army/2019/04/03/the-army-is-willing-to-spend-big-to-support-the-cyber-mission/?fbclid=IwAR2vA-ptNrJEK0W8H7VeO47OkOI8i50wNflWg-gj1ZZWXvkb_6PxEHX1RYg.

A second lesson concerned the insufficiency of Army professional military education in developing cyber expertise across the broader force. On most rotations, the BCT's first exposure to the idea of cyberspace operations came with the arrival of a cyber team six months prior to their CTC rotation.[412] For roughly the first four months of each partnership, the cyber planner's job was less to plan the integration of capabilities and effects than to educate the staffs on the fundamentals of cyberspace, while the expeditionary cyber soldiers conducted numerous capability demonstrations for the infantry platoons to which they would be attached.[413] The single most important element of a successful CSCB rotation, as measured by the brigade's receptivity to cyberspace operations, was the early education of maneuver staffs and the effective socialization of a cyber understanding within them — not the actual execution of battlefield capabilities.[414]

Third, CSCB offered an indication of how the Army might prefer to manage the cyberspace leadership-technical balance. Officers selected as the face of the CSCB mission — those who would primarily interface with brigade combat teams — were so chosen for their communication skills, their leadership ability, and their traditional Army credentials rather than for their strictly technical expertise. While they needed to possess enough technical expertise to lead technical soldiers and to integrate technical effects with conventional maneuver planning, these officers were ultimately successful because of their ability to speak cyber in a language that the maneuver community they supported were able to understand.[415] The Army's recognition of the importance of this cyber-maneuver interface has since been

---

[412] While the Army conceives of cyberspace as a maneuver domain, at the tactical level cyber effects provide a supporting role — albeit an important one — to actions in the physical world. Thus, without a proper understanding of the importance of the cyberspace domain, of the difficulty of maneuver operations in a contested EMS space, or of the nature of securing a population in a contested information environment, brigade staffs could be forgiven for relegating the cyber personnel to a forgotten corner of the staff tent.

[413] Author experience.

[414] Note the historical similarity between CSCB and the field support teams of LIWA — both concerned themselves primarily with training the Army how to think about a new domain and how to leverage new capability.

[415] Author experience.

reflected in its decision to push cyberspace and electronic warfare billets and capabilities to the brigade level, as well as its allocation of cyber slots for Ranger School.[416]

Finally, the results of the CSCB initiative reinforced the primacy of tactical maneuver to the Army's core identity. The Army originally built out its cyber enterprise in a way that was not optimized to deliver cyber effects at the tactical level. Its focus was strategic, and its operations could be comfortably conducted from largely stateside locations. The eventual expansion of this strategic cyber formation took place at the expense of conventional Army billets. Concurrent with this expansion, CSCB partially resulted from a realization that cyber would fail within the Army if it was not made relevant to the broader force.[417] It was an Army internal initiative that was executed without dedicated billets, without a dedicated staff, and without doctrine or capabilities — in other words, CSCB was executed in spite of broader DoD or Cyber Command guidance, not because of it.[418] CSCB's influence on the Army can be measured by the creation of new tactically-focused cyber units, the decision to embed cyber officers and capabilities within conventional maneuver unit staffs, and the decision to consolidate the cyber and electronic warfare branches.

SUMMARY: THE EMERGENCE OF AN INDEPENDENT CYBERSPACE FRAMEWORK

The development of an independent conceptual framework for cyberspace operations at the level of the institutional Army began in earnest with the publication of a series of TRADOC pamphlets from 2007 to 2010. While not doctrine, these pamphlets influenced the trajectory of discussion on cyberspace and the electromagnetic spectrum that had begun to appear at senior leader levels. These pamphlets also

---

[416] Shawn D. Bova, telephonic interview with the author, December 7, 2018.

[417] The Army eliminated its Pathfinder and Long Range Surveillance companies from 2015-2016 based on a gamble that technological surveillance would be an adequate replacement for human surveillance in future war. The decision was also motivated by the "zero-sum" build out of the cyber force, in which the Army had to build a cyber force without a net gain in personnel. I say "partially resulted" because CSCB was also driven by the observation of advanced Russian Electronic Warfare in Ukraine. See Alex Horton, "Army Looks to Deactivate Long-Range Surveillance Companies," *Stars and Stripes*, July 16, 2016.

[418] John "Buck" Surdu commented that the CMF construct originally stemmed from General Keith Alexander's desire to bring cyber to the tactical level, but the initial growth focused only strategic teams in order to gain buy in. The tactical teams never materialized.

demonstrated the beginnings of the type of strong strategic direction that was necessary to overcome entrenched subcultural influences that had been driving development to that point.

Concurrent to these discussions of an appropriate conceptual framework for cyberspace operations were discussions of an appropriate organizational framework. The question of how to structure Army cyberspace operations was marked by significant disagreement between the Army's most relevant involved communities — intelligence, signal, and information operations — over who was most appropriately suited to capability ownership. Ultimately, the ingrained cultural and operational proclivities of each community were deemed too strong to accommodate the cyberspace vision that had begun to emerge among Army senior leaders. In order for cyberspace to develop as a mature operational capability, it would need to achieve independence from the subcultural influences which had played the primary driving role in cyberspace development to that point.

Accordingly, the Army opted for the creation of a new three star cyber command, ARCYBER, rather than elevate either of the existing two star commands within the intelligence or signal communities. The first ARCYBER commander was neither military intelligence nor signal, but a field artilleryman whose selection was a deliberate and resounding affirmation of the service's desire to liberate cyberspace development from its previous subcultural constraints. The second ARCYBER commander was likewise chosen for his operational background as an engineer and former division commander. The creation of ARCYBER was followed by the conversion of the Army Signal Center of Excellence into the Cyber Center of Excellence, a move which satisfied the need for a dedicated training center but which nevertheless suffered from the lingering effects of signal community cultural influence. In 2017, the Army published its first doctrinal manual on cyberspace operations, FM 3-12.

The fusion of cyberspace operations into mainstream Army culture concluded with the Army CSCB pilot. CSCB arose in response to the question of what cyberspace could do for the Army. As such, it focused on the integration of cyberspace personnel and effects into tactical maneuver formations. The pilot resulted in the creation of new, tactically-focused cyberspace organizations; an expanded institutional

commitment to the fields of electronic warfare and information operations; and an expanded emphasis on shaping the Army's cyber force to be maximally relevant to the Army's dominant, combat arms culture. CSCB thus demonstrates the Army's total institutional commitment to the tactical force, even in the presence of a primarily strategic capability.[419]

The Influence of Electronic Warfare

The CSCB pilot and related organizations it inspired led to a structural and operational merger between the fields of cyberspace operations and electronic warfare. Given the now-cozy relationship between these two communities, why did electronic warfare not play a more significant role in influencing Army cyberspace development? The Army's inconsistent history with electronic warfare operations offers a clue.

HISTORY

The 1980s marked the last time the Army fielded dedicated electronic warfare capabilities.[420] These capabilities were housed in the Combat Electronic Warfare Intelligence (CEWI) battalions that emerged after a significant reorganization of the Army intelligence enterprise in 1977.[421] CEWIs possessed high power jammers designed to attack the command and control capabilities of Russians, East Germans, or North Koreans.[422] The placement of EW capabilities within the Army's combat intelligence

---

[419] Interestingly, CSCB also served as the fulfillment of the original vision for the World Class Cyber OPFOR. In further affirmation of this dissertation's main argument, the IO community proved incapable of bringing this vision to fruition due to internecine disagreements within 1st IO Command on who should contribute what to the new WCCO mission. (Giovanni, interview)

[420] The Army's first electronic warfare field manual, *Field Manual 34-10, Division Intelligence and Electronic Warfare Operations*, was published in November 1986.

[421] See Price, *History Vol III*, 291 for background on CEWIs.

[422] Price, *History Vol III*, 322, lists the following capabilities: MLQ-34 Tacjam for VHF and jamming. p. 359: TLQ-17A Traffic Jam ground deployed communications jammer and Quick Fix, helicopter deployed communications jammer; GTE Sylvania/ AEL MLQ-34 Tacjam VHF collection and jammer.

battalions reflected the naturally close relationship between signals collection and signals disruption at the tactical level. As one Army expert wrote:

> Jamming of the U.S. Army model is an integral part of, but is not subordinate to, intelligence. Intensive jamming can be used for brief periods on single channels, as before our attack, to knock out key enemy command and control nets. We also use jamming to screen friendly communication. […] This tactic prevents the enemy from intercepting the friendly communication; instead, he intercepts our jamming.[423]

However, the combined impact of three external events — Goldwater-Nichols, the collapse of the Soviet Union, and Desert Storm — led to a deliberate reduction in the Army's electronic warfare inventory throughout the 1990s.

The 1986 Goldwater-Nichols act made the most sweeping changes to the Department of Defense since the department was established in 1947.[424] Designed to fix problems caused by inter service rivalry,[425] specifically the services' inability and unwillingness to operate as a unified force, the act restructured the chain of command to improve the ability of military services to operate together more effectively in combat.[426] Specifically, the act elevated the position of the Chairman of the Joint Chiefs of Staff and made the combatant commands more independent.[427] As part of this restructuring, Goldwater-

---

[423] Price, *History Vol III*, 323

[424] U.S. Congress, Senate, Committee on the Armed Services, *Hearing to Receive Testimony on 30 Years of Goldwater-Nichols Reform*, November 10, 2015, Washington DC.

[425] Prior to Goldwater-Nichols, the U.S. military was organized along lines of command that reported to their respective service chiefs. This system led to counter-productive inter-service rivalry. Peacetime activities (such as procurement and creation of doctrine, etc.) were tailored for each service in isolation. Additionally, wartime activities of each service were largely planned, executed, and evaluated independently. These practices resulted in division of effort and an inability to profit from economies of scale, and inhibited the development of modern warfare doctrine. The formulation of the AirLand Battle doctrine in the late 1970s and early 1980s laid bare the difficulty of coordinating efforts among various service branches. AirLand Battle attempted to synthesize all of the capabilities of the service arms of the military into a single doctrine. The system envisioned ground, naval, air, and space based systems acting in concert to attack and defeat an opponent in depth. However, the structure of the armed forces effectively blocked the realization of this ideal. The US invasion of Grenada in 1983 further exposed the problems with the military command structure. Although the United States forces easily prevailed, its leaders expressed major concerns over both the inability of the different service branches to coordinate and communicate with each other, and the consequences of a lack of coordination if faced with a more threatening foe.

[426] Goldwater-Nichols had nine objectives: "strengthen civilian authority, improve military advice, place clear responsibility on combatant commanders, ensure commensurate authority for the combatant commanders, increase attention to strategy and contingency planning, provide for more efficient use of resources, improve joint officer management, enhance the effectiveness of military operations, and improve DOD management." From "Hearing to Receive Testimony."

[427] Zimmerman, et al., *Movement and Maneuver*, 8.

Nichols dramatically changed the personnel management of military officers by requiring a joint assignment as a prerequisite for promotion to flag rank. The act's emphasis on joint warfare thus changed not only how the services interacted systematically, but also the broader cultural framework in which those interactions took place. The overwhelming success of the U.S. military in Desert Storm — in which a joint force achieved large scale ground maneuver against a numerically strong enemy through a combined technological and informational advantage, commonly dubbed "network-centric warfare" — was largely seen to validate these Goldwater-Nichols reforms.[428]

Following Goldwater-Nichols, the collapse of the Soviet Union in 1991 led to significant reductions in military expenditure. These reductions forced each service to begin a process of rationalizations, mergers, and downsizing. The combination of budget cuts, the dissolution of the closest peer technological threat, and an increased reliance on the sister services facilitated by Goldwater-Nichols, led to a period of decline in Army electronic warfare. In order to eliminate resource redundancy across the services, the Navy became the joint proponent for electronic warfare, with the responsibility to provide support to all three services when and if needed.[429] As a result, Army electronic warfare capabilities quickly became secondary to their alternative purpose of direction finding and signals intelligence — a purpose which was much more relevant to the intelligence community that owned these systems, and more useful to the type of low-intensity fighting in which the Army found itself during the early 2000s.[430]

---

[428] Zimmerman, et al., *Movement and Maneuver*, 195.

[429] Price, *History Vol III*, 460.

[430] Background on EW taken from Laurie M. Buckhout, "Short History of U.S. Army Electronic Warfare," *SITREP Review of DoD Technology Advancements* (Q1 2016). The history of the Army's Prophet system provides a good example of SIGINT overtaking EW at the tactical level. Officially adopted in 1999, the Prophet was a tactical-level EW asset designed to provide a variety of capabilities to maneuver commanders, to include electronic signals mapping, electronic attack, navigation warfare, selected signals exploitation, and more precise techniques to assist in targeting. When the Army found itself in an environment of persistent counterinsurgency and low-intensity conflict against a technologically unsophisticated foe, the intelligence community which owned the Prophet system began to rely almost exclusively on the system's SIGINT function at the expense of its ability to engage in electronic attack. This habitual receive-only mode of operation eventually became standard operating procedure; when the rise of improvised explosive devices led to a need for increased electronic protection, turning toward the Navy and the Air Force for a solution was more expedient than relying upon the forgotten electronic attack capabilities within the Army's own intelligence community. Furthermore, the case of the Prophet System illustrates split tendencies between the MI and EW communities, with MI inclined to support national collection missions at the expense of the type of tactical use that EW favored. Information on the Prophet taken from "An/MLQ-40 Prophet," Globalsecurity.org, accessed March 12, 2018, https://www.globalsecurity.org/intell/systems/prophet.htm.

The subsequent rise of the internet and the increased threat it posed to national security further solidified the shift in focus from electronic warfare to SIGINT. While the Army aviation community maintained counter-radar capabilities for the suppression of enemy air defense (SEAD), electronic warfare had slipped entirely out of focus for the remainder of the Army. By the early 2000s, the Army had no equipment, no personnel, no updated doctrine, no units, no training, and no facilities dedicated to the conduct of electronic warfare.

The arrival of remote-controlled and electronically-detonated IEDs in Iraq in 2005 encouraged the Army to reconsider its relationship with electronic warfare. The deployment of thousands of CREW (Counter-RCIED) devices into theater — along with qualified EW personnel from the Air Force and Navy — led Army leaders to conclude that they needed to have a trained cadre of electronic warfare specialists and the equipment to fight on a contested electromagnetic spectrum.[431] The creation of the Army IED Task Force in 2005 was followed by a Vice Chief of Staff determination that the Army had to create its own electronic warfare standards, rather than rely on those of other services whose expertise in the sea and air domains did not directly correlate to success on the ground. Thus began a more strategic effort to create a genuine Army electronic warfare capability.[432]

An in-depth internal review of Army EW capabilities conducted in the mid-2000s came to numerous concerning conclusions.[433] First, the study highlighted the extent to which the Army was unprepared to face a serious electronic warfare threat. The Army's assumption of EMS superiority on the battlefield led to the development of C4ISR systems that were largely unprotected against jamming and other electronic techniques. This meant that not only did the Army rely upon vulnerable communications systems, but it also did not train to operate in an EMS-contested environment. Enlisted spectrum managers were the only service members who knew how to operate in the much more benign

---

[431] "Army Creates Electronic Warfare Career Field," Defense-Aerospace.com, February 6, 2009, http://www.defense-aerospace.com/articles-view/release/3/102144/us-army-re_establishes-electronic-warfare-career-field.html.

[432] Buckhout, "Short History."

[433] Ibid.

environment of EMS congestion, but they lacked the knowledge necessary to respond to a full-scale electronic threat. Second, the study highlighted the significant effort undertaken by American adversaries to develop their own EW capabilities. Russia, North Korea, and China were considered the most capable, with regiments comprised of thousands of EW troops and equipment able to degrade much of the equipment in Army programs of record on communications, situational awareness, and command and control.

In 2007, largely in response to this study, the Army Vice Chief of Staff ordered the Army to embrace electronic warfare as one of its core competencies. An internal requirements document identified 2,500 positions across the Army that would need specialized EW officers, warrants, and enlisted personnel. At the time, neither the MI nor Signal communities were willing to support this 2,500 person request, given that both were struggling to meet operational needs in Iraq and Afghanistan and neither wanted to allocate positions to what was seen as a tangential operational requirement.[434] Electronic warfare eventually found a home in the field artillery community as another option in a menu of lethal and non-lethal effects available within the Army targeting cycle.[435] The electronic warfare career field for officers, warrants, and enlisted was approved in February 2009, and established headquarters at the Army Fires Center of Excellence in Fort Sill, Oklahoma.[436]

Training for enlisted and warrants began in 2009, with officers following in 2011.[437] Electronic warfare colors and branch insignia were approved in 2012 to formally distinguish the field from field artillery. Of note, the initial course design for electronic warfare officer training included sections on

---

[434] James R. Armstrong, email correspondence with the author, March 13, 2018.

[435] While electronic warfare was housed with the Army fires community, it was funded through the Intelligence Directorate. Buckhout, "A Short History."

[436] See Jacqueline M. Hames, "Electronic Warfare - A New Way of Fighting," Army.mil, August 21, 2009, https://www.army.mil/article/26408/electronic_warfare_a_new_way_of_fighting.; "Electronic Warfare: Dominate the Electromagnetic Spectrum," Informational Brochure from United States Government Printing Office, http://usacac.army.mil/cac2/cew/repository/ElectronicWarfare_Brochure.pdf.; and "Army Creates Electronic Warfare Career Field," Aerospace.com, February 6, 2009, http://www.defense-aerospace.com/articles-view/release/3/102144/us-army-re_establishes-electronic-warfare-career-field.html.

[437] "Electronic Warfare: Dominate the Electromagnetic Spectrum."

cyberspace operations.[438] The intent, as far back as 2012, was to use the electronic warfare staff planner as a maneuver brigade's touchpoint into the cyber world at a time when there was no interest within the cyber community to drop either cyber authorities or capabilities to the tactical level.

In spite of its initial momentum, the Army's electronic warfare resurgence was short-lived: budget cuts in 2012 once again led to the decision to slash authorizations for EW personnel, such that the whole community never got over 1,100 members total.[439] With the creation of the cyber branch in 2014 and the ongoing convergence of the electromagnetic and digital spectrums, ownership of electronic warfare personnel, training, and capabilities logically shifted to the Army cyber branch, albeit tumultuously.[440] For example, the EW community was hit harder than any other branch or functional area by the officer separation board process in 2014, with twenty-six percent of eligible officers selected for separation compared to a twelve percent average separation rate overall.[441] Promotion rates within electronic warfare also lagged behind promotion rates for the broader Army.[442]

This brief history offers a few insights into how and why cyber developed as it did within the Army. First, both Army electronic warfare capabilities and cyberspace capabilities have expanded and contracted in response to direct battlefield threats or the lack thereof. Furthermore, the initial electronic warfare contraction in the early 1990s was hastened by its placement within an intelligence community that preferred to listen rather than attack. The perceived inferiority of Soviet electronic warfare

---

[438] FA29s were encouraged to attend cyber courses such as the Joint Network Attack Course and Army Cyberspace Operations Planners Course, and earn civilian certifications like Certified Ethical Hacking (Armstrong email).

[439] Given that many of the eventual EW staff officers were still in training when the Army had to decide how to react to federal budget cuts, it made more sense to simply cut these unfilled authorizations than to cut something that served a more immediate and tangible purpose to the operational force.

[440] See C/EM CBA, 2010, and ARCYBER CBA, for the origination of these concepts. Regarding the actual merger, see Amber Corrin and Mark Pomerleau, "Army Merging Electronic Warfare into New Cyber Directorate," C4ISRnet, July 12, 2016, https://www.c4isrnet.com/c2-comms/2016/07/12/army-merging-electronic-warfare-into-new-cyber-directorate/. Currently the training continues to take place at Sill, since they have superior facilities, with a long-term plan to shift to Fort Gordon.

[441] "Human Resources Command Briefing to General Odierno," Powerpoint briefing, July 10, 2014, slide 64. The next highest separation rate was public affairs at twenty-three percent.

[442] The FY14 promotion board to Major had a 33% selection rate; FY15 was 43%, FY17 was 77%. Armstrong, email.

capabilities in the 1980s led to a devaluation of electronic warfare at the expense of SIGINT, until EW capabilities effectively disappeared from the Army's inventory in the 1990s.

This disappearance happened concurrently with an increased awareness of the threat from computer network attack throughout the 1990s. Communication systems were becoming increasingly digital, driven by binary communication over wires rather than analog communication over radio waves. Realization of 1990s-era concepts of information warfare and command and control warfare was therefore seen to require an increased investment in computer network attack and defense, and a decreased investment in conventional methods of analogue communication and jamming. As computer network operations grew in scope and in frequency, their demonstrated ability to project power across great distances in the absence of war came to be seen as the more pressing strategic threat to U.S. defense than conventional electronic warfare methods, which could only be exercised from comparatively close range within the bounds of military conflict.

The convergence of the digital with the EMS a decade later — spurred by the proliferation of wireless networks — led to the natural merger of the cyber and electronic warfare career fields into a single cyber branch. This convergence was hastened by two organizational realities: the growing demand to apply cyber capabilities to the tactical Army, and the fact that the Army's existing cyber force did not have the manpower to fulfill this demand. The underused electronic warfare branch was seen as the solution to this personnel problem. Army leadership recognized that the cyber mission force, and Cyber Command writ large, was designed for national strategic requirements, and as such it would be of little assistance to conventional Army operations. Furthermore, the lack of capacity at joint levels meant that the Army would have to develop its own robust cyber and electronic warfare capabilities to retain information dominance on the modern battlefield. Bringing the electronic warfare population underneath the management of cyber branch was seen as a way to expand the Army's resources at the tactical level without detracting from its ability to support broader joint requirements.

CULTURAL CHALLENGES

Training for the electronic warfare specialists has been historically shorter than that of their cyber counterparts: electronic warfare officers receive 13 weeks of training, while enlisted receive 9 weeks of training. This stands in contrast to the 46 week training progression required of 17Cs, the Army's enlisted cyberspace operations specialists, and the 22 weeks required of 17A cyber officers. The short duration of these electronic warfare qualification courses was primarily due to two factors: first, that electronic warfare only accepted non-commissioned officers and senior lieutenants, and thus did not have to train brand new service members on foundational Army tasks; and second, that its instruction was limited to the physics of the electromagnetic spectrum and the mechanics of Army electronic warfare equipment.

These contrasting training models meant that the majority of electronic warfare personnel that were produced from 2012 to roughly 2017 were not technical experts.[443] They received very little education on the specifics of the electromagnetic spectrum and on the intricacies of maneuvering in and through the spectrum. The lack of technical expertise within the electronic warfare career field presented both operational and cultural challenges with the cyber-EW branch merger.[444] The branch has sought to overcome these challenges by attempting to standardize the initial officer training for both cyberspace and electronic warfare officers such that the two positions would be largely interchangeable, and by changing the electronic warfare officer function from a separate career field to an additional designation available to all 17As. The impending addition of electronic warfare platoons into each brigade combat team will further expand opportunities for both styles of cyberspace officer to serve at the tactical level.[445]

While one could argue that the Army's gradual reduction in electronic warfare emphasis and capability was primarily a rationalist reaction to the anticipated conditions of future war, it would be negligent to overlook the influence that SIGINT community preferences played in shaping the expectation

---

[443] Army Cyber Command DOTMLPF-P Assessment of CEMA Support to Corps and Below (CSCB).

[444] Armstrong, email.

[445] Bova, interview. Enlisted will retain a career field distinction between electronic warfare and cyberspace specialties. Both 17A cyberspace officers and 17B electronic warfare-qualified cyberspace officers will compete with one another for promotion.

of what those future conditions would look like. A brief mention of the trajectory of Russian electronic warfare can help illustrate the extent to which this is the case. Russian electronic warfare doctrine — more accurately translated into "electronic struggle" — does not maintain the same rigid distinction between electronic intelligence and electronic attack that exists in the U.S. model. Instead, the two are integrated into a system of complimentary rather than competing functionality.[446] This integration affords the Russian practice of electronic warfare a level of flexibility that is predicated upon the successful interplay of jamming with SIGINT at both the tactical and operational levels. In other words, the conceptual integration between intelligence and electronic warfare that exists within Russian electronic struggle doctrine has driven an operational integration that allows both collect and attack functions to peacefully and necessarily coexist.[447] This integration stands in contrast to the U.S. Army's bifurcation of intelligence and electronic warfare in both theory and in practice.

The tactical implications of this doctrine are evident in the Russian Army's heavy investment in electronic warfare capability. In contrast to the U.S., which keeps the preponderance of its electronic warfare capability in the Air Force and Navy, Russia's most powerful capabilities are found in the Army. Since 2008 every Russian combat brigade has been given its own electronic warfare company of an estimated 150 to 180 specialists equipped with jammers that reach out roughly 30 miles. The Russian Army contains an additional five independent electronic warfare brigades of 1,200 troops a piece. The Russian electronic warfare branch has its own general officers, with a two-star general as the branch chief. In contrast, prior to the joining of electronic warfare with cyber in the U.S. Army, the highest ranking American EW officer was a relatively inconsequential colonel. In further affirmation of the importance of electronic warfare to Russian operations, a 2016 article in the Russian general staff proposed elevating

[446] "Electronic struggle is presented as an interleaving of electronic intelligence and electronic warfare, rejecting a binary division in lieu of a more continuous concept that always uses elements of both." From Zach Young, "Cyber Report — Full Unified Draft with Footnotes," August 21, 2013.

[447] Young, "Cyber Report."

EW to its own combat arm.[448] Contrast this emphasis with the Army's distribution of EW personnel from 2012 to roughly 2018, in which each brigade had a single officer planner, and each maneuver battalion might have one enlisted liaison. The sole purpose of these staff personnel was to manage requests for Navy and Air Force jamming assets, and to reinforce proper procedures regarding mounted counter-IED systems. Until the cyber-inspired resurrection of tactical electronic warfare capability, the Army did not have any organic EW capabilities beyond these CREW systems.

SUMMARY: THE INFLUENCE OF ELECTRONIC WARFARE

The absence of an independent operational framework in which to house Army electronic warfare capabilities in the 1980s led to their placement within tactical military intelligence formations. This placement resulted in their subsequent neglect, and then disappearance, in favor of traditional signals intelligence collection throughout the 1990s and 2000s. Electronic warfare capabilities were resurrected by necessity in response to the RCIED threat in Iraq in the early 2000s, which was soon followed by a realization of the extent to which the Army was unprepared to operate in a contested EMS environment. The creation of an electronic warfare career management field to better institutionalize the expertise came soon thereafter, yet still a full decade after the Army's first cyber warfare organization.

However, these improvements in personnel management and capability investment were not matched by concurrent developments in the conceptual realm. The release of updated doctrine notwithstanding, the Army failed to make the proper institutional investment in electronic warfare as a fundamentally necessary capability, with the result that the brand new electronic warfare billets were the first to be eliminated following budget cuts in 2012.[449] While the electronic warfare career management field struggled to gain institutional traction with an incomplete force structure, uncertain career paths, decreasing positions due to force cuts, and too few billets at higher echelons, Army cyber saw an explosive

[448] Sydney J. Freedberg Jr., "Electronic Warfare Trumps Cyber for Deterring Russia," Breaking Defense, February 1, 2018, https://breakingdefense.com/2018/02/electronic-warfare-trumps-cyber-for-deterring-russia/.

[449] The Army released an updated version of *Field Manual 3-36, Electronic Warfare*, in 2012.

increase in resources, funding, and institutional support.[450] The result of these deficiencies were such that the Army electronic warfare community was not able to exert significant influence on the manner in which cyberspace operations developed. Instead, the community was absorbed into a newly independent cyberspace field that first was reluctant to embrace electronic warfare in any capacity, and later came to see electronic warfare as the tactical manifestation of cyberspace operations.

The early emergence of cyberspace expertise within the signals intelligence community in the early- to mid-2000s gave cyber the time and space to mature at precisely the moment that Army electronic warfare capabilities were being reborn. The lack of dedicated electronic warfare capabilities or a community of electronic warfare experts in the late 2000s, combined with the concurrent growth of computer network operations across the DoD and the rise of signals intelligence within the Army, contributed to the initial character of cyberspace operations as an intelligence-driven, risk-averse, and compartmentalized field.

Personnel Management Practices

The question of how to properly manage cyberspace personnel had been recognized at the level of the Army chief of staff as early as 2008.[451] At the time, the Army distinguished between five cyber skill categories that corresponded to emerging national cyber workforce roles: planner, engineer, operator, analyst, and developer. Each of these roles required different levels of technical expertise and would perform different offensive, defensive, and exploitative functions. Senior Army leaders considered five different courses of action for a future cyberspace career field.[452]

The first was a mid-career accession model that involved the creation of cyber-specific occupation specialties in the signal and military intelligence branches. Qualified soldiers would be able to transfer into

---

[450] Todd M. Boudreau, "Cyber CoE and Intel CoE Home on Home (HoH) Task Update: CF29 Infusion into Cyber Branch," Information paper, Fort Gordon, GA, January 12, 2016.

[451] "Cyberspace Career Field CSA Briefing, Draft, Pre-Decisional," Powerpoint briefing, August 12, 2008.

[452] Ibid.

the MOS after a few years in service, while officers would have the option of a cyber functional area. The second course of action was similar to the first, except the new MOSs would be open to entry-level soldiers. Third involved the creation of a new cyber branch that would subsume the entire signal corps, the entire future electronic warfare career field, and parts of the signals intelligence community. The fourth course of action relied upon warrant officers in a new cyber MOS to perform all of the Army's high-end computer network operations tasks. The final proposal entailed the development of additional skill identifiers for certain cyber skill sets, similar to the D6 digital network analyst ASI that already existed at the time, with no change to existing MOS structures. Decision-makers favored the ASI model due to its low cost, short time to implement, and minimal impact to other career management fields.

However, the 2009 recommendation to avoid the creation of a new cyber-electromagnetic career field contrasted with the increasing sense within the intelligence, signal, and computer science communities that cyber expertise could not be managed by ASIs alone. In the signal branch, this sense culminated in the creation of the 255S information protection technician warrant officer in 2010, followed by the 25D cyber network defender in 2014.[453] The intelligence community responded with the creation of the 35Q cryptologic cyberspace intelligence collector career field in 2012, which followed on the heels of the creation of two cyber-related additional skill identifiers in the late 2000s.[454]

THE WEST POINT EECS DEPARTMENT

Meanwhile, the Army's small community of computer scientists, represented by the United States Military Academy's Electrical Engineering and Computer Science (EECS) Department, had begun advocating for a separate cyber career field as early as 2002.[455] Comprised of academically trained

---

[453] David Vergun, "Cyber Network Defender MOS Now Open to NCOs," Army.mil, April 14, 2014, https://www.army.mil/article/123328/Cyber_Network_Defender_MOS_now_open_to_NCOs/.

[454] David Vergun, "Army Opens New Intelligence MOS," Army.mil, November 29, 2012, https://www.army.mil/article/92099/Army_opens_new_intelligence_MOS/.

[455] Gregory Conti, telephonic interview with the author, October 19, 2018. See also John Surdu and Gregory Conti, "Join the Cyber Corps: A Proposal for a Different Military Service."

computer scientists and electrical engineers, EECS culture came the closest to embodying the type of hacker spirit that cyberspace necessitated, untainted by any branch affiliation or affiliated predispositions. As an academic department, EECS had the additional freedom to think more broadly than its counterparts in the operational Army, whose efforts were often constrained by the operational, bureaucratic, and cultural influences that this chapter has discussed at length.[456] The conclusions derived from EECS thinking were also not subject to the restrictions of classification or compartmentalization which had hampered similar discussions in the intelligence community.

In 2000, the National Security Agency created the Center of Academic Excellence program as a way to leverage academia to address future security challenges, and West Point became one of the first affiliated programs.[457] As part of this affiliation, West Point received an embedded NSA employee, regular opportunities to send its cadets on NSA summer internships, and the ability to rely on NSA expertise in designing its computer science curriculum.[458] This NSA partnership led West Point to adopt a number of new cyber security initiatives, such as the creation of an academy-wide Cyber Defense Exercise (CDX) in 2001, the founding of a cadet cyber security club, more tailored course offerings in cyber security, and regular cadet and faculty attendance at hacker conferences and research events across the country.[459]

From 2000-2009, EECS used these resources to create a nucleus of officers who had more experience in computer science and cyber security than nearly anyone else in the Army. However, the department's efforts to train cyber-savvy officers were complicated by an Army that was not ready to absorb them. Structural issues prevented the Army from capitalizing on junior officers with relevant cyber expertise, since there was neither a central career field for these officers to enter nor any human resource mechanism to identify their unique skill set. As a result, EECS graduates scattered across the Army upon

---

[456] Conti, interview.

[457] Ibid. See also "Resources for Students and Educators: NSA Partners with Schools," NSA, accessed October 29, 2018, https://www.nsa.gov/resources/students-educators/.

[458] Conti, interview. Anywhere from 3-12 cadets would participate annually.

[459] Ibid.

commissioning to perform functions unrelated to their carefully cultivated undergraduate backgrounds.[460] The emergence of cyber-specific units such as the Army Network Warfare Battalion did not immediately change these structural deficiencies, since cyber assignments for officers were still considered to be deviations from a normal career path. Officers could rarely afford to hold these assignments for more than a few years before being shuffled along to the next critical benchmark for promotion in their primary field.

These structural problems reflected a broader cultural problem: the Army's institutional aversion to technical expertise, combined with its rigid adherence to hierarchy and preference for standardized, easily substitutable solutions did not naturally favor the development of a cyber-related career field.[461] An online survey conducted in 2009 suggested that, even if the Army were to create an independent cyber career field, potential recruits would still be deterred by certain infamous stereotypes of Army culture: inflexibility, compulsory management practices, anti-intellectualism, aversion to technical expertise, and a bias against non-combat personnel.[462]

The creation of Cyber Command in 2009, and the subsequent arrival of a four-star champion for Army cyberspace operations, led to a new revival of EECS theorizing about what a cyber career field might look like.[463] Personal recruiting visits from the commanders of both U.S. Cyber Command and Army Cyber Command reinforced the reputation of the EECS department as the epicenter of the Army's cyber expertise. As a reflection of this expertise, in October 2012, the Secretary of the Army directed the establishment of the U.S. Army Cyber Center at West Point. The center's purpose was to "serve as the Army's premier resource for strategic insight, advice, and exceptional subject matter

---

[460] Signal and Military Intelligence remained popular branches for cyber-savvy officers, as did the Information Systems Management (FA53), Telecommunication Systems Engineering (FA24), Information Operations (FA30), and Space Operations (FA40) functional areas.

[461] One former Army officer and cyber officer put it bluntly: "The immune system of the Army kills off cyber people."

[462] Conti, Easterly, "Recruiting, Development, and Retention of Cyber Warriors."

[463] Gregory J. Conti and John R. Surdu, "Army, Navy, Air Force, and Cyber — Is it Time for a Cyberwarfare Branch of the Military?" *IA Newsletter*, Vol 12 No 1. (Spring 2009): 14-18; Conti, Easterly "Recruiting, Development, and Retention of Cyber Warrior;" Greg Conti, John Nelson, Jacob Cox, and Jon Brickey, "The Case for Cyber," Small Wars Journal, 2012; Todd Arnold, Rob Harrison, and Gregory Conti, "Towards a Career Path in Cyberspace Operations for Army Officers," Small Wars Journal, August 18, 2014; Todd Arnold, Rob Harrison, and Gregory Conti, "Professionalizing the Army's Cyber Officer Force," *Army Cyber Center*, Vol 1337 No II (November 23, 2013).

expertise on cyberspace-related issues […] with a view to building the Army's cadre of cyber-qualified leaders."[464] It was further directed to "develop educational and training programs to foster the rigorous study of the intellectual underpinnings of cyberspace operations and to enhance the competencies of Army personnel in the cyber domain."[465] The center was later renamed the Army Cyber Institute (ACI).

Building off of this momentum, in 2012 several EECS department faculty began to experiment with what a cyber career path might look like. Unaware of whether the Army was actually considering such a move, the officers wrote a draft career progression and branch insignia. A few months later, when the Army announced the creation of cyber branch, the EECS officers' work became the foundational blueprint for the cyber career path.[466] When the cyber branch was finally created in 2014,[467] EECS faculty sent personal letters to the past thirteen years' worth of Cyber Defense Exercise participants to ask if they wanted to volunteer for a branch transfer.[468] Select EECS faculty later served as board members for the first cyber branch voluntary transfer board for officers. [469]

A NEW CYBER BRANCH

The decision to create a new cyber career management field was largely directed by then-Chief of Staff General Ray Odierno, who had grown impatient with the existing split-branch solution between military intelligence and signal.[470] The new cyber branch was intended to realize the chief's vision to

---

[464] John M. McHugh, Memorandum, "Establishment of the Army Cyber Center at West Point," October 19, 2012.

[465] Ibid.

[466] Conti, interview.

[467] John M. McHugh, General Order 2014-63, "Establishment of the United States Army Cyber Branch," August 21, 2014. This order established the Army Cyber Branch effective September 1, 2014.

[468] Conti, interview. Half had gotten out, another quarter were happy with their careers, and about a quarter volunteered.

[469] Ibid.

[470] Maureen O'Connor, interview with the author, September 28, 2018. General Odierno further stated that "Many of our adversaries lack the ability to confront our forces physically, choosing instead to employ virtual weapons with potentially devastating effect. We must take full advantage of these technologies, building our own capabilities to operate in cyber-space with the same level of skill and confidence we enjoy on the land. We will either adapt to this reality or risk ceding the advantage to future enemies." (From Todd Boudreau, "U.S. Army Cyber School Cyber Center of Excellence," Powerpoint briefing, Fort Gordon, GA, January 15, 2017.)

operationalize cyberspace through a single, independent career field that could lead, plan, and execute all facets of cyberspace operations.[471] While technical competence was seen as an important prerequisite for accessions into the branch, it could not come at the exclusion of an overall operational focus. It was understood that cyberspace personnel would have to understand how to employ cyberspace capabilities within the traditional Army operational framework of maneuver, fires, and effects, in order to make cyberspace relevant to the tactical customer.[472]

The branch was created by a panel comprised of subject matter experts from across the signal and intelligence communities.[473] The vision for the branch was far more holistic than anything that had yet emerged from within the respective supporting communities to that point, with a plan for creating different echelons of forces that were capable of supporting national, strategic, operational, and tactical requirements.[474] This holism reflected the effect of institutional Army influence in overcoming service subcultural lenses of interpretation. Furthermore, educating and integrating a cyber support cadre — to include intelligence, signal, and legal personnel — was considered as important to the development of institutional cyber expertise as was the creation of technically competent cyberspace operators themselves.

Cyber branch formed in several phases. The first phase focused on bringing in qualified officers beginning in late 2014.[475] Career paths for warrant officers and enlisted soldiers followed in October of 2015.[476] Following the creation of a core cadre of cyberspace experts, the second phase involved the

---

[471] "Army Cyber Career Field Implementation IPR to CAC CG," Powerpoint briefing, Fort Leavenworth, KS: Combined Arms Center, September 12, 2014.

[472] Ibid.

[473] Panel composition: Cyber CoE 15, Intel CoE 2, ARCYBER 5, INSCOM/780 9, NETCOM/CPB 11, HQDA/CIO G6 2, HRC 2, USMA 1, ACI 1, ARNG 6, USAR 2. (From Stephen Fogarty, "Cyber Career Field Implementation Plan (CMF 17 SME Panel & Way Ahead)," Powerpoint briefing, September 25, 2014).

[474] "Army Cyber Career Field Implementation."

[475] Of note, the first cyber second lieutenants were six members of the West Point class of 2014. Since the branch was not formally established until September, the six officers attended either the signal or military intelligence basic course before transferring into cyber branch later that year. The six lieutenants were products of the Electrical Engineering and Computer Science department's aforementioned cyber leader development program (CLDP). Information taken from "Army Cyber Career Field Implementation Plan."

[476] The initial stages of officer and enlisted accessions were open only to members of select occupations who were already fulfilling cyber-related jobs. Accessions were eventually opened up to all qualified applicants across the Army. "Warrant Officer Transition to CF170," Powerpoint briefing (no date).

wholesale conversion of 29-series electronic warfare personnel into the 17-series cyber branch.[477] The original vision for officer personnel development focused on recruiting those with a bachelor's or higher in one of electrical engineering, computer science, computer engineering, information technology, information assurance, or math.[478] However, while the number of available junior officers with these technical skills was substantial, the Army suffered from an initial deficit of technical aptitude at the higher ranks. Senior cyber officer branch applicants were thus more often selected for their coaching and mentorship skills, whereas junior officers became the branch's predominant technical experts.[479]

The Army cyber branch was initially comprised of three different MOSs: 17C cyber operations specialist, 17A cyberspace officer, and 170A cyber operations technician. Two more MOSs were added after cyber branch took control of the electronic warfare career field in 201X: 17B electronic warfare officer, and 170B electronic warfare technician. Enlisted personnel in the 17C MOS were trained with sufficient flexibility to perform up to eleven different workroles in support of either cyber offense or defense at the national level. Accessions into 17C began in June 2015.[480]

17Cs received 46 weeks of initial entry training split between the 25 week joint cyber analysis course (JCAC) run by the U.S. Navy in Pensacola, Florida, and 21 weeks of additional training at the Cyber Center of Excellence. The curriculum at JCAC offered a comprehensive introduction to cyberspace fundamentals, with instruction in discrete structures, programming fundamentals, computer organization and architecture, operating systems, networking concepts and protocols, Windows, Unix, programming, enterprise-level networking, protocol analysis, wireless technologies, target research/ SIGINT analysis, active exploitation, computer network defense (CND), and forensics methodologies and

---

[477] "Army Cyber Branch Offers Soldiers New Challenges, Opportunities," Army.mil, Fort Gordon Public Affairs Office, Nov 24, 2014, https://www.army.mil/article/138883/army_cyber_branch_offers_soldiers_new_challenges_opportunities.

[478] "Army Cyber Career Field Implementation Plan."

[479] Conti, interview.

[480] Army Career Field Implementation IPR to CAC CG, Powerpoint briefing, September 12, 2014.

malware analysis.[481] While JCAC provided a baseline competency in the vocabulary of cyberspace operations, its graduates were not considered fully trained cyber personnel. The soldiers, sailors, airmen, and marines who graduate from JCAC were thus required to complete a battery of additional training once they arrive at their units in order to become fully qualified in any particular workrole.

Additional training at Fort Gordon, meanwhile, was designed to prepare the enlisted soldier for success in performing eight of the fourteen work roles he or she might fulfill on a national team. The modules provided exposure to both the defensive and offensive perspectives, while maintaining and building upon the skills and knowledge the Soldiers had already gained through six months of JCAC. Soldiers focus on programming, scripting, Windows operating systems, Linux operating systems, networking fundamentals, security concepts, defensive methodologies, offensive analysis techniques, and generic Army warrior tasks.[482] Graduates of the two phase 17C training pipeline fill entry level positions on both offensive and defensive Cyber Mission Force teams, and are prepared for success in eight of the fourteen cyber workroles.

Warrant officers in cyber branch receive 19 weeks of basic training at the Cyber Center of Excellence. Approximately three of these weeks consists of common core training in basic principles of Army operations, to include leadership, the military decision-making process, and targeting. Warrants receive an additional 45 days of Cyber Common Technical Core training, 10 days of industry standard training, 10 days of the Army Cyber Operations Planner Course, three days on the Cyber Effects Request Form (CERF) process, and three weeks of instruction and application in the management of offensive and defensive cyber teams.[483]

There are two initial training paths available for 17A cyber officers. The first, Cyber BOLC, is a 37 week course for newly commissioned second lieutenants. The second, Cyber Operations Officer

---

[481] "Cyber School Course Overview," Powerpoint briefing, no date.

[482] Julianna Rodriguez, "Cyber Common Technical Core Methodology and Content," information paper, Fort Gordon, GA, August 10, 2016.

[483] Cyber Technical College, "Cyber School Course Descriptions," Fort Gordon, GA, September 15, 2016.

Course (COOC), is an introductory course for cyber reserve officers and those who transfer into the branch from another career field. Cyber BOLC is a 37 week sequence consisting of both branch-immaterial training in Army small-unit leadership and tactics as well as technical cyberspace operations training. Branch-immaterial topics include Army operations, intelligence preparation of the battlefield (IPB), military decision making process (MDMP), and targeting, in order to equip the officers with a basic understanding of the core operational process of the conventional Army. The technical phase provides specialized skills, doctrine, tactics, and techniques for defensive and offensive cyberspace operations. The course also features Certified Information Systems Security Professional (CISSP), Cisco Certified Network Associate (CCNA), Cyber Common Technical Core (CCTC), Army Cyberspace Operations Planners Course (ACOPC) and Joint Advanced Cyber Warfare Course (JACWC) training and culminates with an immersive, team-based capstone exercise.[484]

BOLC and COOC share several modules in common which serve to provide a shared technical foundation for all cyberspace officers. These modules include instruction in designing and maintaining network infrastructure; programming; a cyberspace operations planner course that teaches students how to apply standard Army decision-making protocol to cyberspace operations; the Joint Advanced Cyber Warfare Course; and a one-week unclassified module on defensive cyber protection operations. Graduates of both BOLC and COOC also receive industry-standard certifications as a Cisco Certified Network Associate (CCNA) and Certified Information Systems Security Professional (CISSP).

Cyber captains receive continuing professional education at the Captain's Career Course. This 22 week course consists of 15 weeks of common core material that is standard across all branches, plus seven weeks of technical training, research, and a culminating exercise. The course does not include any instruction on actual cyberspace operations — it is focused instead on general officer professionalization and conventional Army operations, from staff communications and the law of war to troop leading

[484] Cyber Technical College, "Cyber School Course Descriptions."

procedures and the principles of the offense. The three week technical portion of the program consists of industry standard coursework on network security, penetration testing, and forensics.

Where do these cyber officers come from? The Army commissions approximately 100 new cyber officer per year, with approximately twenty-five percent coming from the United States Military Academy, sixty percent from the Reserve Officer Training Corps, and fifteen percent from Officer Candidate school.[485] Branch applicants are assessed through an aptitude questionnaire and an in-person interview.[486] Cyber branch is the only branch in the Army that has these screening protocols, and it tends to attract the service's top intellectual and technical talent as a result. The questionnaire is designed by operational cyberspace officers and is intended to test applicant technical aptitude and knowledge. The nature of the questionnaire is such that the majority of cyberspace officers have a science and technology focused academic background.

CULTURAL CHALLENGES OF PERSONNEL MANAGEMENT

The creation of cyber branch highlighted a number of cultural challenges that the Army would need to resolve in order to move cyberspace from the periphery to the core of the service's consciousness. Foremost among these challenges was the tension between the requirements of the Army's traditional officer and enlisted roles and the unique technical demands of cyberspace. The institutional Army maintains a functional divide between its officers and its enlisted. Put simply, officers plan, direct, and lead while the enlisted execute.[487]

Army officers are also expected to lead soldiers from the earliest moments of their careers, when they assume control of a platoon and the responsibility for managing its capabilities on the battlefield.

---

[485] The exact annual breakdown since the branch began is as follows: in FY15 all candidates came from USMA. FY16 15/15/2 USMA/ROTC/OCS. FY17 15/31/7 USMA/ROTC/OCS. FY18 20/60/12 USMA/ROTC/OCS. FY19 25/56/18 USMA/ROTC/OCS 56 (Bova, interview).

[486] The questionnaire tests applicants on a broad range of topics, from programming to basic networking knowledge to electro-magnetic spectrum to RF fundamentals. (Bova, interview)

[487] The Navy maintains a similar distinction, but with stronger mechanisms of structural and cultural separation. In the Air Force, this divide is equally as rigid, but it extends in the opposite direction: the enlisted support the officers, while the officers go to war.

Leadership of fighting formations comprises the core of the Army officer's experience for the remainder of his career. Time spent away from a formation, such as time spent on staff, is considered the dues one must pay in order to get back to the line.[488] Army officers are further expected to be generalists, rather than specialists. The infantry officer, for example, must know the maximum effective distance of a 240B machine gun, but he is not expected to fire the weapon himself, nor to fix it if it stops working. He must intimately understand the fray of combat while staying above it, in order to better make decisions that will benefit the whole.

This distinction between enlisted and officers works when the jobs demanded of enlisted are task-based, relatively low skill, and can be learned in a short period of time. It begins to fall apart when these same jobs are high skill and demand a long period of training or education. The system works when the work demanded of officers involves directing the maneuver of formations of combat power. It falls apart when those formations disappear. Cyberspace challenges each of the premises that underpin the Army's traditional model of officer and enlisted differentiation: it is a domain that demands high-skill individual performance at all levels of execution, and it is a domain in which the same person who executes maneuver is often ideally suited to direct it.

Cyberspace is also a highly technical career field that requires years of study, primarily academic in nature, in order to build a baseline level of expertise. The cyber equivalent of a basic rifleman requires a minimum of two years of rigorous education before he is qualified to perform his function of digging a metaphorical foxhole and firing a metaphorical rifle. To extend the analogy further, this individual must not only understand how to fire his weapon, but also how to build it and all its variants from scratch, how to modify its function, and, in lieu of aiming at a visible target, how to calculate the individual ballistics of each round fired such that it impacts the target in the desired way — rounds which he is also expected to

[488] This leadership first model stands in contrast to the Air Force and Navy, where officers do not take command of formations until far later in their careers. These different leadership models had implications for how members of each service approached the management of CMF teams: the Army and Marine Corps would look at a 120 person team and say that's the size of a company, it should be commanded by a captain; the Air Force would look at a 120 person team and say that has the same number of people as a squadron, it should be commanded by a colonel. (Surdu, interview).

tailor make by hand. In the analogy described above, only officers with degrees in physics and mechanical engineering would be ideally suited to becoming basic infantry riflemen. What happens to the enlisted-officer divide under such circumstances? The Army's approach to its two most highly technical cyber workroles provides insight into the difficulties the Army has had in answering this question.

TECHNICAL WORKROLES

Interactive On-Net Operator

The first such workrole is the interactive on-net operator (ION).[489] Training for this workrole requires several months of instruction and practical assessment. IONs must pass the National Security Agency's Remote Interactive Operator Course (RIOT), which prepares students to operate under Title 50 authorities. The Army initially insisted on sending its enlisted soldiers to this training, since it is fundamentally a "doing" job — the digital equivalent of the infantry's trigger-pullers, albeit with more intellectual aptitude, more risk assumed, and less individual dispensability. Enlisted soldiers with the potential to succeed in the course were identified through a pre-course written assessment, which tested both technical aptitude and logical reasoning. Those who succeeded on the pre-course assessment were allowed to enroll in the training program.[490] However, few of the Army's enlisted soldiers have the training, experience, and aptitude required to meet course performance standards. The enlisted graduation rate has hovered between forty and fifty percent as a result, in contrast to a junior officer pass rate of over eighty percent.[491]

---

[489] "Interactive On-Net Operator," INSCOM 780th Military Intelligence (Cyber) Brigade Career Opportunities, accessed 10 June 2019, https://www.inscom.army.mil/MSC/780MIB/cyberskills/netop.html.

[490] Author experience in 780th 2013-2016.

[491] Helphenstine, email. The average pass rate O1-O2 was 81.8 percent as of February 2018. Fifty percent is the rough average of O, E, and CIV overall pass rates in the Army. (Justin Helphenstine, email correspondence with the author, February 20, 2018). This fifty percent failure rate stands in contrast to that of the Air Force, which sends more experienced candidates. Sydney J. Freedberg, Jr. "Cyber Course Fights Training Shortfalls: NSA, IONs, and RIOT," Breaking Defense, September 27, 2018, https://breakingdefense.com/2018/09/cyber-force-fights-training-shortfalls-nsa-ions-riot/?fbclid=IwAR29KvAgtVtQlk5ob1pL2sauYFr21gVHcn3QU_55mFT1Gy5vXTB_V5VYS5k.

Driven by a combination of insufficient graduation rates and vacant billets, the Army engaged in a twofold plan to fill the demand for cyberspace operators. First, it began to regularly send officers to RIOT training in 2014, thus mimicking what was already common practice in the Air Force. While enlisted soldiers still attend the course, its most successful graduates remain newly commissioned cyber lieutenants with a four year degree in a technical field. In contrast to the usual Army career model of leadership first, these officers then go on to serve as cyber operators for the first several years of their careers.

Second, in July of 2017, the Army diverged from its sister services in a substantial way when it established the Title 10 Basic Operator Course at Fort Gordon, Georgia.[492] These Army Cyber Operators (ACO) were trained conduct cyberspace operations from Army platforms in support of Army and Combatant Command requirements. Because these soldiers operated from Army infrastructure under Title 10 authorities, they did not need to attend RIOT. By sending soldiers to the Basic Operator Course first, and then only sending the best of those graduates to RIOT, the Army was able to establish a sizable on-net workforce that was capable of conducting operations in support of Title 10 requirements.[493] The existence of this Title 10 cyberspace operator workforce, in conjunction with the Army's implicit focus on providing cyberspace support to ground campaigns, contributed to the selection of an Army three star general as the commander of Cyber Command's first counter-ISIS task force, Joint Task Force Ares.[494]

---

[492] William J. Hartman, Memorandum for Commanders and Staff Operationally Controlled by U.S. Army Cyber Command "Authority to Operate for Army Cyberspace Operators," Fort Belvoir, VA: U.S. Army Cyber Command, July 7, 2017.

[493] In a twist of irony, given the Army's historic struggle with RIOT, the creation of the Army Cyber Operator billet and the Basic Operator Course caused USCYBERCOM to name the Army as the Joint Curriculum Lead for operators.

[494] On JTF-Ares, see USCYBERCOM TASKORD 16-0063 to Establish Joint Task Force (JTF)-Ares to Counter the Islamic State of Iraq and the Levant (ISIL) in Cyberspace. May 5, 2016. See also Michael Martelle, "Joint Task Force ARES and Operation GLOWING SYMPHONY: Cyber Command's Internet War Against ISIL," National Security Archive, August 13, 2018, https://nsarchive.gwu.edu/briefing-book/cyber-vault/2018-08-13/joint-task-force-ares-operation-glowing-symphony-cyber-commands-internet-war-against-isil. The selection of the Army to command JTF-Ares was affirmed by Michael S. Rogers, then-commander of USCYBERCOM, in an interview with the author, January 2, 2019.

Cyberspace Solutions Engineer

The second workrole under study, and arguably the more technically demanding, is the cyberspace solutions engineer (CSE). CSEs are the Army's software developers and computer programmers. As such, a CSE "is a versatile, highly trained individual responsible for the analysis of system vulnerabilities, product research, capability development, documentation, and implementation of software and hardware solutions that operate in and through cyberspace and serve as a force multiplier for maneuver forces."[495]

Shortly after the 780th Military Intelligence Brigade was established in October of 2012, it was directed to provide 87 full-time CSEs to support U.S. Cyber Command mission teams. At the time, there was no established training standard, program, or curriculum within the Army or the joint community to field CSEs, nor did a specific MOS exist that required the CSE skill set. Of the multiple cyber-specific workroles within Cyber Command mission teams, CSE was the only one without an NSA-certified training pipeline. Furthermore, the skills required to field a CSE were not of the type that a military training sequence could easily impart — in the private sector, computer programmers and software engineers are usually college graduates with several years of programming experience. Those CSEs who were working within the brigade prior to this directive had developed their skills independently of the Army, and had been identified and placed into appropriate work centers on an individual basis rather than through a formalized process.[496]

In July of 2013, the brigade launched an initiative to build a training curriculum that could turn an individual with little to no programming experience into an intermediate-level computer programmer.[497] The curriculum would be designed to enable the placement of graduates into specific work centers across the interagency partnership, and to enable each graduate to succeed with minimal

---

[495] "Tool Developer Qualification Course (TDQC) Standard Operating Procedures (Draft)," 780th Military Intelligence Brigade, May 19, 2017.

[496] Walter Schell, email correspondence with the author, Jan 25, 2018. Thomas Bichard, email correspondence with the author.

[497] All CSEs within the brigade contributed to the initiative (Schell, Bichard).

oversight.[498] In early 2014, the group developed a three-phase, 35 week course curriculum in conjunction with the University of Maryland Baltimore County (UMBC).[499] Called the Tool Developer Qualification Course (TDQC), the first iteration ran from 26 September 2015 to 4 August 2016 and had twelve total graduates. As of spring 2018, TDQC had 29 total graduates between two course iterations.[500]

Potential course candidates are identified through an aptitude assessment that is administered to select enlisted personnel and select warrant officers within the 780th MI Brigade. The TDQC assessment tests critical thinking and logic rather than technical skill based on a presumption that TDQC candidates will have little to no programming experience. The assessment is only available to soldiers who have the aptitude and desire to become a computer programmer, and who are already in the cyber branch or willing to transfer into the branch.[501]

The TDQC takes place in three phases. The first phase consists of an introduction to the mathematical principles that underpin coding, as well as Python and C programming languages. The second phase concerns data structures and algorithms and object-oriented programming using Python. The third and final phase teaches secure programming best practices, operating systems, x86 Assembly language, SQL development in Python, and network programming in C.[502] Those who complete the

---

[498] The course focused on building proficiency in two programming languages, Python and C, based upon the predominant languages of industry and partner organizations. Individuals were expected to achieve intermediate proficiency in these two languages by the end of the course (Bichard, email). The brigade worked with a specific interagency development organization, chosen due to a preexisting partnership and to similarities in mission, to determine the standard proficiencies required of an entry-level programmer. Members of the group also collaborated with partners in the Air Force, which at the time was the only other service with a CSE cohort of any significance (Schell, email).

[499] UMBC got the course material accredited through the American Council of Education (ACE), which allowed individuals who complete the course to achieve college credit.

[500] Bichard, email.

[501] Those who pass the assessment are then placed on an order of merit list for entry into the course. Upon graduating from the TDQC, an individual will have six months to prepare for the basic skill level exam and validation panel. An individual will be certified as a Basic CSE once they have successfully passed the basic skill level exam and validation panel.

[502] Throughout the course of their career, CSEs will progress through three certified skill levels: basic, senior, and master. Each skill level has unique requirements and responsibilities, listed below. The creation of a standardized skill level progression, as well the language used to describe each tier, is in keeping with how the Army evaluates individual ability in other unit skill sets, such as parachutist and marksman. The Army has since designated basic, senior, and master skill levels to each of the different workroles on a cyber mission team. These designations help to more easily justifying incentive pay for the achievement of certain skill levels.

course, qualify as Basic CSEs, and go on to perform the function of a CSE are eligible to request assignment incentive pay.

CULTURAL IMPLICATIONS

The Army's approach to building its most technically demanding workroles stands in contrast to what has been adopted by the other services, and as such it offers several critical insights into the influence of Army service culture. First and most significant is the Army's insistence to populate these billets with enlisted soldiers. The Army is alone in its insistence on using enlisted soldiers to fill the most technically demanding workroles, in spite of low enlisted passing rates and the far more suitable technical preparation of its officers.[503] It is also the only service that has attempted to build enlisted software developers.[504] The Army's cultural disposition to view officers as leaders first and technical experts second has thus kept the institution from envisioning a future in which the very technical skill of an officer cohort may demand that it is not wasted on leadership or administration. This reluctance to deviate from the leader-first framework has been detrimental to retention cyber career field: without opportunities to exercise their technical skill, much of the Army's top officer talent has fled to the civilian sector.[505]

Cyberspace thus presents the Army with a unique personnel management challenge: how does the service retain the top-down, pyramid-based command structure in which officers direct combat resources while the enlisted execute, when the skill required for task execution more often resides within the officer corps itself? Furthermore, if the foremost technical experts lie within the officer corps, how does the Army balance the officer's professional mandate to lead organizations with the contemporary

---

[503] Of note, CSE training has a far better pass rate than basic operator training.

[504] By law, one cannot force an enlisted soldier to obtain a college degree, yet a college degree, or the equivalent in self-study, is necessary to become a competent software developer, engineer, or operator. This means that officers fresh off of four years of study in the hard sciences are more well positioned to be the technical experts of the field than their enlisted or warrant officer counterparts.

[505] Josh Lospinoso, "Fish Out of Water: How the Military Is An Impossible Place for Hackers, and What to Do About It," War On the Rocks, July 12, 2018, https://warontherocks.com/2018/07/fish-out-of-water-how-the-military-is-an-impossible-place-for-hackers-and-what-to-do-about-it/. It is worth noting that talent flight is not a problem unique to the Army; however, each service has attempted to solve the problem in its own way.

reality that an officer might be more valuable in a singularly technical role? In other words, cyberspace presents a scenario in which officers are expected to possess a skill set that favors technical expertise over organizational leadership, while the larger institution is structured in such a way as to favor organizational leadership over technical expertise.

Efforts to address this problem within the officer corps led to a debate over whether to create two potential career tracks for cyber officers: a technical track, and a leadership track. This model would allow those who have technical expertise and a taste for organizational leadership to pursue the latter track, while those who simply want to be left alone to code may pursue the former. Detractors argue that those who want to remain technical should become warrant officers, while supporters argue that the reality of the Army's bleeding talent demands a more creative, culture-shifting solution.[506] The same problem exists among non-commissioned officers, though to a lesser degree — just how much leadership should we demand of our highly technical non-commissioned officers when such assignments would be a poor use of their skill set?

The Army's management of officer coding talent demonstrates this tension in action. Officers with the aptitude and desire to serve as software developers were initially given the option to serve as such only if their expected ability to lead was not needed elsewhere.[507] More often than not, this leadership first model resulted in highly talented coders being sent to serve in an administrative company command or to pay their dues on staff. Although the Department of the Army recently coded the officer billet of senior developer as key developmental, commensurate with company command for career progression, there is tacit agreement within cyber branch that an officer must still command in order to be competitive for promotion.

Regardless of what cyber branch may think is good for its officers, the reality is that the larger Army still controls the mechanisms of promotion for both officer and NCO populations. The officer and

[506] The problem with relying on warrant officers for all technical workroles is that it would result in an even more exaggerated pay differential between military and private sector private sector personnel, which would likely further complicate retention efforts.

[507] Author experience.

NCO evaluations that are used across the Army still incentivize leadership over technical skill or experience. However, even if the Army were to successfully create separate technical and leadership tracks for its officers and enlisted, that would not preclude the possibility of a compensation problem, wherein different officer and enlisted cohorts receive different pay for the same work. The differentiation of responsibility within each cohort's career progression, such that an enlisted software developer still has incentive to stay enlisted, becomes paramount to talent retention in the cyber branch.

In contrast to the Army, the Air Force and the Navy have proven less willing to rely upon their enlisted populations for higher skilled workroles, due in part to service cultures which maintain different views of the enlisted and officer roles. In the Air Force, for example, the dominant pilot culture has led to an expectation that officers cannot lead until they have demonstrably proven their individual operational expertise. Allowing Air Force cyber officers to pursue purely technical career paths has faced less institutional resistance than similar efforts within the Army.[508] Meanwhile, the Navy has attempted to solve the technical talent problem through the imposition of a limited career field called the cyber warfare engineer.[509] Officers may serve up to five years as cyber warfare engineers before they must either leave the service or transfer into another career field. The Air Force and Navy have also shown a greater willingness to hire out their technical talent through contractors and the direct commission of qualified civilians. One can speculate that the Army's reluctance to fully embrace similar tactics — though it has implemented a limited direct commission program as of 2018 — stems from a stronger cultural imperative as to what a maneuver formation should look like.[510] The Army's designation of cyberspace as

[508] See chapter 4.

[509] See chapter 5.

[510] Debra S. Wada, Memorandum from Department of the Army: Assistant Secretary of the Army for Manpower and Reserve Affairs to CG, ARCYBER, "Civilian Cyberspace Effects Career Program," January 18, 2017. Corey Dickstein, "Army Launches Direct Commissioning Program for Civilian Cybersecurity Experts," *Stars and Stripes*, December 5, 2017.

maneuver terrain, rather than as an environment which supports maneuver, could be a contributing factor to its embrace of a traditionally maneuver-centric personnel strategy.[511]

Second, the Army's approach to training and certification stands as a testament to the importance of standardized training within Army culture. From the outset, Army leadership in the cyber realm was heavily concerned with creating a standardized training and qualification course for its cyber soldiers, as well as a set of standard procedures and battle drills to drive the collective operation of a cyberspace team. On the individual level, this effort translated into a set of Joint Qualification Standards (JQS) for the basic cyber operator certification that has since become the standard across the joint force.[512] It also resulted in the creation of a complete individual training pipeline for enlisted software developers in TDQC that is not matched by similar programs across the services.

At the team level, the importance of standardized training has resulted in the creation of sub-unit and team-level validation exercises that have enabled Army mission teams to achieve an arguably higher degree of operational proficiency than their inter-service peers.[513] The idea for team validation exercises originated in late 2014, as an increasing number of mission and support teams began to approach initial operating capacity, but lacked specific guidance as what that should mean.[514] Past Cyber Command exercises had focused more on testing higher staff command and control functions than on assessing the

---

[511] The expertise problem in cyberspace — in which officers are more naturally suited to the higher skilled jobs that, in a more conventional maneuver domain, would be performed by their enlisted counterparts — is mirrored in two other Army career fields: the medical corps and the judge advocate general (JAG) corps. Each of these fields requires a level of expert knowledge that can only be acquired through years of education, and that cannot be taught through training. Furthermore, unlike the methodical application of state-sanctioned violence, the legal and medical professions exist independently of the Army and function independently of war. Certification as a professional in these fields thus requires the attainment of an advanced academic degree that is recognized as legitimate by the civilian stewards of the profession. In the medical service corps and JAG corps alike, officers are defined first as experts in their fields, and as leaders second, if at all. The immense body of knowledge, and the ongoing professional education that maintenance of that knowledge requires, means that these officers are neither expected nor required to lead formations. They are paid instead to practice their craft at an individual level, and they are given an initial rank whose institutional respect is commensurate with the level of expertise they possess. The Army's recent experiment with direct commissioned cyber officers suggests an attempt to mimic the JAG and medical corps models, without having to fully embrace them.

[512] The JQS is classified; its analysis is beyond the scope of this document.

[513] Anecdotal evidence from current unit members.

[514] 100CMT was the first team to complete a brigade VALEX in October 2015. NMTs still use Cyber Knight, a CNMF-run event, for pre-FOC certification. Teams must re-certify every two years unless fifty percent or more of their personnel fall into an untrained status. (Michelle Camacho, text correspondence with the author, February 2018).

internal workings of each cyber team. Sub elements within teams also lacked opportunities to exercise their full potential during routine operations. Leadership within the brigade, accustomed to an Army in which brigade commanders have control over the certification of elements within their charge, decided to implement a training system in which the brigade commander could certify team performance through periodic validation exercises. The analogies used to justify these exercises often referenced the certification of tank crews, flight crews, or gun crews prior to major training exercises or combat: one would not cobble together a new tank crew the night before a mission and expect them to succeed, so why treat cyberspace any differently?[515] These cyber team validation exercises have since become an additional, brigade-internal requirement to certify the proficiency of a team prior to its declaration of full operational capacity. They have also become the standard of team training within the Navy and the Air Force.

This push to standardize training has not been without its problems. Since cyberspace is first and foremost a creative domain, the skill to operate within it cannot be mastered through the memorization of a rote 10-level checklist, or through the type of muscle memory that guides rifle marksmanship.[516] The push for training at the expense of education can thus result in a superficial competence that will ultimately fail when faced with dynamic operational problems. Furthermore, the rigid standardization of training leaves little room for cultivating skill in new technologies or for anticipating new technological trends. This defect becomes exceptionally important when one considers the nature of weapons in cyberspace: while the function of a tank, artillery piece, or rifle changes little over the lifecycle of a service member's career, the code that defines a so-called cyber weapon is a living, interactive organism that may change daily. Training, as traditionally defined, will quickly become inadequate for this type of challenge.

---

[515] These analogies extended to discussions of how to certify elements within cyber teams as well. One battalion commander, a former artilleryman, often used the example of battery commanders certifying their gun teams to support the idea of cyber mission team leaders certifying their sub-elements.

[516] The inadequacy of the "training first" model, as opposed to a model build on continuing education and critical thinking, was evident from the author's experience at Fort Meade from 2013-2016. See also Max Smeets, "When Routine Isn't Enough: Why Military Cyber Command Needs Human Creativity," War on the Rocks, December 5, 2017, https://warontherocks.com/2017/12/routine-isnt-enough-military-cyber-commands-need-human-creativity/.

The cyber schoolhouse has taken pains to achieve the proper balance between training and education, as evidenced by a white paper published by three schoolhouse administrators:

> Technology and cyberspace operations change faster than courseware and there is no way to ensure students retain a desired set of [knowledge, skills, and abilities, or KSAs] beyond a training course. Moreover, the best possible outcome of the latest KSA approach is a graduating population prepared for last year's challenges. On-the-job training (for years) remains the only known path to expertise. In conclusion, keeping up with *the latest* in cyberspace operations is a strategy which risks an unprepared CMF. Training *the latest* is nice, but training for what comes next is better. […] Our objective must not be clearly defined tasks, conditions, and standards but a workforce adept at learning and growing in the course of problem solving.[517]

To build problem-solvers capable of encountering new challenges rather than simply trained soldiers executing a mental checklist, the school adopted a method of instruction that was designed to mimic real-world operational problems. The instructor's job becomes one of designing operationally-relevant challenges that students then navigate themselves. This method, as well as its intended end state, is well-communicated in the course objectives of Cyber Common Technical Core: (1) demonstrate the ability to solve problems, (2) demonstrate the ability to research, and (3) demonstrate the ability to quickly gain and maintain technical situational understanding of a cyberspace operational environment. Taken in total, the Army's approach to building its technical cohort reinforces the importance of two key cultural influences: entrenched service expectations of enlisted-officer differentiation, and the importance of standardized training. These influences have shaped the Army's approach to cyberspace in a way that is distinct from the other services.

---

[517] Ryan Tate, Natasha Orslene, Julianna Rodriguez, "Training for Effect: The Army Cyber School Training Strategy," information paper, Fort Gordon, GA, 2017.

SUMMARY: PERSONNEL MANAGEMENT PRACTICES

The Army's cyberspace personnel management practices evolved in several phases. The first phase — as described in this chapter's subcultural subsections — consisted of an ad hoc approach to personnel management that was delegated to the individual branches by default. Spanning from roughly 2000 to 2009, this period was marked first by the absence of senior leader recognition that there was a serious personnel management problem, followed by the lack of consensus on the extent to which existing personnel practices were deficient. Absent a centralized cyberspace personnel management strategy, the signal and military intelligence branches relied upon additional skill identifiers (ASIs) to identify and safeguard their cyber talent. However, since the Army does not manage personnel by ASI, this effort was recognized by all branches as merely an interim measure.

In 2008 Army senior leadership engaged in a discussion of long-term cyberspace personnel management strategy. Central to this discussion was the question of whether or not the branch delegation model was sufficient. While a number of proposals were on the table — to include the creation of a new cyberspace branch comprised of the intelligence, signal, and electronic warfare career fields — the Army chose to retain their existing personnel model. With cyberspace personnel management up to the independent branches for the foreseeable future, the signal and military intelligence communities worked to create new, cyberspace-focused military occupation specialties for both enlisted soldiers and warrant officers.

Concurrently, the United States Military Academy's Electrical Engineering and Computer Science Department engaged in a concerted effort from 2000 to 2009 to produce officers with a strong computer science foundation. These efforts yielded a small nucleus of officers who had more experience in computer science and cyber security than nearly anyone else in the Army at the time. However, structural and cultural obstacles prevented the Army from using these officers effectively. Unlike their enlisted counterparts, cyber-savvy officers did not have a designation to mark their unique skill sets. Even

if they had, it is unlikely that the Army would have been culturally prepared to recognize their importance.

The arrival of a joint U.S. Cyber Command in 2009, followed by the creation of an Army Cyber Command in 2010, marked the beginning of a new phase in the personnel saga. Army senior leadership began to converge onto the gradual consensus that effective cyberspace personnel management — as well as the effective realization of the nascent conceptual framework that had begun to develop for Army cyberspace operations — would require the Army to liberate the field from its previous subcultural stewards. This vision became a reality when Chief of Staff General Raymond Odierno directed the creation of an independent cyberspace branch in 2014.

The creation of an Army cyberspace branch was followed by the consequent integration of cyberspace operations into the mainstream Army service culture. The clashes that resulted from this integration offer telling insight into the extent to which cultural influences can persist even when situational evidence suggests that a different approach might be necessary. Foremost among these influences is branch's decision to rely upon its enlisted population to do the bulk of its high-skill operational work in order to maintain the traditional officer role as one who leads operations rather than executes them. This reliance has persisted in spite of the fact that cyberspace officers are far better suited to perform these highly technical workroles than are their enlisted counterparts.

Conclusion

The first fifteen years of cyberspace evolution in the U.S. Army, from roughly 1995 to 2010, consisted of a collection of individual efforts that were dominated by the military intelligence, signal, and information operations subcommunities and went unmediated by strong strategic direction from senior Army leadership. Absent clear top-down guidance, each community defaulted to an understanding of cyberspace that was heavily shaped by their existing cultural and operational predispositions: military intelligence developed cyberspace as a new variant of SIGINT; signal embraced the idea of network

defense in theory while continuing to prioritize network maintenance in practice; and the information operations community — whose initial approach was arguably the most innovative — gradually lost focus on cyberspace innovation as the community coalesced around contrary ideas of inform and influence in the late 2000s.

The creation of Army Cyber Command in 2010 marked the beginning of a period of transition to a more unified service approach, albeit one hindered by continued disagreement between the intelligence and signal communities over who should play the dominant role in the new warfighting domain. The establishment of an independent cyber career field and attendant training structures in 2014, along with the Chief of Staff directive to drop operations to the tactical level, finally granted cyberspace the institutional momentum it needed to move from a peripheral to a core Army function.

This movement from periphery to core required the resolution of a number of tensions between the nature of cyberspace and mainstream Army service culture. Most importantly, the Army had to present cyberspace in terms that traditional warfighting communities could understand so that it could be easily integrated into maneuver operations. The result was a designation of cyberspace as maneuver terrain through which forces must move in tandem with operations in the physical world. This mentality developed concurrently with the Army's reconceptualization of 21st century warfare in the mid 2000s, in which the hastening convergence of the physical and virtual worlds resulted in increased battlefield complexity. This convergence is now enshrined in the joint concept of multi-domain battle, but its early reflections in Army institutional thinking has had several consequences for the Army's subsequent cyberspace development.

First, if cyberspace is maneuver terrain, then cyberspace officers must speak the language of the maneuver community, and maneuver officers must learn how to think about this added layer to their operational space. This transposition of maneuver language onto the cyber domain is particularly evident within CSCB, but can also be seen within cyber-specific doctrinal publications and internal discourse. The need for cross-community understanding led to the integration of cyber education across the Army PMEs,

as well as the emphasis on common core and Army fundamentals within officer education at the cyber schoolhouse. Had the Army chosen to designate cyberspace as something apart from maneuver, akin to its designation of space — vital to the conduct of land warfare in the 21st century, yet not necessary for land warriors to perfectly understand — then we would not have seen this level of crossover integration.

Second, the designation of cyberspace as maneuver terrain which Army forces must learn to negotiate as they do physical space has resulted in the push to change how the Army thinks about ground force maneuver. Few other services have been as aggressive in this type of holistic cyberspace integration as has the Army through the CEMA Support to Corps and Below initiative. CSCB is not just about pushing capabilities to maneuver forces or adding capabilities to weapons platforms: it is about changing how maneuver leaders and staffs think about the operational space by redefining the parameters of maneuver operations.[518]

Third, the designation of cyberspace as maneuver terrain, and the subsequent effort to operationalize cyberspace through the deliberate selection of combat-minded leadership, led the Army to approach operations in cyberspace with the same tactical mission focus as they do operations in physical space. The risk-aversion that defined the strategic intelligence community from which Army cyber partially developed was thus gradually replaced with the action-oriented, terrain-seizing initiative that is native to maneuver culture. However, this institutional push toward maneuver elevated the risk of tension between the technical and non-technical members of the cyber community, as well as between the technical nature of cyberspace and the non-technical nature of the Army writ large.

The Army's approach to building out a service cohort within the cyberspace domain offers three additional insights into the process of an innovation's assimilation into the dominant service culture. First is the primacy of ground warfare and tactical leadership, as we have seen with CSCB. Second is the importance of standardized training, which is evident through the service-leading training program for

[518] The Navy's Information Dominance construct comes the closest among the services, but it has not resulted in the creation of more tactically-focused cyber units; see chapter 5 for more detail.

enlisted software developers and the creation of now service-standard team validation exercises. Finally, the Army's adherence to traditional relationships between officer and enlisted in the cyberspace domain have resulted in an effort to train enlisted personnel in the most technically demanding workroles, in contrast to the approach of the other services.

CHAPTER 3 | **Cyberspace Development in the U.S. Air Force**

Thus far, I have argued that the path of an innovation is driven by patterns of behavior ingrained in a service's subcommunities. I have also argued that the influence of these communities is higher during periods of uncertainty, when top-down direction is unclear or nonexistent. Because different functional communities will have different perspectives regarding the purpose of an innovation or a new technology, these communities will compete with one another for the advancement of their respective visions within the service. Over time, tensions between competing interpretations will resolve themselves in a way that aligns with the broader service mission and the dominant service culture. Thus, the final operationalization of an innovation will emerge as the gradual, evolutionary product of interaction and bargaining among service communities. Fundamentally, this argument is about the struggle for control and competition among different communities within a military organization.

The pattern described above emerged clearly in the last chapter's discussion of the U.S. Army, a predominantly low-tech service whose primary emphasis is on the individual soldier rather than the equipment he carries or operates. In order to solve the problem of cyber, which emerged as a strategic, intelligence-based enterprise of little direct relevance to the Army's tactical soul, the Army pushed cyberspace operations to the level of individual maneuver units while concurrently expanding the notion of cyber fires and cyber effects to more appropriately fit within the service's existing conceptual frameworks. There, a dedicated subset of the Army's cyber personnel could devote their resources to the types of problems relevant to small units, such as the proliferation of aerial drones, the defensibility of tactical communication networks, or the impact of the adversary's use of cyberspace within the maneuver commander's assigned area of operations.[519] In a sense, this effort to embrace tactical cyber represented a resurrection of the forgotten concepts of both electronic warfare and information operations. By

[519] Lapowsky, "The Pentagon is Building a Dream Team;" "AUSA Cyber Hot Topic 2018, Panel 3: Cyber Support to Corps and Below."

increasing the relevance of cyberspace to the broader Army mission of fighting and winning land wars, the push for tactical cyber allowed the Army's cyber branch to enjoy a type of mainstream success that its predecessors did not.[520]

What type of pattern should we expect to see in the Air Force, a decidedly high-tech service whose decades-long existence has depended upon iterative advances in technology? The Air Force played an instrumental role in the development of computing technologies, and consequently embraced the operational potential of cyberspace well over a decade before the other services: the Air Force's first coherent conceptual framework for what we know today as cyberspace operations was published in 1995, shortly before the creation of the Air Force's first cyberspace operations unit.[521] However, while the highest echelons of the Air Force recognized that cyberspace was something important, there was little consensus as to where, organizationally, it should go. Frequent reorganizations of Air Force cyberspace personnel over the next decade prevented the mission from developing with consistency, and in some instances even undid the progress that had been established in previous years. As a result, after a decade of organizational experimentation, the Air Force approach to cyber today is in largely the same place as it was in 2007.[522]

Given this history, the puzzle then becomes: why did the Air Force, which had emerged as the military thought leader on the subject of cyberspace and information warfare in the mid-1990s, subsequently take so long to develop a consistent operational approach? What caused the progress of preceding decades to come undone? This chapter argues that the movement of cyberspace operations across different subcommunities over time — and, in particular, the contrasting perspectives among these

---

[520] By predecessors, I mean the information operations, psychological operations, and electronic warfare communities. While similar in both concept and function to cyberspace operations in that they are intended to attack adversary information systems and modify adversary behavior, these fields have never enjoyed the level of institutional attention that the Army's cyber branch currently enjoys.

[521] "Cornerstones of Information Warfare," Air Force White Paper, 1995.

[522] Robert J. Elder, telephonic interview with the author, August 8, 2018. This conclusion is also supported by the 2018 movement of AFCYBER to Air Combat Command, where its predecessor units were placed in 2006 before the shift into space command.

communities as to how cyberspace operations should develop — was causal to the mission's uneven patterns of growth.

The Air Force

ORIGINS, HISTORY, AND CULTURE

The development of the Air Force as an organization, from its early origins as an aeronautical division within the U.S. Army Signal Corps to its establishment as an independent service in 1947, is inseparable from the development of airpower as a strategy.[523] When technology opened access to the sky, air theorists quickly realized they needed a strategic framework to justify why the movement into this third dimension of war would be important. This theorizing heritage has heavily influenced the Air Force's sense of itself as a service. As Carl Builder summarizes, "The Air Force was conceived around a strategic theory and midwifed by strategists. Its continuing existence — its justification as an independent institution — rests upon strategic theory."[524]

One of the most influential of these strategic theories was put forth by the Italian strategist Giulio Douhet.[525] In 1921, he argued that victory in war was contingent upon one's ability to "conquer command of the air" — and that, more importantly, a failure to conquer the air meant "defeat and acceptance of whatever terms the enemy may be pleased to impose."[526] This argument led to the conclusion that the existence of an independent air force was both a necessary and a sufficient condition

---

[523] The Army Signal Corps established its first aeronautical division in 1907, which bought its first airplane from the Wright brothers in 1908. This turned into the Army Air Corps in 1926, followed by the Army Air Force in 1941. See "Aeronautical Division, U.S. Army Signal Corps," NGA.mil, accessed August 9, 2018, https://www.nga.mil/About/History/NGAinHistory/Pages/AeronauticalDivision,USArmySignalCorps.aspx.

[524] Builder, *Masks*, 67

[525] The British commander Hugh Trenchard advanced similar ideas: his design for the bombardment of Germany in 1918 developed into the first articulate program of strategic bombardment, and his belief that the airplane was essentially an offensive weapon designed to gain air ascendancy through offensive action greatly influenced the American air strategist Billy Mitchell. From James L. Cate, "Development of Air Force Doctrine 1917-1941," *Air University Quarterly Review*, Vol 1 No 3 (Winter 1947).

[526] Giulio Douhet, *The Command of the Air* (New York: Coward-McCann, 1942), 28-29.

for ensuring national defense.[527] From this premise arose the basic theoretical tenets of early air power: that airpower had become the decisive instrument of war; that the effective use of airpower required air superiority; and that achieving air superiority required the centralized control of air power through an institutionalized and largely autonomous Air Force.[528] With the theoretical framework in place, the next problem was in defining how to achieve air superiority.

By the conclusion of World War I, western air forces had experimented with virtually every mission of airpower familiar with us today, to include aerial reconnaissance, close air support of ground troops, air-to-air combat, and strategic bombing. A number of factors caused American air theorists to embrace the idea of strategic bombing above all. First, the strategic use of airpower — a type of offensive air warfare designed to attack the whole of enemy national structure, from their economic centers to their industrial base to their national will — offered war-weary military leaders and politicians an escape from another war of attrition on the ground. By attacking directly into the enemy's national heartland, long-range strategic bombing opened the possibility of pursuing objectives that were beyond the range and access of the more terrestrially and temporally bounded armies and navies, and thus of ending conflict more quickly and decisively.[529]

Second, and more importantly for an Air Corps that remained stuck inside an Army, strategic bombing offered the greatest promise of delivering full institutional autonomy. Far from mere bureaucratic posturing, American airmen believed that full autonomy was necessary to realize airpower's potential.[530] While the Army could plausibly lay claim to the close air support mission, and while elements

---

[527] In 1921, American air theorist Billy Mitchell published a book entitled *Our Air Force. The Keystone of National Defense* that had similar themes, and whose title alone granted particular emphasis to this first tenet of Douhet's strategy.

[528] Builder, *Masks*, 68. Zimmerman, et al., *Movement and Maneuver,* found this claim to continue to hold true, such that the Air Force continues to argue for airpower as the decisive instrument of war and for air superiority as the service's utmost competency: "Air Force leaders and their doctrine espouse the idea that airpower can dominate any arena and, thereby, be the decisive factor that wins wars." (81-82).

[529] Murray and Millett, *Innovation in the Interwar Years,* 97. See also Cate, "Development of Air Force Doctrine," 16: "[Billy Mitchell] had by 1925 advanced a theory of war based on an air attack against the enemy's national resources rather than against his armed forces." By the late 1920s, belief in this possibility was so strong that the Army Air Corps began to see the bomber as the beginning and end of modern air power (Murray and Millett, 123).

[530] Ibid., 122.

of both the Army and Navy had reason to justify the use of aircraft for the purposes of intelligence, reconnaissance, and communication, strategic bombing did not logically fit within the missions of either service, and so naturally lent itself to an argument for something new.[531] It helped that the doctrine of strategic bombing was such that its very success demanded independence from the ground commanders who might otherwise desire to control it.[532] The heavy bomber thus offered the possibility of achieving independence from the same armies and navies that the most radical air theorists believed were no longer necessary to prevail in future wars.[533]

By the late interwar years, bombardment and autonomy had become so inextricably bound together "that the questioning of bombardments by an air corps officer was not only impolitic but unwise."[534] Strategic bombing had been embraced as both a means and an end: a means by which autonomy might be justified, but also something which was increasingly considered to be the primary purpose of military aviation.[535] The widespread use of strategic bombing by Allied forces in World War II was seen as a validation of this strategy, regardless of what the empirical evidence may have suggested regarding its effectiveness.[536] In 1947, the National Security Act established the Air Force as a third branch of military service, equal in stature to the Army and Navy. Emboldened by the successes of World

---

[531] The Army briefly laid claim to this close support mission, under the belief that: "No one arm wins battles," but the "… coordinating principle which underlies the employment of the combined arms is that the mission of the infantry is the general mission of the entire force. The special missions of the other arms are derived from their powers to contribute to the execution of the infantry mission" (1923 revision of the Field Service Regulations, U.S. Army). Accordingly, Training Regulation 440-15 (1926), stated that the organization and training of the air units should be "…based on the fundamental doctrine that their mission is to aid the ground forces to gain decisive success." This mindset pervaded early instruction at the Air Service Tactical School as well, which deliberately omitted consideration of independent air force operations. Information taken from Cate, "Development of Air Force Doctrine."

[532] Cate, "Development of Air Force Doctrine."

[533] Murray and Millett, *Innovation in the Interwar Years*, 112. See also Billy Mitchell: "The advent of air power which can go to the vital centers and entirely neutralize or destroy them has put a completely new complexion on the old system of war. It is now realized that the hostile main army in the field is a false objective and the real objectives are the vital centers. […] Armies themselves can be disregarded by air power if a rapid strike is made against the opposing centers." From *Skyways*, (Philadelphia, 1930), p. 253.

[534] Murray and Millett, *Innovation in the Interwar Years,* 122.

[535] Ibid., 122-123.

[536] Planners could conveniently ignore the evidence that strategic bombing was too costly and of questionable effectiveness because technological developments allowed for the replacement of the WWII-era fleet of thousands of bombers with a single, massively equipped "stealth" bomber. Wylie, *Military Strategy*, 66.

War II, and encouraged by the nuclear deterrence mission of the Cold War, this early Air Force quickly established its role as the nation's singular global strategic strike force.[537]

The Air Force conception of itself and of its role in national defense has remained largely unchanged since these earliest days of Cold War nuclear deterrence.[538] Today, that mission is captured in the service mantra of "global strike, global reach, global vision."[539] While the methods may have changed, the core concept of reaching into enemy territory to directly attack enemy centers of gravity has remained central to Air Force operations and strategy. As it did seven decades ago, the Air Force continues to see itself as the decisive arm of warfare, an independent, strategic, and primarily offensive force of "global reach, global vigilance, and global power."[540] As such, it must maintain the ability to strike anywhere, at any time, in order to punish or deter aggressors. As *Air Force Doctrine Document (AFDD) 1: Basic Doctrine* states:

> Air Force Doctrine describes the various operations and activities that underpin the service's ability to provide global vigilance, global reach, and global power, which allows us to anticipate threats and provide strategic reach to curb crises with overwhelming power to prevail. Global vigilance is the ability to gain and maintain awareness […] anywhere in the world; […] Global reach is the ability to project military capability responsively […] to any point on or above the earth […]. Global power is the ability to hold at risk or strike any target anywhere in the world […].

This statement is in keeping with the sentiment of Douhet, written nearly one hundred years prior, that airpower is

---

[537] Frank R. Pancake, "The Strategic Striking Force," *Air University Quarterly*, Vol 2 No 2 (Fall 1948): 48-56: "The main burden of preserving the security of the United States rests squarely on the strategic striking force of our air arm" which must be "capable of launching destructive attacks immediately upon commencement of hostilities."

[538] This is not to say that strategic bombing itself has remained the dominant mission within the service — on the contrary, a noticeable shift in doctrine and procurement toward tactical fighter power in the 1970s has since allowed fighter pilots to overtake bomber pilots at the top of the service hierarchy (Zimmerman et al., *Movement and Maneuver*, 83). Rather, it is to say that the Air Force's historic strategic bombing mission and its contemporary role of global strike are part of the same theoretical legacy: one which marshals the various elements of air power to influence enemy targets that are otherwise inaccessible to the surface forces.

[539] Zimmerman et al., *Movement and Maneuver,* 80.

[540] *Air Force Doctrine Document 1* (2015), 4.

> the offensive weapon *par excellence*. It is pre-eminently an offensive weapon not only because it can attack land and naval forces almost at will, but also because it can circumvent them and strike directly at the enemy's capacity to wage war by destroying his industrial, logistical, and administrative centers. If demanded, the cutting edge of air power could even be laid against the very threads which hold a culture together as a viable society. Herein lies its most awesome power and its greatest use as a deterrent force.[541]

This Air Force mission of global strike, together with the boundless medium in which it takes place, led to the development of a mindset called "airmindedness." Airmindedness is described as "a global, strategic mindset providing perspective through which the battlespace is not constrained by geography, distance, location, or time."[542] As articulated by AFDD 1:

> Elevation above the earth's surface […] has helped create a mindset that sees conflict more broadly than other forces. Broader perspective, greater potential speed and range, and three-dimensional movement fundamentally change the dynamics of conflict in ways not well understood by those bound to the surface. The result is inherent flexibility and versatility based on greater mobility and responsiveness. […] With its speed, range, and three-dimensional perspective, airpower operates in ways that are fundamentally different from other forms of military power. Airpower has the ability to conduct operations and impose effects throughout an entire theater and across the range of military operations, unlike surface forces that typically divide up the battlefield into individual operating areas. Airmen generally view the application of force more from a functional than geographic standpoint, and classify targets by generated effects rather than physical location.[543]

Airmindedness results in a broader view of war, a multidimensional perspective to the application of power, and a sense that the Air Force is comprised of problem-solvers by nature.[544] To airmen, the destruction of hostile forces and the control of territory — the most traditional measurements of military success — represent but two options on a spectrum of operations whose full breadth and width is available

---

[541] Robert N. Ginsburgh and Edd D. Wheeler, "The Evolution of Air Warfare," *Air University Review*, Vol 23 No 3 (March-April 1972).

[542] Dr. Dale L. Hayden, "Air-Mindedness," *Air & Space Power Journal* Vol 22 No 4 (Winter 2008): 44-46.

[543] *Air Force Doctrine Document 1* (2015), 14

[544] *Air Force Doctrine Document 1* (2015), 14; "The Air Force prides itself on innovation and flexibility. A lot of people call this air-mindedness: given how we operate, we think we see problems differently than other services do. We're problem-solvers by nature and we tend to be flexible." See also Zimmerman et al., *Movement and Maneuver*, 80.

to the Air Force alone. This "necessarily different" perspective of the airman has unique implications for how the Air Force thinks about war: airpower is offensive, strategic, and boundless in both application and reach; it is versatile, able to affect targets at all levels of war through a variety of means; and it must necessarily be centrally controlled by airmen, who alone possess the perspective to employ it effectively.[545]

CULTURAL IMPLICATIONS

Several conclusions about Air Force culture are evident from this brief history. First, the Air Force is a service whose existence depends on the technology it is able to cultivate. The development of airpower strategy was contingent upon the development of a technology, the airplane, which alone made airpower possible. The success of the airplane in combat was in turn contingent upon the development of a number of technologies, from radar to radio to large-scale data automation, that allowed airmen to outsmart the weather, enemy air defenses, and other aircraft in order to strike deep in the enemy heartland and defend against enemy attempts to do the same.[546] To borrow once again from the words of Carl Builder, "If flight is a gift of technology, and if the expansion of technology poses the only limits on the freedoms of that gift, then it is to be expected that the fountain of technology will be worshipped by fliers and the Air Force."[547] The Air Force is alone among the major three services in both its dependence on and its embrace of technological innovation as necessary to its institutional survival.[548]

This history of technological innovation has left a deep impression on Air Force culture, such that airmen are seen to have a technological acumen which is unique among the services.[549] This emphasis on

---

[545] *Air Force Doctrine Document 1* (2015), 33

[546] Frederick L. Moore, "Radio Counter-Measures," *Air University Quarterly* Vol 2 No 2 (Fall 1948): 57-66.

[547] Builder, *Masks*, 19.

[548] Zimmerman et al., *Movement and Maneuver*, 48: "The service's emphasis on innovation has allowed it to adapt to shifts in technology beyond manned flight, even when embracing such changes has not been easy. Advanced technology is a critical component of what it means to be an airman, regardless of specialty. Indeed, dedication to innovation, or using advanced technologies to address national security problems, has been described as a unifying element of Air Force culture."

[549] Ibid., 78: "Advanced technology is a critical component of what it means to be an airman, regardless of specialty. Indeed, dedication to innovation, or using advanced technologies to address national security problems, has been described as a unifying element of Air Force culture."

technology and technological innovation also lends the service a unique relationship to its human capital. As Lieutenant Colonel Jeffrey Donnithorne writes in *Culture Wars: Air Force Culture and Civil-Military Relations*, "The service's love for technology is not a disembodied one; rather, the Air Force prizes the human connection to technology as manifest in the airplane."[550] In other words, the Air Force considers its technology to be only as good as the people who are trained to use it. The Air Force is therefore uniquely dependent on its ability to attract high quality personnel who possess a high technological aptitude and an ability to think in unconstrained ways.[551]

However, the broad swath of missions assigned to the Air Force and the broad swath of domains in which those missions take place, has made it difficult for the service to develop a unified cultural narrative outside of its core dedication to technological innovation.[552] More than any other service, the Air Force's wide range of capabilities — from air, space, cyberspace, and the nuclear realm — makes it difficult for the service to properly define or articulate its central identity. The resultant sense of "occupationalism" among service members who work in distinct mission areas only complicates the challenge of formalizing a holistic Air Force mission statement.[553] While this diversity of capability has allowed the Air Force to successfully adapt to shifts in technology beyond manned flight, at its worst, it can lead the Air Force to act as a "conglomerate of activities" rather than a unified fighting service.[554]

Furthermore, while much of aerial combat entails a type of individualized tactical decision-making, the full potential of airpower cannot be realized through the type of tactical, force-on-force approach that defines most of surface combat. On the contrary, such a mindset limits the potential of a service which operates in a fundamentally unbounded domain. The Air Force thinks instead in terms of

---

[550] Jeffrey Donnithorne, *Culture Wars: Air Force Culture and Civil-Military Relations* (Maxwell Air Force Base, Ala.: Air University Press, 2013), 28.

[551] Zimmerman et al., *Movement and Maneuver*, 86.

[552] Ibid., 81-82. The Air Force's five core mission areas are air superiority, global precision attack, rapid global mobility, global ISR, and command and control.

[553] Ibid., 81.

[554] Ibid., 90.

creating strategic effects, which they achieve by targeting enemy centers of gravity that are otherwise beyond the reach of their sister services.[555] As technology has evolved, the methods available to achieve these strategic effects have grown to include non-lethal capabilities — cyberspace, electronic warfare, and space — which allow for the very real but reversible degradation of adversary capability. Unconstrained by the limitations of surface forces, and in command of capabilities which can strike anywhere, at anytime, at any level of war, the Air Force sees conflict as a strategic game of worldwide influence, in which finding ways to affect the enemy is as important as figuring out how to destroy him.[556]

The fundamental instrument of this strategic influence is the aircraft, and the fundamental master of the aircraft is the pilot.[557] It follows that the most salient cultural divide in the Air Force is that between pilots and everyone else.[558] Pilots — specifically pilots of manned aircraft — are considered the true warfighters, and thus represent the epicenter of Air Force culture. However, because only officers can fly,

---

[555] Here we could define enemy centers of gravity broadly as "the critical links and nodes of those systems the adversary depends on for effectiveness," a quote taken from an interview with a retired Air Force LTC.

[556] Once again, this statement is not to diminish the role of tactical fighters, close air support, or any of the service's other non-bomber-related missions. However, these missions have not held the same grip on the service's strategic imagination, or on its conception of global strike as the penultimate purpose of airpower. We can expect variation in how different types of pilots might approach the idea of cyberspace — with fighters perhaps more attuned to the need for joint campaign planning and more inclined to take a theater-level operational approach than strategic bombers, for example — but, in line with this dissertation's thesis, we can also expect this variation to subside as cyberspace becomes absorbed into the doctrinally dominant service idea of global strike.

[557] Technological advances — particularly in the area of remotely piloted aircraft (RPAs) — are beginning to challenge this paradigm. However, it is safe to say that, no matter how small the manned aircraft community becomes, and no matter how significant RPAs become to future war, the near-mythological image of the pilot and his aircraft will continue to hold sway over the Air Force cultural imagination. Col Mark D. Wells describes it well: "Given centuries of Western military development and the obvious human admiration for courage, bravery, self-sacrifice, and victory, it hardly seems possible that our Homeric notions of the warrior ethos will undergo any fundamental change. […] Regulations cannot do what emotion and the power of human responses can. Cyber warriors, drone operators, computer specialists, and satellite drivers, may—and, perhaps most certainly, will —determine the outcome of any future major conflict. But like the American Indian tribes of two centuries ago, human emotion as much as logic will dictate the hierarchy among Air Force personnel. If we search for common themes, it seems difficult to overlook the impact of mythology and a certain romantic view of how each group or subgroup can contribute to the welfare of the whole. However expanded the contemporary definition of *warrior*, we collectively seem to default to our earliest human origins engaged in conflict." From Mark D. Wells, "Tribal Warfare: The Society of Modern Airmen," *Air and Space Power Journal* Vol 29 No 3 (May-June 2015):82-87.

[558] Air Force pilots are divided by function into one of ten Air Force Specialty Codes (AFSCs): 11B (Bomber), 11E (Experimental Test), 11F (Fighter), 11G (Generalist), 11H (Helicopter), 11K (Trainer), 11M (Mobility), 11R (Reconnaissance/Surveillance/ Electronic Warfare), 11S (Special Operations), and 11U (Unmanned) (see Air Force Officer Classification Directory (AFOCD): April 30 2018). It is worth noting that distinctions also exist between these pilot subcommunities, but pilots of all stripes are still considered a cut above the ground-bound career fields which support them. While bomber pilots were originally dominant, a shift towards the use of tactical air power in the Vietnam War which, was furthered by the use of air power to support ground fighting in both Gulf Wars, has since allowed fighter pilots to overtake bomber pilots at the top of the service hierarchy — a position which they still hold today (Zimmerman et al., *Movement and Maneuver*, 83-84). For example, of the 24 Chiefs of Staff the Air Force has had since its founding, 15 have been fighter pilots and only 5 have been bombers. The last bomber pilot to serve as Chief of Staff reigned from 1978 to 1982.

the Air Force is distinct among the services in the officer-only composition of its warrior caste, and in the unique structural hierarchy that it creates: the enlisted support the officers, and the officers go to war.

The Air Force is also distinct in the locus of its fundamental decision-making unit, at the level of the individual aircraft rather than the maneuver formation. The distributed nature of air combat is such that the physical massing of forces is considered both unnecessary and counterproductive. As a result, the individual aircraft and the pilot who flies it are seen as fundamentally strategic tools which must be entrusted to make tactical decisions of potentially strategic consequence. While decision-making and control in the Air Force are centralized in order to properly manage risk, execution is decentralized, often to the level of the individual pilot in a single aircraft. This idea of centralized control and decentralized execution is described as the oldest tenet of airpower, one which allows for the unrivaled massing of effects and which encourages the control of airpower by a single airman.[559]

The exclusive use of officers as pilots has additional consequences for how the Air Force approaches career development. First, the level of individual skill required to fly an airplane is such that technical expertise is considered not simply a prerequisite to leadership, but the core proficiency of an officer. This has led to a strong historical and cultural norm in which individual mission proficiency, rather than the successful leadership of other airmen, is considered the most important proving ground on which an officer's career rises or falls.[560] As a result, Air Force officers assume leadership positions far later in their career than their surface counterparts, and only after first proving their operational competency as an individual flyer.[561] This emphasis on individual technical development has become the standard model for the Air Force's operational community, such that the Air Force expects its warfighting officers to be

---

[559] *Air Force Doctrine Document 1* (2015), ch 5. For historical context, see also Phillip K. Heacock, "The Viability of Centralized Command and Control," *Air University Review* Vol 30 No 2 (Jan-Feb 1979): 34-38.

[560] Dean C. Clothier, telephonic interview with the author, April 11, 2018.

[561] Zimmerman et al., *Movement and Maneuver*, 79, 91.

technical experts first. To put this distinction more sharply, while Army officers exist to lead soldiers, Air Force officers exist, by and large, to fly airplanes.[562]

The support community, however — the communicators, intelligence officers, logisticians, and everyone else who is not a pilot — follows a different model, one which more closely aligns with the surface force ideal of a generalist leader. Because support officers are considered managers of a functionality, rather than executors of a capability, their career management pathway is designed to foster broad exposure to the full breadth and depth of their field. Technical expertise is seen to detract from a support officer's ability to make decisions about the capabilities under his command. In these support branches, technical expertise resides with the enlisted, whom the officers are expected to manage. Support officers are thus groomed less for their individual technical expertise than for the breadth and depth of their managerial understanding. These contrary career models will have implications for the future Air Force cyber story.

AIR FORCE SUBCULTURES

The Air Force is comprised of a number of functional subcultures, each with their own purpose, mission, and culture. As described above, the broadest distinction is between the operational community — which is epitomized by pilots but also extends into the nuclear missile and space fields — and the support community. Characteristics of this distinction are most evidently manifested in the relative treatment of officers and enlisted. In operations, officers are warfighters first, leaders second: they are the locus of expertise for their particular field, and they are expected to hone their individual operational skill before branching into other missions. While pilots actually comprise a scant eighteen percent of personnel in the Air Force, the cultural norms they embody are still strong enough to influence broader institutional

[562] The fact that Air Force officers take control of formations much later in their careers has had implications for what they consider an appropriate leadership model for cyberspace organizations. Whereas the Army and Marine Corps might look at a 120 person cyber team as something akin to a line maneuver company, and thus appropriate for a captain, the Air Force — in which captains are considered too junior to be placed in charge of large formations — would assign that formation to a lieutenant colonel or higher. (Surdu, interview).

expectations of officer and enlisted behavior.[563] In contrast to pilots, support officers are managers who are groomed to be generalists through exposure to a broad array of assignment types. Support officers are neither expected nor intended to be specialists in their field, since such specialization is seen to detract from the officer's ability to make decisions about the resources under his command. Expertise within the support community therefore resides with the enlisted airmen.

In addition to this operational/support distinction, there are five subcommunities which have interacted to affect the outcome of Air Force cyberspace operations: signals intelligence, communications, space, the nuclear/strategic bomber community, and electronic warfare. I will evaluate the culture of each of these subcommunities along four dimensions: tolerance of risk, delegation of decision-making, mission orientation, and technical aptitude. Tolerance of risk refers to the extent to which a community is risk accepting or risk averse. Delegation of decision-making refers to whether consequential decisions are retained at high or low echelons of leadership. Together, these dimensions anticipate the extent to which management within a community is hierarchical or flat, as well as the consequent level of individual initiative which the community encourages. Mission orientation describes whether the community supports operations or executes operations, and will dictate subsequent personnel management practices. Finally, technical aptitude describes the extent to which the community values the cultivation of individual technical skill.

Intelligence

The first subcommunity, signals intelligence, exists to intercept and analyze enemy communications signals. The execution of these duties requires the use of sophisticated technological equipment and the application of rigorous analytical methods. Airmen in this field tend to be of both

[563] "Military Demographics," AFPC.af.mil, updated March 31, 2019, https://www.afpc.af.mil/Portals/70/documents/03_ABOUT/Military%20Demographics%20Mar%2019.pdf?ver=2019-04-18-104044-823.

high intellectual caliber and high technical aptitude, and are put through three months of rigorous technical training.[564]

As a support function, expertise resides within the enlisted corps, which means that the enlisted are trusted to make consequential analytical decisions. Officers are trained as intelligence generalists with an understanding of intelligence beyond a specific technical area.[565] They are expected to have enough technical knowledge to be able to make sound decisions about the capabilities under their charge, but are not bred to be technical specialists. This balance of expertise results in a flatter and more collegial organizational culture than that found within the operational Air Force. It is an environment dominated by analytical assessments rather than by operational decisions, by thought rather than by action, and by the continuous execution of mission regardless of location or setting. Regarding risk, the community can be said to have a high tolerance of risk in all areas save the exposure of collection assets and capabilities. In other words, airmen are willing to push the boundaries of what is able to be collected through the creative use of new gadgetry and new capabilities, but will stop short of action which could reveal their precise collection methods. In summary, the Air Force signals intelligence community is tolerant of risk, delegates decisions to low levels, has a support mission orientation which results in a flatter organizational culture and generalist officers, and possesses a high emphasis on technical aptitude.

Electronic Warfare

Comprising the reverse function of signals intelligence is the field of electronic warfare (EW): rather than collecting enemy signals, electronic warfare seeks to disrupt them. Electronic warfare is waged to secure and maintain freedom of action in the electromagnetic spectrum. As such, it is defined as any military action involving the use of electromagnetic and directed energy to control the electromagnetic

---

[564] "Signals Intelligence Analyst," AirForce.com, accessed June 30, 2018, https://www.airforce.com/careers/detail/signals-intelligence-analyst.

[565] Brauner et al., "Improving Development and Utilization of U.S. Air Force Intelligence Officers" (Santa Monica, CA: RAND Corporation, 2009), xi.

spectrum or to attack the enemy.[566] It comprises both offensive and defensive elements, described as electronic attack and electronic protect, intended to protect friendly emissions as well as exploit those of the adversary.

Electronic warfare is intimately tied to advances in technology. Technology first enabled the utilization of the electromagnetic spectrum through the use of radios in the early 1900s. The advent of radar prior to World War II led to the development of radar jammers and countermeasures. The Cold War saw the development of radar with integrated electronic protection, followed closely by the development of new electronic attack methods in response. Conflicts in the Vietnam and the Middle East featured intense battles for dominance of the electromagnetic spectrum that most recently concluded with the problem of electronically-detonated improvised explosive devices.[567]

Because the development of electronic warfare countermeasures depends on an understanding of electronic technology, the anticipation of future technological developments is of vital importance for electronic warfare as a field.[568] Electronic warfare has thus tended to harbor a close relationship with Air Force intelligence in order to stay abreast of the latest in enemy technology. For example, numerous intelligence, surveillance and reconnaissance systems and methods are used to collect the data needed to build the various electronic databases required to effectively employ EW.[569]

Air Force electronic warfare personnel are subdivided according to the function they perform and according to the type of weapon system they support. These subdivisions have resulted in an electronic warfare community that lacks a central career field manager. They have also resulted in a collection of electronic warfare personnel whose primary sense of identity derives from their weapon system rather than from their particular technological expertise. In other words, electronic warfare pilots tend to

---

[566] Department of Defense, *Joint Publication 3-13.1 Electronic Warfare* (Washington D.C.: Department of Defense, January 25, 2007).

[567] See Price, *History Vol III*, for a comprehensive review of electronic warfare developments in these conflicts.

[568] *Annex 3-51 Electronic Warfare* (Maxwell Air Force Base: Curtis E. LeMay Center for Doctrine Development and Education, 2014): 4.

[569] Ibid., 5.

consider themselves pilots first, and electronic warfare officers second.[570] Past proposals to gather these personnel into a single unified community were rejected on the premise that the weapon system they supported was more important than their electronic warfare skills.[571] However, in spite of these differences, the cultural lifeblood of electronic warfare in the Air Force is the jamming of enemy radars and the suppression of enemy air defenses. Electronic warfare involvement in cyberspace thus began with the problem of how to counter air defense systems that had become increasingly digital.[572] Based on its culture and history, one can expect an electronic warfare approach to cyber that is task-oriented, tactically-focused, offensively-minded, risk-acceptant, and oriented fundamentally at technological systems rather than human psychology.

Communications

The communications community, prior to their consolidation into the cyberspace career field in 2009, comprised the Air Force's communication systems managers. Communications was initially a highly technical career field, with communicators historically seen as technical authorities who specialized in radio, radar, telephone, and computer systems.[573] As technology evolved, threats changed, and the pool of available manpower receded, requirements for increased efficiency and lower cost led to a dilution of the communicator's technical aptitude. Multiple, technically-specific communications career field designations were gradually consolidated or eliminated in order to replace the field's technical specialists with general purpose officers who would be capable of managing a variety of systems.[574] This resulted in a community

---

[570] Dean C. Clothier, telephonic interview with the author, September 11, 2018.

[571] Ibid.

[572] Ibid.

[573] Joseph R. Golembiewski, "From Signals to Cyber: The Rise, Fall, and Resurrection of the Air Force Communications Officer" (Thesis, Air University, June 2010), 11.

[574] Ibid., 15: "By 1945, *Army and Air Forces Manual 35-0-1, Military Personnel Classification and Duty Assignment,* listed 36 military occupation specialties that could be judged as being part of the communications officer family of jobs. By 1976, this list had been reduced to about 20 air force specialty codes, and in 2000 there were only four." This reduction coincided with an increase in the complexity of technology, rather than a decrease.

of marginally technically proficient officers who were trained to be interchangeable managers rather than technical experts or specialists. Regarding risk, the potentially widespread consequences of network mismanagement combined with the relative ease with which a system can be inadvertently or carelessly compromised creates a risk averse, procedural culture of system administrators in which centralized control predominates and initiative is discouraged.

Space and Nuclear

Moving on to the service's operational realm, space and the strategic nuclear community share a number of similarities that have led to overlapping cultures. The Air Force space community effectively began with the creation of Air Force Space Command in September 1982, with a mission to operate and maintain early warning radar systems and space-tracking systems.[575] Space Command acquired the space launch mission from Air Force Systems Command in 1990, and the intercontinental ballistic missile (ICBM) mission upon the dissolution of Strategic Air Command in 1992. In 1994, the Air Force merged the space and missile career fields to create the space and missile operations field (13S).[576] Today, the space and missile defense field contains five different officer specialty functions: satellite command and control, spacelift, missile combat crew, space surveillance, and space warning. Training for space and missile officers is short, but technical.[577] The mentality of the space community varies by function. Missileers possess towards a more operational, war-like mindset than their space counterparts due to both their readiness to launch ICBMs and their organizational roots in Strategic Air Command. The remaining

---

[575] Phillips, "Engendering Cybermindedness," 36.

[576] Georges Vernez, Craig Moore, Steven Martino, and Jeffrey Yuen, "Improving the Development and Utilization of Air Force Space and Missile Officers," (Santa Monica, CA: RAND Corporation, 2006), xvii. The Air Force assigns approximately 70% of its 13S lieutenants to missile combat crew positions, which means that the majority of space officers begin their careers as missileers.

[577] Some of the knowledge requirements the AFOCD lists for space officers include: communication system fundamentals, orbital mechanics, launch trajectory and reentry concepts, space lift and rocket propulsion, C2 structure, and nuclear codes and code handling procedures.

space operations officers tend to possess a less operational mindset due to their function of "space force enhancement," or space support.[578]

Space is in the business of launching satellites. The strategic nuclear community is in the business of safeguarding the nation's nuclear arsenal. Both activities are immensely consequential if handled improperly. In addition, both activities generally require a long time horizon of planning and preparation, with the space acquisitions process taking anywhere from seven years to upwards of a decade. Furthermore, the management of satellites and the delivery of nuclear weapons require a global perspective and a strategic mindset, even more so than that which characterizes the rest of the Air Force. Both communities are thus highly risk averse, heavily regulated, and follow a hierarchical decision model in which low-level initiative and operational creativity are discouraged. Procedures and checklists serve to mitigate opportunities for human error, with little opportunity for deviation from pre-set operational plans. The resultant operational tempo is slow and methodical. The space community in particular does not value timeliness as part of their risk calculus; delays are regrettable, but ultimately insignificant when the cost of a mistake can be measured in the hundreds of millions of dollars. The space community therefore tends to place a higher value on technical expertise, while the nuclear community — particular nuclear strategic bombers — places a higher emphasis on a warfighting culture.[579]

Cyberspace

Each of the communities described above differs in important ways from the culture of cyberspace. Cyberspace operations tend to unfold quickly over dynamic terrain, and make use of infinitely modifiable weapon systems which demand close collaboration between the weapon designer and

[578] Phillips, "Engendering Cybermindedness," 47.

[579] Clothier, interview.

its user.[580] Changes to both weapons and terrain can happen on the fly, thus requiring tight decision cycles that are delegated, within limits, to the individual operator level. Missions are meticulously planned and follow a preparation sequence whose length depends on the complexity of the target. Technical expertise is the currency of influence, with both officers and enlisted expected to possess a high level of technical aptitude. In addition, the process of identifying vulnerabilities, designing weapons, and executing operations requires a unique balance of creative inspiration and methodical rigor, such that cyberspace personnel expect a high degree of individual autonomy in how they pursue their work. The resultant culture of cyberspace organizations demands a comfort with operational ambiguity, values initiative and creativity, accepts risk, cultivates deep technical expertise, and enables rapid decision-making through a flat and individualistic organizational structure.

CULTURAL SUMMARY

What does the above exploration tell us about Air Force culture, and what might that culture reveal about the Air Force's later approach to cyberspace? From its origins in the early 20th century to the present day, airpower has evolved in accord with the Airman's original vision of warfare from a distance, bypassing the force-on-force clash of surface combat. Originally manifested in long-range aircraft delivering kinetic weapons, airpower has evolved over time to include those non-lethal supporting capabilities conducted over networks and the electromagnetic spectrum.[581]

The evolution of the tools of airpower has resulted in a necessary embrace of technology as the fundamental currency upon which air superiority rests. Officers must therefore be not only be warfighters, but comfortable technologists who can prove their promotion potential through demonstrated operational

---

[580] It is worth noting that, while operations in cyberspace can happen quickly once initiated, they still take an immense amount of time and effort to plan. The expectation that cyberspace effects can be achieved instantaneously is often a source of tension between cyberspace forces and their supported operational planners: the effects one can achieve in cyberspace is dependent upon the targets one can access, which means that the time horizon for true effects-based planning will vary according to the complexity of the effect desired and the security of the target. The idea that cyberspace operations are "fast-paced" is thus only partly true.

[581] *Air Force Doctrine Document 1* (2015), 12.

competence at the individual level before they can be expected to lead others. While tension still exists between the technical and operational communities, the fact remains that the Air Force has the most technologically welcoming culture of the military services.

Structurally, the potential of Air Force capability to achieve singularly destructive strategic effects has led to an institutional model of centralized control and decentralized execution, with a relatively low tolerance for risk and a procedural approach to operations. We can therefore characterize the Air Force as an offensive, strategic-minded yet risk-averse service that takes an unconstrained view of achieving effects in war, and that takes a strategic approach to the process of innovation.[582] It is culturally welcoming of technology, and its operational mandate of holding targets at risk makes having the potential to exercise power as important as demonstrations of its actual use. Based on this characterization, we should expect the technologically-dominant Air Force to embrace cyberspace earlier than its sister services, with an offensive bent that sees cyberspace as an affirmation, if not a complete fulfillment, of the Air Force mission of global strike. Furthermore, the Air Force's comfort with strategic theorizing — born as it was of a strategic theory — suggests that the service will likewise develop a strongly theoretical orientation toward cyber technology.

The Air Force in Cyberspace: 1947-1999

AIRPOWER AND THE INVENTION OF COMPUTERS

The Air Force has long had a keen understanding of the role of electronics in war, since its core purpose of ensuring air dominance depended upon machines and the technology that underpinned them.[583] The physical demand for computational technology had its origins in the U.S. Air Force, specifically in the twin problems of fire control and air defense during World War II. The challenge of hitting a moving aircraft with a moving artillery shell required extensive computations that outpaced the

[582] Zimmerman et al., *Movement and Maneuver*, 91.

[583] George Dyson, *Turing's Cathedral: The Origins of the Digital Universe* (New York: Vintage Books, 2012), 68-70.

ability of "human computers" to accomplish. Engineers, mathematicians, and scientists set out to build a machine that could complete these computations faster than humans. This effort resulted in the creation of the ENIAC, the first computing machine, in December 1945.[584] By 1948, the increasing importance of electronics in war led airpower theorists to argue that

> The role of electronics and communications in military air operations is a most vital one. The effective employment of air power is dependent upon adequate exploitation of the principles of electronics and their application to air warfare. It can be concluded that electronics and communications, though not weapons themselves, are indispensable to the employment of weapons and in the final analysis spell the difference between victory and defeat in an air war.[585]

By 1955, there was a groundswell of planning activity in the Air Force dedicated to finding new applications for computing technology.[586] Air Force ownership of the nuclear mission and related nuclear defense created a natural demand for ever-improving systems for communication and data analysis. This demand resulted in the creation of such early computer systems as the Semi-Automatic Ground Environment (SAGE), a series of networked radar systems created for homeland defense in 1954,[587] and the 1962 Worldwide Military Command and Control System (WWMCCS) to improve communication during nuclear crises.[588]

These new, complex technological systems greatly expanded the amount of information Air Force decision makers had to process, while improved missile technology rapidly compressed the amount of time available to process it. Consequently, the Air Force became greatly interested in how nascent

---

[584] Scott, McCartney, *ENIAC - The Triumphs and Tragedies of the World's First Computer* (New York: Walker and Company, 1999) 53-54, 101. It could take up to a month to produce a range table by hand

[585] Wendell W. Bowman, "Electronics in Air War," *Air University Quarterly* Vol 3 No 1 (Summer 1949): 48-57.

[586] Harold R. Johnson, "Organizational Integration — Key to the Military Application of Computer Technology," *Air University Review* Vol 17 No 1 (Nov-Dec 1965): 37-43.

[587] Jason Healey, "From Cybernetics to Cyberspace," *Air Force Magazine* (January 2019. For context, SAGE had a memory of "8192 words of 32 bit length" (Charles A. Zraket and Stanley E. Rose, "The Impact of Command, Control and Communications Technology on Air Warfare," *Air University Review* Vol 29 No 1 (Nov-Dec 1977): 82-97.

[588] Gordon T. Gould, "Computers and Communication in the Information Age," *Air University Review* Vol 21 No 4 (May-June 1970): 5-18. The WWMCCS was the direct result of President Kennedy's realization during the 1962 Cuban Missile Crisis that he was not receiving information fast enough. While more aspirational than operational, it established the vision for what the ideal communications platform might look like.

computing technology might be used to improve data-processing and decision-making in real-time.[589] The 1960s saw ample discussion of computer science, with ideas ranging from potential air-relevant research directions to the impact of computers on organizational management. By the late 1960s, the Air Force had become the largest user of computers and communication technology of any U.S. government agency, and had a number of programs dedicated to the study of what was then called information science.[590]

THE RISE OF THE ELECTRONIC AIR FORCE

The increasing digitization of the Air Force throughout the 1960s and 1970s coincided with the growth of the electronic warfare mission in response to the Vietnam War.[591] Electronic warfare was originally given to Air Force Security Service (USAFSS), the Air Force's proponent organization for cryptology and communications security, in 1967.[592] The formal introduction of electronic warfare into intelligence community led to two significant reorganizations in the late 1970s: the creation of the Air Force Electronic Warfare Center (AFEWC) as a subcomponent of the USAFSS in July 1975, and the redesignation of the USAFSS as the Electronic Security Command (ESC) in August 1979.[593] The transition of the USAFSS into the ESC gave the Air Force intelligence community formal responsibility over the use of electronic warfare in combat, in addition to its preexisting intelligence duties. At the same

---

[589] Clifton L. Nicholson, "Command and Control and the Decision-Making Process," *Air University Review* Vol 15 No 1 (Nov-Dec 1963): 77-81 and Dr. Hans H. Zschirnt, "Research in Computer Sciences," *Air University Review* Vol 16 No 1 (Nov-Dec 1964): 47-67.

[590] Rowena W. Swanson, "Information Sciences: Some Research Directions," *Air University Review* Vol 17 No 3 (March-April 1966): 56-68.

[591] The Vietnam War offered opportunities to apply electronic warfare systems and hone electronic warfare techniques that were originally developed in support of nuclear bombers during the early years of the Cold War. See Price, *History Vol II*, for a comprehensive history of electronic warfare in both eras.

[592] Harold P. Myers, John P. Williamson, Gabriel G. Marshall, eds., "A Continuing Legacy: From USAFSS to 25th Air Force 1948-2015," (San Antonio: 25th Air Force History Office), 17.

[593] "The establishment of ESC was in response to the recognized need within the Air Force for a consolidated/major-command-level organization which could provide products, services, equipment, and personnel to assist Air Force commanders to exploit or disrupt opposing electronic and C3 systems and to prevent opposing systems from exploiting or disrupting Air Force electronic or C3 systems." From Doyle E. Larsen, "Electronic Security Command Alert Center," https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/cryptologic-spectrum/esc_alert_center.pdf. Major General Larsen served as the first commander of the ESC.

time, the ESC lost responsibility for a portion of its communications security mission when the USAFSS Telecommunications Center was transferred to the Air Force Communications Service (later the Air Force Communications Command, among other designations).[594]

Part of the Air Force Electronic Warfare Center mission was to determine how to disrupt adversary command and control systems. The substantial intelligence required to execute said mission meant that the preponderance of the organization's workforce had an intelligence background, while leadership of the organization tended to be electronic warfare officers.[595] The mission to disrupt adversary command and control, as well as to counter adversary air defense, adapted as needed to changes in technology. As the systems they were attacking became increasingly digital, the methods used to attack did as well.[596]

Coincident with the growth of electronic warfare mission was the realization that the Air Force's own electronic systems were vulnerable and would need to be secured.[597] A 1972 report for Air Force Systems Command highlighted the "growing requirement to provide shared use of computer systems containing information of different classification levels and need-to-know requirements in a user population not uniformly cleared or access approved."[598] A few years later, in 1976, a Boeing employee named Thomas Rona realized that, "countermeasures aimed at the external information flow of weapon systems will be further improved to the point that they may well become crucial in influencing the outcome of future engagements."[599] A 1977 article further described the impact of advancing

---

[594] Ibid. See also: "Air Force Communications Command," AFHRA.af.mil, January 10, 2009, https://www.afhra.af.mil/About-Us/Fact-Sheets/Display/Article/433902/air-force-communications-command/.

[595] Clothier, interview.

[596] Ibid.

[597] In addition to realizations about the need for computer security, the Air Force also encountered challenges with data storage and information management, and the existence of a generation gap between "technocrats" and traditional managers. The Air Force first encountered these problems in the 1970s, and variations of them still plague the cyber forces today. See Gould "Computers and Communication," and Lewis M. Jamison, "The Information Explosion: Can the Air Staff Handle It?" *Air University Review* Vol 20 No 3 (March-April 1969): 83-89.

[598] Healey, "From Cybernetics to Cyberspace."

[599] Thomas Rona, "Weapon Systems and Information War," (Washington D.C.: Office of the Secretary of Defense, July 1, 1976).

technologies on future doctrine. It argued that the decisive point of future operations would be "the orchestration of sensors and electronics which will gather, process, and distribute battle and target information in almost real time and simultaneously produce a common coordinate grid to locate targets and guide weapons."[600] This provided an early intimation of future Air Force theories of information superiority and command and control warfare.

In 1979, Lieutenant Colonel Roger Schell authored an influential paper in which he argued that computer security would become the "achilles heel" of the Air Force.[601] These premonitions proved particularly prescient during the 1986 "Cuckoo's Egg" incident, in which German hackers penetrated the Lawrence Berkeley National Laboratory to steal unclassified details on President Reagan's Strategic Defense Initiative.[602] The Air Force Office of Special Investigations (AFOSI) played a crucial role in the forensic portion of this first national cyber incident.[603] Then, in 1988, the Morris Worm incapacitated ten percent of the early internet. Though this event was perpetrated by a teenager rather than a nation-state, it resulted in immediate organizational change with the creation of an Air Force Computer Emergency Response Team (AFCERT) at Kelly Air Force Base, Texas. AFCERT reported to the Electronic Security Command, which had been given responsibility for the Air Force computer security mission in 1985.[604] This partnership between AFCERT and the ESC reflected an early recognition of the overlap between signals intelligence and cyber skills and capabilities.[605]

---

[600] David T. Macmillan, "Technology: the Catalyst for Doctrinal Change," *Air University Review* Vol 29 No 1 (Nov-Dec 1977): 16-23.

[601] Roger R. Schell, "Computer Security: The Achilles Heel of the Electronic Air Force?" *Air University Review* Vol 30 No 2 (Jan-Feb 1979): 16-34.

[602] Cliff Stoll, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage* (New York: Pocket Books, 1989).

[603] Healey, "From Cybernetics to Cyberspace."

[604] Myers et al., "A Continuing Legacy," 17.

[605] Healey, "From Cybernetics to Cyberspace." See also Jason Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986-2012* (The Atlantic Council: Cyber Conflict Studies Association, 2013), 31-32 and 107-119.

Table 4. Air Force Intelligence Organizations, 1948-2019

Unit	Date of Formation	Mission	Subordinate To
Air Force Security Service (USAFSS)	20 Oct 1948	Perform the cryptologic mission and provide communications security	Air Force Headquarters
Electronic Security Command (ESC)	1 Aug 1979	Provide intelligence to commanders and improve Air Force electronic warfare. Gained the computer security mission in 1985.	Air Force Headquarters
Air Force Intelligence Command (AFIC)	1 Oct 1991	Provide intelligence support to national decision makers and air commanders through intelligence, security, EW, foreign technology, and treaty monitoring.	Air Force Headquarters
Air Intelligence Agency (AIA)	1 Oct 1993	Provide intelligence and information operations support to commanders and national decision-makers. Consolidated existing intelligence commands, agencies, and elements into a single command. Responsible for cyberspace capability in the form of information operations throughout the 1990s.	1993-2001: AFHQ 2001-2007: ACC
Air Force Intelligence, Reconnaissance, and Surveillance Agency (AFISRA)	8 June 2007	Organize, train, equip, and present assigned forces and capabilities to conduct ISR for combatant commanders and the nation. Lost the cyberspace capability to 8AF/ACC in 2006.	Air Force Headquarters
25th Air Force	29 Sep 2014	Provide multi source intelligence, surveillance, and reconnaissance (ISR) products, applications, capabilities, and resources, to include cyber and geospatial forces and expertise. Is also the service cryptologic component responsible to the NSA for cryptologic activities. Able to conduct Title 50 cyberspace operations.	Air Combat Command

ELECTRONIC COMBAT AND INFORMATION WARFARE

With computers now firmly established as part of the "electronic Air Force," and with an increasing awareness of the security implications therein, the late 1980s saw a shift in Air Force internal discourse from a predominantly defensive to an offensive mindset. It was in 1988 that the idea of "electronic combat" first appeared, described as another dimension of modern war that transcended the previous notions of air, land, and sea power, and which was wholly distinct from the component of modern war known as electronic warfare.[606] The 1991 Gulf War reinforced this theorizing: labeled "the first information war," Desert Storm had officers of all services arguing that rapidly gaining and exploiting information would be the key to success in future conflict.[607] It is noteworthy that the information warfare theorizing of the early 1990s, particularly in the Air Force, had less to do with discrete attacks on communication systems and more to do with the more abstract notions of "thickening the fog of war" in order to achieve military objectives with substantially reduced collateral damage or casualties.[608]

The lessons of the Gulf War led to a series of significant reorganizations within the Air Force intelligence community. First, in 1991, the Electronic Security Command was redesignated as the Air Force Intelligence Command (AFIC). The new organization consolidated, restructured, and streamlined intelligence functions and resources under a single command in order to more effectively provide direct intelligence support to national decision-makers and field commanders.[609] Two years later, the command reorganized again, this time through a demotion into the Air Intelligence Agency (AIA), a field operating agency which reported directly to the Air Force Chief of Staff for Intelligence.

---

[606] Robert M. Chapman, "Technology, Airpower, and the Modern Theater Battlefield," *Air Power Journal* Vol 2 No 2 (Fall 1988): 42-52.

[607] Edward Mann, "Desert Storm: The First Information War," *Air Power Journal* Vol 8 No 4 (Winter 1994): 4-15.

[608] See Alan W. Debban, "Disabling Systems: War-fighting Option for the Future," *Air Power Journal* Vol 7 No 1 (Spring 1993): 44-52 and Owen E. Jensen, "Information Warfare: Principles of Third-Wave War," *Air Power Journal* Vol 8 No 4 (Winter 1994): 35-45. The supremacy of this type of abstract theorizing was affirmed in a telephonic interview with Lieutenant General Bradford J. Shwedo, August 29, 2018. Lt Gen Shwedo served as the Chief of Offensive Information Warfare for the Air Force in the mid-1990s.

[609] Myers et al. "A Continuing Legacy," 22. AFIC merged the personnel and missions of the Foreign Aerospace Science and Technology Center (FASTC), the Air Force Special Activities Center, elements of the Air Force Intelligence Agency, and the ESC into a single command.

It was also in 1993 that the Air Force restructured its Electronic Warfare Center to create the Air Force Information Warfare Center (AFIWC, now the 688th Cyberspace Wing of the 24th Air Force).[610] Combining AFEWC's electronic warfare responsibilities with the security functions from the Air Force Cryptologic Support Center, the AFIWC received a primary mission to channel all electronic battlefield information toward the goal of gaining information dominance over any adversary.[611]

The creation of AFIWC marked the beginning of the development of what we would today call cyberspace operations, under the purview of the Air Force's intelligence community.[612] These early efforts were led by the then-commander of the Air Intelligence Agency, Lieutenant General Ken Minihan, a future director of the National Security Agency and one of the service's early pioneers of information warfare.[613] Having grown up in the intelligence community, Minihan believed that technological evolution would soon render the standard method of signals intelligence — capturing data in transit — defunct. Instead, the increasing digitization of information systems meant that future efforts would need to focus on capturing signals at rest — on actively compromising host machines in order to extra information that may never transit electronic networks.[614] Minihan's theorizing laid the conceptual foundation for the development of what the signals intelligence community would later call computer network exploitation. Furthermore, the 1993 creation of AFIWC marked the beginning of a thirteen-year period in which cyberspace operations were developed in tandem with the intelligence community. Accordingly, only around half of AFIWC was comprised of signals intelligence personnel, with the rest coming from a variety of backgrounds suitable for the information warfare mission.[615]

---

[610] Healey, "From Cybernetics to Cyberspace." On Desert Storm, see Mann, "Desert Storm: The First Information War."

[611] Myers et al. "A Continuing Legacy," 24.

[612] Shwedo, interview. Robert P. Otto, telephonic interview with the author, August 16, 2018. Kenneth A. Minihan, telephonic interview with the author, January 15, 2019.

[613] U.S. Congress, House, Subcommittee on Military Procurement and Research and Development, *Information Superiority for the 21st Century Battlefield*, March 20, 1997 (statement of Lieutenant General William L. Donahue, Deputy Chief of Staff, Communications and Information, Headquarters, Department of the Air Force).

[614] Shwedo, interview.

[615] Minihan, interview.

Several decades of theorizing and reorganization culminated in the publication of a 1995 white paper called *Cornerstones of Information Warfare.* Co-signed by the Secretary of the Air Force and Air Force Chief of Staff, *Cornerstones* laid out the first doctrinal foundation for information warfare in the Air Force. In it, the authors offer a fitting justification as to why the information space is indeed a new domain of warfare:

> Before the Wright brothers, air, while it obviously existed, was not a realm suitable for practical, widespread military operations. Similarly, information existed before the Information Age. But the Information Age changed the information realm's characteristics so that widespread military operations within it became practical.[616]

As a new operational domain, the information space was presented as uniquely important to the Air Force for two reasons: first, it could enable the accomplishment of air objectives, and second, because the Air Force was dependent upon information technology in a way that the other military services were not. Information warfare was described as any activity intended to deny, exploit, corrupt, destroy, or protect information, and it included psychological operations, military deception, operations security, and electronic warfare. The document's definition for information attack as "directly corrupting information without visibly changing the physical entity within which it resides" describes what later came to be known as computer network operations.[617] In a statement which echoes the transformation of cyberspace into its own operational domain over a decade later, *Cornerstones* describes information itself as a "separate realm, potent weapon, and lucrative target," one in which widespread military operations were now practical and necessary.[618] Accordingly, information warfare is described as "activities that deny, exploit, corrupt, destroy, or protect information," through the means of psychological operations, electronic warfare,

---

[616] *Cornerstones of Information Warfare.*

[617] Ibid., 10.

[618] Ibid., 2.

military deception, physical destruction, security measures, and "information attack."[619] It is this latter category which serves as the most direct forerunner to today's idea of cyberspace operations.

THE FIRST CYBER UNIT: 609 INFORMATION WARFARE SQUADRON

Building on the heels of *Cornerstones* theorizing, the Air Force directed the creation of the 609th Information Warfare Squadron (IWS) in 1995. Activated on 1 October, 1995, this was the first Air Force unit that was exclusively dedicated to what we would now call cyber warfare, and the first operational cyber unit in U.S. history.[620] The intent behind the 609 IWS was to "fully operationalize information warfare on behalf of the Air Force Component Commander."[621] Whereas AFIWC existed to develop tools and concepts which could later be transferred to warfighting commands, it was not an explicitly operational organization, and as such did not provide direct capability to the warfighter. The 609 IWS was created to do what AFIWC could not, which was to field combat capabilities to the operational Air Force. Its mission was to defend the 9th Air Force (9AF) and the geography of Central Command from information attacks.

At the time, however, there was no official Air Force doctrine on how to defend or attack in the information space, so the squadron had the task of creating its own concept of operations and standard operating procedures. Furthermore, there was no Air Force Specialty Code (AFSC) for "information warriors," which meant that personnel with the requisite background and skill had to be identified and hand selected from all the existing specialties within the Air Force.[622] The squadron commander and operations officer were each chosen for their previous information warfare experience. Lieutenant Colonel Water E. "Dusty" Rhoads, a former F-117 stealth pilot, had previously served as the Chief of Information

---

[619] *Cornerstones of Information Warfare*., 5-6.

[620] System Technology Associates, Inc., "609 IWS: A Brief History Oct 1995-Jun 1999," Shaw Air Force Base, South Carolina: 20th Fighter Wing, 2006.

[621] U.S. Congress, House, Subcommittee, *Information Superiority.*

[622] "609 IWS: A Brief History," 4.

Warfare Branch at the headquarters of Air Combat Command. Meanwhile, Major Andrew K. "Andy" Weaver, the squadron operations officer, had helped co-author the aforementioned *Cornerstones of Information Warfare*.[623] Shortly after their selection, Rhoads and Weaver selected eight additional cadre members from a cross section of operational backgrounds, to include computer security, acquisitions, intelligence, communications, flight operations, administration, and space operations.

The initial proposal for an information warfare squadron was actually pitched in 1994, when the commander of Air Combat Command realized that the Air Force did not have an operational unit responsible for the increasingly significant task of fighting in the information space — nor did the Air Force have any formal definition of what information warfare actually meant. Moreover, while the Air Force Information Warfare Center (AFIWC) had been developing information warfare capabilities since its inception in 1993, it remained, fundamentally, an exploratory intelligence organization, and as such it was not well-disposed to support Air Force operations.[624] In order to field operational IW capability to the Air Force, the Air Force Council recommended the creation of information warfare squadrons that could then be aligned with fighting Air Force units. When the idea for an Air Force operations unit dedicated to information warfare was first proposed to top Air Force leadership, the commander of 9AF volunteered to sponsor the mission.[625] As the command responsible for the increasingly volatile Middle East and North Africa, 9AF was eager to benefit from whatever offensive and defensive digital firepower an information warfare squadron would be able to provide.

There were two significant challenges to the stand-up of the 609th. First, in the words of its first commander, "nobody really understood what information warfare was […] because back then there wasn't anybody that knew what a cyberwarrior was."[626] Second, the offensive component of the 609th's

---

[623] "609 IWS: A Brief History," 5.

[624] Fred Kaplan, *Dark Territory: The Secret History of Cyber War* (New York: Simon and Schuster, 2016), 108.

[625] "Transcript: Lessons from our Cyber Past - The First Military Cyber Units," Transcript from *Lessons from our Cyber Past: The First Military Cyber Units*, event by the Atlantic Council's Cyber Statecraft Initiative, March 5, 2012, 3.

[626] "Transcript: Lessons," 3.

mission, which comprised thirty percent of the unit's personnel but took up seventy percent of the unit's effort, was heavily classified, thus complicating efforts to both expand understanding of what the unit could contribute across the institutional Air Force, and to gain input on doctrinal development.[627] Both challenges would persist in similar form through the creation of U.S. Cyber Command fifteen years later. A manpower shortage prompted the squadron to hire contractors to accelerate the development of its initial concept of operations.

The official concept of operations was published on 4 October 1996. While the concept was secret, unclassified excerpts provide an adequate glimpse into 609 IWS operations. The 609 IWS was responsible for developing methods that would allow combatant commanders to affect adversary communication systems while simultaneously protecting their own. In other words, it was responsible for both offensive and defensive information warfare. The 609th outlined three primary tasks that would enable these twin missions: first, to develop IW strategies in support of component and theater-level plans; second, to integrate offensive IW capabilities into air missions; and third, to conduct defensive counter information (DCI) missions in order to secure Air Force systems.[628] In order to ensure that all IW capabilities were well-integrated with planning and operations, the squadron would have to work alongside conventional Air Force planners within the Air Operations Center, the central hub that plans, directs, and supervises all Air Force operations in a deployed setting. Regarding DCI, the 609 IWS had two primary tasks: first, to use active and passive measures to defend friendly information systems from attack, and second, to assist in the recovery of an attacked system.[629] This combination of offensive and defensive IW meant that 609 IWS was the first unit in history to combine offensive and defensive cyber operations in direct support of a war fighting commander, and it did so in a way that mirrors what is generally expected of cyber units today.[630]

---

[627] "609 IWS: A Brief History," and Kaplan, *Dark Territory*, 109.

[628] "609 IWS: A Brief History," 7.

[629] Ibid., 8.

[630] Healey, "From Cybernetics to Cyberspace," and Healey, *Fierce Domain*, 35-36 and 39-41.

Because there was no career field for information warfare, squadron leadership received a special authority which allowed it to circumvent normal manning procedures, and which in turn enabled the selection of only the most qualified personnel from across the Air Force. The unit manning structure authorized 93 personnel, of which 30 were officers and the remaining 63 were enlisted.[631] These personnel were divided into a command section, three operational flights, a standardization and evaluation office, and a training office. The squadron also had necessarily wide latitude in selecting its equipment, since a validated operational system for the defense of information systems did not exist at that time. Unit leadership focused their search on both government and commercial off-the-shelf systems. By August 1996, the squadron had selected a system of intrusion-detection and defense sensors that allowed them the real-time capability to defend networks from intruders.[632]

With defensive equipment in place, 609 IWS began the process of developing a standardized training and qualification program in order to develop a common level of expertise among unit members. The diversity of background among squadron members proved a challenge in designing the training program, as several of the cadre members did not possess the requisite knowledge of computer networking to become qualified on the defensive system. The unit established a baseline networking course to rectify this discrepancy among cadre. Further qualification for DCI crews — those who would actually operate the defensive equipment — arrived in the form of tailored contractor courses in June of 1996.[633]

From 12-20 June 1996, the squadron participated in its first large-scale exercise when it sent two cadre members to Blue Flag 96-3 at Hurlburt Air Force Base, FL. While no actual capabilities were employed, the exercise educated the 609th on where and how their mission would integrate with the Air

---

[631] The 1:3 ratio of officers to enlisted demonstrates the contrast between Air Force and Army personnel management: Air Force organizations tend to be more officer-heavy due to the cultural expectation that officers must be technical experts before they can lead.

[632] The squadron tested several systems against one another through Electronic Systems Center (ESC) and Hansom Air Force Base, MA, before selecting the best capability.

[633] "609 IWS: A Brief History," 11.

Force's existing operational processes.[634] The first exercise in which the 609 IWS did demonstrate capabilities occurred in August 1996, at the Joint Warrior Interoperability Demonstration (JWID). The 609 IWS's mission was to conduct defensive operations for all command and control architecture in use at the exercise. The squadron employed two IW crews consisting of four-person teams, each with a crew commander, two information warfare officers, and a runner/trainee. In addition to conducting local exercise network defense, the crews established a network data link with remote sensors in support of a second exercise at Hanscom Air Force Base, Massachusetts. 609 personnel successfully demonstrated its network monitoring and defense capability by rebuffing the intrusion attempts of a Defense Information Systems Agency (DISA) red team, in the first successful employment of its defensive equipment.

Simultaneous to this exercise, another contingent of 609 personnel supported Fort Franklin V at Hanscom Air Force Base in Massachusetts. While JWID took place at the 609th's home duty station of Shaw Air Force Base, Fort Franklin V was the squadron's first off-station deployment of both crews and equipment. The 609 IWS, augmented by personnel from the AFIWC and the MITRE Corporation, was one hundred percent successful in repelling all red team attacks against its networks. This same red team compromised the majority of networks not defended by the 609 IWS.

The 609 IWS declared initial operating capability on 23 August, 1996, based upon its demonstrated ability to (1) provide counter information planners to the Air Operations Center (2) conduct defensive operations against information attacks and (3) provide tactical warning and attack assessment of information attacks against 9 AF units.[635] Of note, because the squadron lacked official training standards at the time IOC was declared, the squadron's initial defensive crews were considered by the Air Force to be not formally certified. In the absence of any precedent for certifying information warfare teams, and in the absence of guidance from higher headquarters, the squadron adopted a standards and evaluations

[634] These operational processes were housed in the Air Operations Center (AOC).

[635] "609 IWS: A Brief History," 15.

program using the space operations program as a model. This use of the space operations program reflected the space community's early interest in and influence on cyberspace operations.[636]

From late 1996 to late 1998, the 609 IWS achieved a number of training and operational milestones to further solidify the importance of its mission to the broader Air Force. It supported Blue Flag 97-1 in February 1997, with full integration of both offensive and defensive IW capabilities. This exercise was the first time that the squadron interfaced with conventional planners and warfighters as a fully integrated member of the team. As part of this total integration, IWS planners coordinated all available IW capabilities with the Air Tasking Order (ATO) in a total effort to support the commander's objectives. These capabilities included psychological operations (PSYOP), Compass Call, electronic warfare (EW), military deception, and operations security (OPSEC), in addition to nominating IW targets for physical destruction and the integration of various classified IW capabilities. Further, it was at this exercise that the squadron developed information warfare threat condition (INFOCON) procedures which served as the threat categorization standard for later joint cyber units.[637] Blue Flag 97-1 served as something of a proof-of-concept for the totality of IWS capabilities, from providing the joint forces commander with a single focal point for all IW related activity, to securing Air Operations Center (AOC) networks, to providing an aggressor team that increased AOC awareness of potential adversary capabilities.[638]

In November 1996, the unit was called to defend the information network at another 9AF base. The squadron installed remote sensors on critical network nodes, and then monitored and defended that network on a permanent basis. In February 1997, the unit was called to deploy a sensor package at a third 9AF base, for a total of three geographically diverse 9AF/USCENTAF units under the 609 IWS's

---

[636] Ken Minihan asserted that the space community expressed a high level of interest in information operations early on based on a perceived opportunity to develop a force structure that they could organize, train, equip, and then operate in the joint environment. Furthermore, most of the black information operations systems in the late 1990s were held by the Air Force space community.

[637] "Transcript: Lessons," 10-11. "609 IWS: A History," 19.

[638] "609 IWS: A Brief History," 16-19.

defensive watch. In March 1997, the squadron deployed its first defensive system within the CENTCOM geographic area. Network packages installed in Saudia Arabia were linked back to the 609 IWS operations floor in South Carolina, providing the first real-time defense against information attacks within CENTCOM boundaries. In May 1997, the squadron received a permanently assigned liaison officer from the Air Force Office of Special Investigation (AFOSI), thus allowing the unit to collaborate on computer crime and investigative issues with relevant federal agencies.[639]

In September 1997, 609 IWS began continuous defensive operations on all assigned networks, providing the first 24/7 network defense capability in the Air Force. Later that month, the unit sent teams to participate in operation Bright Star, a CENTCOM exercise that represented the squadron's first overseas deployment in direct support of AOC operations. Their primary mission was to demonstrate a capability to deploy an information operations team to an overseas location; protect Air Force networks from both real world and exercise threats; develop, coordinate, and integrate an information operations plan with the strategic planning cell;[640] and support the DCI and plans teams with real world intelligence and exercise data through reach back capability to the U.S.[641] One of the most difficult problems throughout all of these exercises was the coordination of the many players who provided input to the overall IW plan.[642]

In April 1998, faced with an evident need to expand 609 IWS capability, the Air Force had to decide whether to retain the IWS concept and replicate it across other units, or to deactivate the 609 and transfer mission functions to other organizations. In order to save manpower and money, the Air Force opted for the latter. Most of the squadron's functional responsibilities were tasked to Detachment 3, 67th Intelligence Group, Air Force Intelligence Agency, thus putting the information warfare component right

---

[639] "609 IWS: A Brief History," 22.

[640] Note the change in terminology from IW to IO. This was concurrent with the publication of a new Air Force Doctrine Document in 1997, and with the broader DoD's shift from to less militant phraseology (Warner, "Notes on Doctrine.")

[641] "609 IWS: A Brief History," 23.

[642] "Ibid., 11, 18, 26.

back into the intelligence community from where it came. The 609 IWS was officially deactivated on 30 June 1999.[643]

What can we learn from this brief organizational history? First, the Air Force's first cyberspace unit was fundamentally operational in nature. In other words, it was hitched to the service's core mission of air superiority and air combat rather than to a supporting function like intelligence or communications. The operational intent of the unit was reflected in its selection of a former pilot as its first and only commander, as well as in the deliberate selection of cadre members from diverse operational backgrounds. The unit's charter and composition, taken in tandem with the tone of the *Cornerstones of Information Warfare* document that inspired it, suggested an early affirmation of cyberspace as an operational rather than a supporting domain.

Second, the eclectic service backgrounds of the unit members suggest an implicit recognition that it would take a variety of perspectives to develop an adequately creative approach to the problem of information operations. Because the unit was stood up with little guidance from its higher command — it was created specifically to figure out how the Air Force might operate in cyberspace, not to execute a mission that had already been determined — its members were documented to have relied upon their individual backgrounds and on private sector best-practices in establishing a way forward.[644] The hand-selection of the unit's members at the outset became particularly important to the capabilities the unit developed and the doctrine it built to guide their employment. The cross-section of organizational backgrounds present in the initial cadre selection was thus less the result of random chance than of a deliberate recognition by the commander that background experience matters, and would implicitly shape how the unit crafted its approach.

Third, the history of the 609th IWS shows that the Air Force was alone among the services in its efforts to operationalize the cyberspace domain in the early 1990s. As the first operational cyber unit in

---

[643] "609 IWS: A Brief History," 31.

[644] Ibid., 5.

U.S. military history, the 609 IWS established the procedural and conceptual foundations for how the Air Force would approach what later became cyberspace operations. Furthermore, while the 609th may have been technologically primitive by today's standards, its model, methods of operation, and level of integration were similar to those seen in cyber units today. This suggests that not only did the 1990s Air Force have the right general intuition about cyberspace, but that they got many of the operational specifics right as well.

SUMMARY: 1947-1999

The Air Force's relationship with computers began with the operational problem of air defense in World War II and the early Cold War. The expansion of the service's reliance on electronic systems led first to a realization that those systems were vulnerable and would need to be protected, and second that those systems could be exploited and attacked to gain battlefield advantage. These ideas converged in the theories of electronic combat and information warfare, as exemplified in Desert Storm and doctrinally instantiated in the *Cornerstones of Information Warfare* publication of 1995.

The Air Force's electronic and digital theorizing coincided with the creation of new organizations dedicated to the electronic and digital realms. Beginning with the Electronic Security Command in 1979 and continuing to the creation of the first operational cyberspace unit, the 609th Information Warfare Squadron, in 1995, these reorganizations marked a relatively unified Air Force response to the problem of computer security and the lessons of Desert Storm. These efforts led the Government Accountability Office to conclude in the mid-1990s that the Air Force has "had better success in detecting and reacting to attacks than either the Navy or Army."[645] The 609 IWS, as the first operational cyberspace unit in the U.S. military, offered a particularly strong example of the Air Force's service-wide leadership in cyberspace innovation at a time when there was little strategic guidance coming from the joint community.

---

[645] U.S. Government Accountability Office, *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*, GAO/AIMD 96-84, (Washington D.C., May 22, 1996).

However, this late-1990s cyber success story also raises an important question: if the 609 was so successful, why was it ultimately disbanded? Furthermore, if the Air Force had an effective organizational and operational solution to the cyber problem as early as 1995, why did it take another decade to establish centralized control, and another fifteen years to create a cyber career field?[646] The convoluted organizational history of Air Force cyber that would emerge in the 2000s reflects the service's struggle to decide exactly where cyberspace operations belonged. The increasingly offensive nature of the cyberspace mission led many to believe that it belonged within the operational Air Force, while its undeniable dependence upon increasingly digitized forms of signals intelligence led others to argue that it should remain within the intelligence community. This debate would play out through various reorganizations from 1999 to the present, all of which would affect the consistency of Air Force cyber development.

The Air Force in Cyberspace: 1999-the Present

CYBERSPACE, INFORMATION OPERATIONS, AND INTELLIGENCE

The dissolution of the 609th in 1999 marked the return to a period in which cyber — at this point now called information operations — and signals intelligence resumed their close relationship within the intelligence community. Since few others in the Air Force were interested in pursuing information operations, and since elements of it, to intelligence professionals, looked and felt a lot like an aggressive form of SIGINT, intelligence leadership had little difficulty integrating the new mission into their organizations and operations.[647] By 1999, the growth of the information operations mission within the intelligence community had led to considerable discussions over the prospect of integrating the AIA with a major command. While the initial proposal was to merge the AIA with Space Command, by July of 2000,

[646] Air Force officers continued to grapple with the problem of how to integrate cyberspace operations into the Air Operations Center nearly twenty years after the 609 IWS had established their own successful method. See Bradley A. Rueter, "Cyberspace Integration within the Air Operations Center," (Thesis, Air University, May 2013).

[647] Otto, interview.

that idea was discarded in favor of a merger with Air Combat Command (ACC). To the then-commander of ACC, this move meant "normalizing information operations as a typical operational activity."[648]

Following shortly on the heels of this announcement, in 2000, the AIA activated two new organizations with a cyber focus: the 70th Intelligence Wing, a cryptologic intelligence organization at Fort Meade, Maryland, and the 67th Information Operations Wing at Kelly Air Force Base, Texas.[649] Both organizations were populated predominantly by signals intelligence personnel. In the absence of an information operations or cyber-related career management field, personnel for these organizations were individually managed and hand-selected for their unique technical skill.[650] The period from 1999-2000 also saw the redesignation of a number of intelligence units to information operations units. These moves served as further affirmation of the increasing importance of information operations within the intelligence community, as well as the increasing demand for IO support across the broader Air Force.[651]

In February 2001, due largely to the growth of information operations, the AIA was formally moved from the Air Force intelligence staff to Air Combat Command.[652] At the time, the ACC was an enormous operational command responsible for both strategic and tactical combat forces.[653] The move was publicized as a way to more effectively provide IO support to warfighting commanders, something which it was assumed could not be done if the capabilities remained distributed within the intelligence community.[654] Moving the AIA into a combat command was also an explicit reflection of the manner in

---

[648] Space command idea and "normalizing" quote from history attached to the Hayden memorandum (FOIA).

[649] From page 48 of an expert of organizational history that was attached to a memorandum received via FOIA request. Memorandum to Lieutenant General Donald G. Cook, Vice Commander of Air Combat Command, from Lieutenant General Michael V. Hayden, Director of the National Security Agency, October 16, 2001.

[650] Shwedo, interview.

[651] This redesignation affected a number of intelligence wings, groups, and squadrons, to include: 566th IOS (Aug 2000), 29 IOS (1999), 67 IOS (2000), 451st IOS (Oct 2000), 566th IOS (Aug 2000), 23rd IOS (Aug 2000), 25 IOS (Aug 2000), 33rd IOS (Aug 2000), 68th IOS (Aug 2000), and the 426th IOS (Aug 2000), 26 IOG.

[652] Bob Arguero, ed., "Air Intelligence Agency and Air Combat Command to Merge," GovCon., accessed June 28, 2018, https://www.govcon.com/doc/air-intelligence-agency-and-air-combat-comman-0001. Hayden, historical narrative attached to "Memorandum," 48.

[653] "Air Combat Command History," ACC.af.mil, updated Feb 10, 2017, https://www.acc.af.mil/About-Us/ACC-History/.

[654] Arguero, "Air Intelligence Agency."

which information operations blurred the Air Force's traditional distinction between intelligence and operations. As a "warfighting weapon," there was a concern that IO had certain operational demands that neither the AIA's intelligence culture nor its intelligence authorities would be able to accommodate.[655] In this sense, the decision to place an intelligence agency under more direct operational leadership was a reaffirmation of the same logic which led to the creation of the 609 IWS in 1995.

However, as a combat command, the ACC did not have an adequate understanding of the idiosyncrasies of the intelligence mission, nor did it know how to effectively prioritize for intelligence needs.[656] Furthermore, there remained a great deal of confusion within the command over what information operations really meant.[657] As a result, the AIA lost much of its previous control over money and manpower, and fell victim to decisions based on arbitrary considerations of organizational symmetry rather than on mission need — as in, we need a colonel in charge of this element because that is what we are used to, not because it is what is appropriate.[658] In a move of further organizational disharmony, ACC leadership began to lobby for full control of the Air Force's cryptologic mission — to include its Title 50 funding — once they began to recognize its importance to cyberspace operations.[659] In 2001, then-Director of the NSA General Michael Hayden wrote an influential memo to quell this debate, in which he articulated that it was unwise and contrary to national policy to subordinate the service cryptologic commander to a major command that did not have intelligence priorities.[660] This memo set a precedent

---

[655] "Warfighitng weapon" from Arguero, "Air Intelligence Agency." Perception taken from Otto interview.

[656] Otto, interview.

[657] Hayden, historical narrative attached to "Memorandum," 47-50.

[658] Otto, interview.

[659] Ibid.

[660] Hayden, "Memorandum." Hayden writes: "National Security Council Intelligence Directive (NSCID) 6 gives me the specific responsibility for "managing SIGINT resources, personnel, and programs." Putting Consolidated Cryptologic Program (CCP) financial management at ACC puts managing those resources at a HQ that is neither within the cryptologic community, nor connected to me or my line of authority in any way. […] My continued support of AIA's integration into ACC remains predicated on the requirement that, as Chief of the Central Security Service, I maintain operational control of SIGINT resources from the lowest echelons of AF units conducting SIGINT operations through the Air Force SCE. […] I understand that ACC and AIA fundamentally disagree and are at an impasse on the issue of functional management of personnel and associated resources. […] AIA's position, which I support, is based on a foundation of legal and policy documents including EO 12333, NSCID 6, DODD 5100.20, and USSIDs 1/4/3000. […] I remain convinced that AIA's integration into ACC is the right thing to do for our Air Force as we operationalize Information Operations."

in which the Air Force cryptologic enterprise would remain distinct from — and at times hostile to — the Air Force operational cyber component.[661]

The period of 1999-2006, in which the Air Force greatly expanded the footprint of its information operations mission, offers a few important, but conflicting, lessons. First, the dissolution of the 609 IWS and the transition of its capabilities into the Air Intelligence Agency suggested that cyber, now called information operations, effectively belonged with its SIGINT corollary in the intelligence community. Intelligence personnel had not only the technical expertise to succeed in cyberspace, but they enjoyed a deep historic relationship with a national cryptologic enterprise that had been engaged in Title 50 cyberspace operations for years. The official transition of a number of intelligence squadrons into information operations squadrons was the most public manifestation of this mutual interdependence between the two disciplines.

However, the simultaneous transfer of the AIA from the Air Force intelligence staff to Air Combat Command in 2001 sent an even stronger signal that cyberspace comprised its own kind of operations. If it was the case that cyberspace was "a distinct warfighting domain" where "combat operations are conducted," then neither the domain nor the activity conducted therein would be able to reach full operational maturity in an intelligence organization.[662] Against this backdrop of ambiguity, both the operational and intelligence communities continued to push for a greater share of the cyberspace mission through the early to mid-2000s.

DOCTRINAL CHANGES

The organizational reshuffling of information warfare-turned cyberspace operations from 1995 to the mid-2000s coincided with a doctrinal overhaul that brought the information domain to the fore of the service's operational consciousness. The first Air Force doctrinal publication to mention concepts related

---

[661] Otto, interview.

[662] Introduction to "Concept of Cyber Warfare," Eighth Air Force Operational Concept, June 1, 2007, 1.

to information warfare was the March 1992 edition of *Air Force Doctrine Document (AFDD) 1: Basic Doctrine.* Fresh off the heels of the first Gulf War, this publication discussed the importance of targeting command and control nodes as a prerequisite to achieving air superiority. AFDD 1 contained the seeds of the ideas which would later germinate into the doctrinal concepts of command and control warfare and information warfare. Of note, the released date of this publication preceded the first official DoD guidance on information warfare by six months.[663]

In September of 1997, and two years after the release of *Cornerstones of Information Warfare*, the Air Force released a significant update to AFDD 1. This update discussed information warfare and information superiority extensively, with deference given to the Air Force's unique heritage in these realms and its cultural predisposition to succeed in them. Recognizing information as "another medium in which some aspects of warfare can be conducted," it listed information superiority as one of six core service competencies, placing the information realm alongside such core Air Force missions as air and space superiority and global attack.[664] This prioritization of the information environment was affirmed in a new description of the Air Force purpose: "The United States Air Force, through operations in the air, space, and information environments, is a global strategic power that can protect national interests and achieve national objectives by rapidly projecting potent air, space, or joint force land power anywhere on earth."[665] The 1997 version of AFDD 1 was also the earliest Air Force doctrinal publication to mention the terms "cyber" and "cyberspace."[666]

---

[663] DoDD TS 3600.1, *Information Warfare*, was published in December 1992, after the lessons of the Persian Gulf War solidified the importance of information technology and C2W. This was DoD's first and boldest pronouncement on the topic of IW, though it was highly classified and had limited distribution. The document defined IW as: "the competition of opposing information systems to include the exploitation, corruption, or destruction of an adversary's information systems through such means as signals intelligence and command and control countermeasures while protecting the integrity of one's own information systems from such attacks. The objective of information warfare is to attain a significant enough information advantage to enable the force overall to predominate and to do so quickly." See also Michael Warner "Notes on Doctrine."

[664] Headquarters, Department of the Air Force, *Air Force Doctrine Document 1: Basic Doctrine* (Washington, D.C.: Headquarters, Department of the Air Force, September 1997), 7.

[665] *Air Force Doctrine Document 1* (1997), foreward.

[666] Compare this with the first mention of cyberspace in an Army doctrinal publication: the 2008 version of FM 3-0, *Operations*.

In 1998, the Air Force released its first doctrine on information operations, Air Force Doctrine Document 2-5, *Information Operations.*[667] The document mades a few key assertions. First, it addressed the terminological confusion that marred early efforts to militarize the information space by distinguishing between information operations, information warfare, command and control warfare, and a short-lived concept called "information-in-war." It defined information warfare as the combat-focused subcomponent of information operations, and information-in-war as all the non-weaponized uses of information which contribute to the commander's battlefield situational awareness.[668] In other words, information-in-war included the use of things like digitized intelligence feeds and command and control systems, while information warfare encompassed efforts to sabotage these same systems that belonged to the enemy. By this definition, information warfare was seen to include and expanded upon previous notions of command and control warfare (C2W).

Second, AFDD 2-5 affirmed the same conclusions of cultural compatibility which were established in AFDD 1: namely, that the strategic perspective and global experience gained from operating in the aerospace continuum made the Air Force uniquely qualified to play a leading role in the development and application of new information warfare capabilities. It further stated that dominating the information spectrum was an indispensable and synergistic component of aerospace power, as critical to conflict now as controlling air and space or occupying land had been in the past.[669] So, the document affirmed that not only is the Air Force uniquely suited to succeed in the information space, but succeeding in the information space is also uniquely necessary for the Air Force.

---

[667] The Department of Defense had made the lexical switch from information warfare to information operations in late 1996, largely in reflection of new foreign and domestic concerns about the potential "militarization" of the internet (Warner, "Notes on Doctrine"). In October of 1998, JP 3-13.1 *Information Operations*, attempted to clear up some of the confusion by declaring IO a broadening of information warfare, which was explicitly reserved for military application.

[668] Information in war can be vaguely described as all those uses of information which facilitate a commander's situational awareness, to include intelligence feeds and command and control systems. Information warfare, in contrast, are those offensive and defensive uses of information to deliberately deceive or imperil the enemy, and to avoid succumbing to the same fate among friendlies.

[669] Headquarters, Department of the Air Force, *Air Force Doctrine Document 2-5: Information Operations* (Washington, D.C.: Headquarters, Department of the Air Force, Aug 5, 1998), 1.

The Air Force updated its *Basic Doctrine* in November of 2003 to reflect many of these, and other, changes. The document opens with the argument that "the rapid maturation of space and information warfare" and "the leveraging power of information technology have transformed the effectiveness of air and space power."[670] Accordingly, information operations is listed as one of the seventeen functions of air and space power, while information superiority remained one of six Air Force core competencies. IO is further clarified as consisting of three components: influence, electronic warfare, and network warfare, the latter of which is comprised of network defense, network attack, and network support. These definitions marked the first time that discussion of network warfare — specific actions taken to attack and defend digital networks — appeared in an Air Force doctrinal publication.

The 2003 update to *Basic Doctrine* was significant for several reasons. As the foundational doctrinal publication for the entire U.S. Air Force, the fact that AFDD 1 devoted such comprehensive discussion to the information environment sent a significant message about emerging Air Force priorities. While the DoD's since de-classified *Information Operations Roadmap* of 2003 declared that IO would be a "core capability of future military forces," neither the Army nor the Navy had similarly robust coverage of IO in their core service doctrine this early.[671] Second, the separation of IO into newly-articulated constituent parts — influence, electronic warfare, and network warfare — offers insight into how the Air Force conceives of the information space as consisting of interrelated cognitive, electro-magnetic, and digital network components. Consequently, it also offers insight into how the Air Force would attempt to organize itself to tackle each of these delineated geographies.[672]

---

[670] Headquarters, Department of the Air Force, *Air Force Doctrine Document 1: Basic Doctrine* (Washington, D.C.: Headquarters, Department of the Air Force, Nov 17, 2003), i.

[671] Donald Rumsfeld, "Information Operations Roadmap," Washington, D.C.: Department of Defense, October 30, 2003. For context, while the Army's 1996 version of FM 100-6, *Information Operations*, is as if not more detailed than any similar Air Force publication on IO, and while its 2001 version of FM 3-0, *Operations* (the service equivalent of AFDD 1) contains an entire chapter dedicated to information superiority, it lists information superiority as an enabling operation, rather than a core service function. The fact that the Air Force declared information superiority as one of six core operational competencies in 1997 speaks volumes about the high prioritization the service placed on the information domain.

[672] Specifically, the transition of intelligence squadrons into information warfare squadrons from 1999-2006 reflects the perspective of many senior Air Force thought leaders that the various components of information and influence should not be operationally separated. This idea of information convergence was resonant in the early 1990s, died off during the GWOT of the 2000s, and is now making a comeback as all three services scramble back toward an information operations-based center.

The 2005 update to AFDD 2-5 reiterated each of these changes, while it also affirmed IO as integral to all AF operations and necessary in achieving air superiority.[673] The 2003 update to *AFDD 1* affirmed the transformation of information operations from a peripheral enabling operation to the integral prerequisite for victory in air and space. The doctrinal and organizational changes which characterized the Air Force approach to the information environment from 1995-2006 reflect this transformation.

[673] Headquarters, Department of the Air Force, *Air Force Doctrine Document 2-5: Information Operations* (Washington, D.C.: Headquarters, Department of the Air Force. Jan 11, 2005).

Table 5. Air Force Cyberspace Terminology, 1995-2010

Term	Date	Publication	Definition
Information Warfare	1995	Cornerstones of information Warfare	Action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own military information functions. Comprised of PSYOP, EW, MILDEC, physical destruction, OPSEC, and information attack.
Command and Control Warfare	1995	Cornerstones of information Warfare	A form of IW that addresses those activities directed against the adversary's ability to direct the disposition and employment of forces, or those which protect the friendly commander's ability to do the same.
Information Superiority	1997	AFDD 1	The ability to collect, control, exploit, and defend information without opposition; to deny the adversary from doing the same.
Information Operations	1998	AFDD 2-5	Those actions taken to gain, exploit, defend, or attack information and information systems; includes both information warfare and information-in-warfare.
Information-in-warfare	1998	AFDD 2-5	The ability to provide global awareness throughout the range of military operations via integrated ISR assets; information collection and dissemination activities; and global navigation and positioning, weather, and communications.
Information Warfare	1998	AFDD 2-5	Operations conducted to defend the Air Force's own information and information systems, or to attack that of an adversary. Consists of offensive counterinformation and defensive counterinformation.
Information Operations	2003	AFDD 1	Actions taken to affect adversary information and information systems while defending one's own. Consist of influence, electronic warfare, and network warfare.
Network Warfare	2003	AFDD 1	The integrated planning and employment of military capabilities to achieve desired effects across the digital battlespace. Consists of network attack, network defense, and network warfare support.
Network Attack	2003	AFDD 1	Those operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, to include the computers and networks themselves
Network Defense	2003	AFDD 1	Those defensive measures to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction
Network Warfare Support	2003	AFDD 1	Those operations to provide information to find, fix, track and assess both adversaries and friendly sources of access and vulnerability for the purpose of immediate defense, threat recognition, targeting, planning and engaging in network operations.
Cyberspace	2010	AFDD 3-12	A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecoms networks, computer systems, and embedded processes and controllers.
Cyberspace Superiority	2010	AFDD 3-12	The operational advantage in, through, and from cyberspace to conduct operations at a given time and in a given domain without prohibitive interference.
Cyberspace Operations	2010	AFDD 3-12	The employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace (JP 3-0)

SUMMARY: 1999-2005

The dissolution of the 609 IWS in 1999 marked the return of cyberspace operations to the intelligence community. This return was marked by the activation of two cyberspace-focused wings, the 70th Intelligence Wing and the 67th Information Operations Wing, underneath the Air Intelligence Agency in 2000. The intelligence community's increasing involvement in cyberspace operations resulted in two significant organizational changes: the conversion of intelligence units to information operations units, and the movement of the Air Intelligence Agency from the Air Staff to Air Combat Command. Competing priorities between the AIA and ACC led to a noticeable friction between the two organizations, and reinvigorated the discussion of where cyberspace operations ultimately belonged.

These organizational changes were accompanied by doctrinal changes that further affirmed the Air Force's embrace of the information domain. Beginning with *Air Force Doctrine Document 1* in 1992 and continuing through its 1997 and 2003 revisions, the Air Force enshrined information superiority as a core service mission alongside its roles in air and space. This effort culminated in the 2003 release of *AFDD 2-5, Information Operations*. Furthermore, these doctrinal developments of 1999-2005 were undertaken with the explicit affirmation that the service's experience in the aerospace continuum, and the strategic perspective that resulted therein, made it ideally suited to play a leading role in the new realm of information warfare.

The Air Force in Cyberspace: 2005-Present

A NEW SERVICE MISSION STATEMENT

However, neither the Air Force's doctrinal nor its organizational changes proved sufficient to bring cyberspace fully into the mainstream of service consciousness. While there may have been an intellectual acknowledgement that cyberspace was an emerging warfighting domain, the larger Air Force culture had yet to embrace the idea in practice. Defensive efforts to secure Air Force networks were uncoordinated and scattered among major commands, while offensive capabilities remained hidden within various signals

intelligence organizations.[674] While pockets of successful cyber activity existed within the Air Force, they were not well integrated into — or well known by — the service writ large. Importantly, the service also lacked a sense of urgency about the potential vulnerabilities of the computer systems it was increasingly relying upon to power its networks and its machines.[675]

In 2005, Secretary of the Air Force Michael W. Wynne and Chief of Staff General T. Michael Moseley attempted to address these problems by changing the Air Force mission statement to include cyberspace.[676] "The mission of the United States Air Force," the new statement read, "is to deliver sovereign options for the defense of the United States of America and its global interests — to fly and fight in Air, Space, and Cyberspace."[677] For Secretary Wynne, the purpose of the mission change was twofold. First, as the former Under Secretary of Defense for Acquisition, Technology, and Logistics, Secretary Wynne saw that the service rush to field sophisticated command and control systems was not accompanied by a commensurate effort to ensure that these systems were secure.[678] The military services were fielding systems without regard to their potential exploitation by an adversary. This was an especially important problem for the Air Force, which was responsible for strategic communication platforms that were relied upon by all military services and other elements of the federal government. Moreover, while the National Security Agency had nominal responsibility for certain aspects of cyber defense, that responsibility did not extend into the protection of operational military networks.

---

[674] Elder, interview. Those activities which we would now call cyber defense (network maintenance and network support) were scattered between a number of organizations which farmed out personnel to the major commands, to include the Air Force Communications Agency (AFCA) and the Air Force Command and Control and Intelligence, Surveillance, and Reconnaissance Center (AFC2ISRC).

[675] Wynne, Michael W., telephonic interview with the author, Aug 28, 2018.

[676] Secretary Wynne in particular knew that this move would be controversial, but he also felt it was the only way to get the service — and the services — to realize the urgency of the cyberspace mission.

[677] Michael W. Wynne and T. Michael Moseley, Air Force Document (AFD) 111003-050, "Letter to the Airmen of the United States Air Force," December 7, 2005.

[678] Wynne, interview.

A PROVISIONAL CYBER COMMAND AND CAREER MODEL

For Wynne, there was a desperate need for a unified cyber command that was responsible for these strictly military problems.[679] However, for these aspirations to be realized, cyberspace operations would have to gain a twofold independence: first, from the intelligence community in which they were housed, and second from any other undue cultural influence that would restrict or constrain the development of a clear vision of how to fight in cyberspace.[680] In 2006, the Secretary and Chief directed the creation of an operational command for cyberspace.[681] This new organization would consolidate the Air Force's scattered cyber capabilities under a single operational command, distinct from the intelligence community and integrated into Air Force global effects operations. Importantly, the command would also entail the transfer of the Air Force's electronic warfare assets from Air Combat Command into the new operational cyber command, as well as the realignment of three space control squadrons and an intelligence detachment.[682] Following on the heels of this announcement, the Air Force Strategic Plan for 2006-2008 articulated a need to "develop […] cyberspace as an Air Force core competency.[683]

The task of standing up a command fell to the commander of the 8th Air Force (8AF), Lieutenant General Robert Elder.[684] While both the Air Intelligence Agency and Air Force Space Command were considered as alternate headquarters, neither was seen as sufficiently capable of developing cyberspace as

---

[679] Wynne, interview. Of note, the former Secretary stated that, had he been made Secretary of the Army or Navy instead of the Air Force, he would have changed their service missions as well. In his words, "it was all about making sure the military woke up to the problem."

[680] Ibid. He specifically mentioned his insistence to allow cyberspace units to develop unconstrained by the perspectives of other service communities, so that they could "tell me how cyber fights."

[681] T. Michael Moseley and Michael W. Wynne, Memorandum, "Establishment of an Operational Command for Cyberspace," September 6, 2006.

[682] Clothier, interview.

[683] "Air Force Strategic Plan 2006-2008," October 5, 2006, http://www.au.af.mil/au/awc/awcgate/af/af_strat_plan_06-08.pdf.

[684] Given Secretary Wynne's insistence on maximal independence for cyber, why the Air Force go with a three, rather than a four star cyber command? A three-star command is the largest command a service can create without congressional approval. Once created, the service may then petition congress for a fourth start. This was seen as the quickest way to get the command rolling, an intermediate solution en route to the longer-term goal of a four-star cyber major command.

an independent warfighting domain.[685] As the 8AF commander wrote in the introduction to the command's first concept of cyberspace operations, "warfighting differentiates the Air Force from other services and agencies."[686] At the time, 8th Air Force was the Air Force's strategic nuclear strike command, the modern-day version of the Strategic Air Command that had been a fixture of the Cold War organizational landscape.[687] The decision to put cyber command into 8AF reflected the Chief of Staff's intent to

> redefine air power by extending our global reach and global power into a new domain — the domain of electronics and the electromagnetic spectrum. The new mission of the MIGHTY EIGHTH will be to integrate the Air Force's global kinetic and non-kinetic strike capability in support of the combatant commander through the full range of military operations.[688]

The integration of cyberspace capability into 8AF was intended to mark a transition from an exclusively kinetic-focused nuclear strike command to a "global effects integrator" that could present both lethal and non-lethal strike capability for global war-fighting.[689]

On November 1, 2006, provisional Air Force Cyber Command (AFCYBER (P)) was activated under 8AF. It absorbed the 67th Network Warfare Wing and the AFIOC from the Air Intelligence Agency for offensive and defensive capability, as well as the network security operations which had

---

[685] Headquarters, U.S. Air Force, "Air Force Cyberspace Command Path to FOC," Powerpoint briefing, September 12, 2007, slide 12.

[686] Introduction to "Concept of Cyber Warfare."

[687] "Eighth Air Force Fact Sheet," AFHRA.af.mil, February 19, 2019, https://www.afhra.af.mil/About-Us/Fact-Sheets/Display/Article/432272/eighth-air-force-air-forces-strategic-acc/. In 1992, SAC was merged with Air Combat Command as a result of the diminishing danger of massive nuclear warfare and the disappearance of a meaningful distinction between strategic and tactical missions. Excepting intercontinental ballistic missiles, which were transferred to the Air Force Space Command in 1993, SAC retained its nuclear strike capabilities under the ACC as the 8th Air Force.

[688] T. Michael Moseley, Memorandum to Lieutenant General Robert J. Elder, "Operational Cyberspace Command 'Go Do' Letter," November 1, 2006.

[689] Headquarters, U.S. Air Force, "Air Force Cyberspace Command Path to FOC."

previously been independently run by the major commands.[690] The 8AF inherited a number of new tasks as the Air Force's global effects integrator and the higher headquarters of the new Air Force Cyber Command. First, to enable the more coordinated employment of Air Force cyberspace operations and to "fully integrate these with air and space operations."[691] Second, to provide trained and ready forces "to conduct sustained offensive and defensive operations through the electromagnetic spectrum," a task which specifically included the consolidation and integration of command and control, electronic warfare, and intelligence, surveillance, and reconnaissance in addition to the network warfare contained in AFCYBER (P).[692] Third, to operate a 24/7 Air Operations Center capable of managing all kinetic and non-kinetic activity effected by the command, and to develop associated tactics for managing such a broad spectrum of capability. Fourth, the command was to establish a long-term plan for the development of a four-star cyber major command and a cyber career management field. Concerning cyberspace operations, the command would be responsible for all offense, defense, and network support, and it would also be the executive agent for Department of Defense cyber crime.[693]

Within this global effects framework, AFCYBER (P) established its own set of objectives. These objectives included the following:

- Deter and prevent cyberspace attacks against vital US interests
- Prevent and rapidly respond to attacks and reconstitute cyberspace operations
- Integrate cyberspace power into the full range of global and theater effects
- Defeat adversaries operating through cyberspace
- Freedom of action in cyberspace for US and Allied commanders
- Persistent cyberspace situational awareness[694]

---

[690] Elder, interview. See also Maryann Lawlor, "Command Takes Network Control," Signal Magazine, October 2006. The Air Force established the Air Force Network Operations Command (AFNETOPS) at Barksdale Air Force Base, Louisiana, in July in order to centralize command and control (C2) of the operations and defense of its portion of the Global Information Grid (GIG). Until AFNETOPS, each major command and even local bases were responsible for their networks' administration. AFNETOPS helped to standardize network operations tactics, techniques, and procedures.

[691] Moseley, "Go Do Letter."

[692] Ibid.

[693] "AFCYBER Activities and Initiatives," September 2007. The Air Force was listed as the executive agent for DoD and industry cyber incident reporting and response, via the Defense Cyber Crime Center (DC3) partnership.

[694] Department of the Air Force, "The Air Force Roadmap for the Development of Cyberspace Professionals 2008-2018," Washington, DC: HQ USAF/A3O-CF, April 15, 2008, 2.

In addition to offensive and defensive cyberspace missions, AFCYBER (P) had an additional interest in pursuing cross-domain cyberspace operations. These involved the use of cyberspace capabilities to achieve effects in and across other domains. Cross-domain cyberspace operations would allow Air Force cyber forces to contribute to the achievement of air superiority by "disrupting or destroying adversary integrated defenses or even networked air-to-air operations," to counterland objectives by "interdicting adversary C2 links or by conducting close support with friendly ground or air forces to defeat ground attacks," and counter-space functions "by denying adversaries access to their satellite systems as well as ensuring continued access for coalition forces."[695] One can speculate that it was in cross-domain cyberspace operations that AFCYBER (P) hoped to prove its relevance to both the broader Air Force and the joint community.[696]

Lieutenant General Elder, the 8AF commander and a career bomber pilot, adapted to the demands of cyberspace by employing a mission-focused management style which relied upon liaison relationships and cross-training, rather than consolidation, to build proficiency within the new cyber command.[697] The cyber organizations that 8AF inherited contained a mix of cyber operators, intelligence, and communications personnel, with most of the technical expertise coming from the intelligence professionals.[698] Elder opted to send 8AF liaison elements to each of his geographically dispersed cyber units rather than pull those units up to 8AF as a way to allow these highly skilled cyber personnel to remain where they could be best supported.[699] At the same time, he cross-trained as many personnel as he could, particularly those who worked in the Air Operations Center, in order to minimize

---

[695] "Roadmap," 3.

[696] William T. Lord, "USAF Cyberspace Command: To Fly and Fight in Cyberspace," *Strategic Studies Quarterly* (Fall 2008).

[697] The commander of the 67th Network Warfare Wing at the time noted that he never faced any resource issues while under 8AF/ACC. In contrast, he argues that resource and personnel issues began to appear following the transfer of AFCYBER to space.

[698] Elder, interview.

[699] Ibid.

the friction between offensive, defensive, and network support functions.[700] This effort yielded a number of successes, from real-world operations to exercise support to the creation of the service's first Concept of Cyber Warfare in June of 2007.[701]

Concurrent to the standup of AFCYBER (P), the Air Force began an initiative to create a cyberspace work force. Representatives from four communities participated in the discussion: electronic warfare, communications, intelligence, and space.[702] At the heart of the debate was the question of how much of each community needed to move into a new cyber career field. Each community had a different idea of the right answer. Electronic warfare was torn between the conversion of all EW billets and the conversion of only the non-fighters. Pushback from the electronic warfare's fighter pilot community — who did not want to surrender their fighter pilot identity — led to strong support for the latter course of action. Intelligence leadership, under the premise that all cyber warfare is a subset of intelligence and that the Air Force intelligence community effectively birthed cyberspace operations, fought for the subordination of the new cyberspace career field to the intelligence community. Meanwhile, the communicators, eager to reverse decades of force cuts and to assert a new type of operational relevance, supported the near-wholesale conversion of their career field.[703]

These discussions culminated with the creation of a document called *The Air Force Roadmap for the Development of Cyberspace Professionals, 2008-2018.*[704] This document provided a broad outline of the Air Force cyberspace strategy along with detailed guidance on how the service planned to create a new cyberspace workforce. Cyberspace forces would need to fulfill four core competencies — establish the domain, control the domain, and leverage the domain — and four enabling competencies — conduct

---

[700] Elder, interview.

[701] Robert J. Elder, Memorandum to Commander, Air Combat Command, "Operational Cyberspace Command "Go Do" Letter, One-year Report," December 28, 2007.

[702] Clothier, interview. Electronic warfare, communications, and intelligence drove the discussion. Space was present, but did not participate to the extent that the other three communities did.

[703] Ibid.

[704] "Roadmap," 8.

intelligence, engineering and acquisition, research, and space. While the document recognized the presence of significant overlap between space and cyberspace functions, it had yet to determine how to distribute these functions among space and cyberspace personnel.[705]

Based on these functions, the Air Force established four cyberspace roles around which to build its new workforce. Cyberspace operators would plan, direct, and execute offensive and defensive cyberspace operations. As such, they would need an intimate familiarity with the technologies and characteristics that comprise cyberspace, a general knowledge of networks, and an understanding of the tools and weapon systems to employ therein. Cyberspace specialists would build, maintain, and protect friendly portions of cyberspace under the auspices of defensive cyberspace operations. Competencies for these specialists would range from system administration to network engineering to radio frequency fundamentals.[706] Cyberspace analysts would provide intelligence support to cyberspace operations. In addition to the basic qualifications of the intelligence field, they would be required to possess additional skills in networking, operating systems, internet protocols, system architectures, and the electromagnetic spectrum.[707] Finally, cyberspace developers were highly educated software and hardware engineers who would design and build cyber warfare tools.[708]

In order to fill these positions, the *Roadmap* outlined a plan to transition different specialty codes from each of the aforementioned fields — intelligence, communications, electronic warfare, and space — into a new cyberspace career field. Electronic warfare, intelligence, and communications would each make an initial contribution of between 300 and 500 personnel.[709] Officers in the new career field would be split between non-rated cyberspace and rated electronic warfare focus areas. Implementation of the non-rated cyberspace officer construct required the phase-out of the 33S communicator specialty, while

---

[705] "Roadmap," 7.

[706] Ibid., 8.

[707] Ibid., 9.

[708] Ibid.

[709] Clothier, interview.

implementation of the rated electronic warfare officer required the transformation of the 12X electronic warfare specialties. Non-rated cyberspace officers would fulfill jobs in terrestrial-bound cyberspace and space organizations, while rated electronic warfare officers would provide cyberspace and electronic warfare functionality on Air Force flying platforms. Meanwhile, the creation of a cyber enlisted cohort entailed the fusion of 14 different occupation specialties from a variety of backgrounds — to include communications and the maintenance of Air Force special mission platforms — into a new, 1B career field.[710] Central to each of these career field transitions into a new cyberspace profession was the need to enact a culture change from one of "support" to one of "operations."[711]

By the end of 2007, the Air Force had emerged as the recognized service leader in cyberspace.[712] While the other services were engaged in the patchwork pursuit of various cyberspace-related initiatives, neither the Army nor the Navy had the level of decisive senior leader engagement or senior leader direction that existed in the Air Force in 2007. Moreover, no other service had produced the type of detailed professional roadmap for the creation of a cyberspace workforce as had the Air Force in its 2008 publication.[713]

---

[710] These 14 Air Force Specialty Codes were: Knowledge Operations (1B0X1), Cyber Systems Operations (1B0X2), Cyber Surety (1B0X3), Client Systems Specialist (1B1X1), Cyber Transport Systems Specialist (1B1X2), RF Transmission Systems Specialist (1B1X3), Cyber Spectrum Specialist (1B1X4), RADAR Systems Specialist (1B1X5), Airfield Systems Specialist (1B1X6), Cable/Antenna Systems Specialist (1B1X7), Control Systems Specialist (1B1X8), Mission Systems Maintenance (1B1X9), On-Net Operations (1B4X1), and Electronic Warfare Operations (1B4X2). See "Roadmap," Annex B.

[711] "Roadmap," 18.

[712] Elder, "One Year Report." Neither the other services nor U.S. Congress were fully on board with this development. The other services did not want to see the Air Force unilaterally take over the new cyberspace domain, even though they remained reluctant to embrace the domain themselves, and Congress was skeptical of the tone of the Air Force's cyberspace-themed recruiting ads. See Julian E. Barnes and Peter Spiegel, "Air Force Ads' Intent Questioned," *Los Angeles Times*, March 30, 2008.

[713] While the Army had considered different courses of action for the creation of a cyberspace cadre in 2008, its selection of the status quo solution precluded the execution of the type of workrole analysis that the Air Force conducted for its "Roadmap."

FALSE START: CYBER GETS NUKED

However, in late August of 2007, a significant incident of nuclear mismanagement halted the Air Force's cyber momentum and led to the reversal of previous personnel decisions.[714] A B-52 nuclear bomber flew from Minot Air Base, North Dakota, to Barksdale Air Base, Louisiana, with six live nuclear weapons. Neither the pilots, nor anyone else at either air base, realized that the missiles were live until roughly 36 hours after the plane had landed.[715] Air Force leadership took this oversight as an indication that the pursuit of new technologies had caused the Air Force to lose sight of its core priorities, which had, in turn, resulted in the dangerous degradation of the service's nuclear proficiency.[716]

In the service's subsequent operational pause, two events occurred that had a direct effect on the establishment of the 24th Air Force. First, the *Report of the Secretary of Defense Task Force on Department of Defense Nuclear Weapons* Management, colloquially known as the Schlesinger Report and released in September 2008, recommended that the Air Force place all of its nuclear weapons under a single command in order to rectify the "unambiguous, dramatic and unacceptable decline in the Air Force's commitment to perform the nuclear mission."[717] The Air Force responded with the creation of the Air Force Global Strike Command (AFGSC), which was tasked to oversee all long-range nuclear-capable bombers and intercontinental ballistic missiles.[718] The creation of AFGSC meant that all non-bomber-related functions, to include cyberspace operations, would be removed from 8AF in order to allow the command to focus exclusively on its nuclear mission.[719] This meant that AFCYBER lost its global strike

---

[714] This, combined with several other incidents, led to the eventual firing of both Secretary Wynne and Chief of Staff Moseley by Defense Secretary Bob Gates.

[715] Douglas L. Raaberg, "Commander Directed Report of Investigation, Prepared by MG Douglas L. Raaberg, Investigating Officer, Concerning An Unauthorized Transfer of Nuclear Warheads Between Minot AFB, North Dakota, and Barksdale AFB, Louisiana," August 30, 2007.

[716] Otto, interview; James R. Schlesinger, "Secretary of Defense Task Force on DoD Nuclear Weapons Management," September 12, 2008.

[717] "Panel Urges Air Force to Unify Nuclear Command," *The New York Times,* September 12, 2008.

[718] "Air Force Global Command Fact Sheet," U.S. Air Force web page, November 30, 2015, https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104462/air-force-global-strike-command/.

[719] "History of the Twenty-Fourth Air Force and 624th Operations Center," 24th Air Force Heritage Pamphlet, 24 AF Office of History, January 17, 2014.

patron at the same time that Air Force Space Command (AFSPC) had to surrender its intercontinental ballistic missiles.[720]

With AFCYBER now homeless, the AIA — which had recently been redesignated the Air Force Intelligence, Surveillance, and Reconnaissance Agency (AFISRA) and returned to its original home under the Air Staff A2[721] — began to lobby for the return of cyberspace to its intel origins.[722] At the time, AFISRA still had command of the Air Force's electronic warfare and information operations missions, and it still maintained the ability to conduct Title 50 cyberspace operations through its cryptologic affiliation with the National Security Agency.[723] The natural synergy between SIGINT and cyber led many within the intelligence community to lobby for ownership of cyber command.[724] However, the events of 2005-2006 established the clear precedent that there was a distinction between intelligence and warfighting, and that cyberspace was not intelligence. As such, it would not return to the intelligence community.

---

[720] AFSPC received ICBMs after the dissolution of Strategic Air Command in 1993. See "Air Force Space Command History," Air Force Space Command web page, accessed June 29, 2018, https://www.afspc.af.mil/About-Us/AFSPC-History/.

[721] The purpose of this move was twofold: to better reflect the character of ISR as a domain-neutral asset which should serve all Air Force major commands, rather than just the ACC, and second, to broaden the scope of the intelligence agency beyond SIGINT. It also reflects the perpetually changing answer to the questions: what do we do with intel? See "Air Intelligence Agency to Become Air Force ISR Agency," AF.mil, May 15, 2007, https://www.af.mil/News/Article-Display/Article/126859/air-intelligence-agency-to-become-air-force-isr-agency/.

[722] Clothier, interview. Specifically, Major General John C. Koziol, the commander of AIA, saw cyber as another form of SIGINT with the potential to create effects.

[723] John N.T. Shanahan, telephonic interview with the author, August 2, 2018. See also "Command Takes Network Control."

[724] Ibid.

CYBER MOVES TO SPACE

In addition to the Schlesinger Report, the second significant event which affected the development of Air Force cyber command was a major, DoD-wide intrusion onto military networks.[725] This event reiterated the urgency of coordinated network security, and reinforced for the Air Force the need to give its cyber command significant operational authority. While the provisional Air Force cyber command had been established with the intent of eventually becoming a four-star major command, the nuclear-induced pause in cyber growth led to a reevaluation of whether a major command was feasible.[726] As momentum for a major command stalled, AFCYBER leadership within 8AF pushed for the creation of a cyber numbered Air Force (NAF), a three-star, independent operational command, instead. In August of 2009, AFCYBER became the 24th Air Force underneath Air Force Space Command.

The justifications for this move into space command were threefold. First, the interdependence of cyber and space led to an expectation that placing them together would lead to mutually beneficial outcomes.[727] Both were strategic-minded, technologically-savvy organizations whose hardware depended on one another to function, so there was an expectation that the two communities would get along. Second, Air Force Space Command already had a relationship with U.S. Strategic Command, which had been the unified command for military cyber, space, and nuclear forces since 2002.[728] Given that AFCYBER would have to report to strategic command anyway, it made sense to place it within a command that already had this established relationship. Third, and perhaps most importantly, space command had lost sixty percent of its personnel when its nuclear ICBM mission was transferred to 8AF.

---

[725] While this intrusion remains nameless in the 24th Air Force official history, one can speculate that it was BUCKSHOT YANKEE. See William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* (Sept-Oct 2010), or Kim Zetter, "The Return of the Worm that Ate the Pentagon," *Wired*, December 9, 2011, which argues that Buckshot Yankee was causal in the formation of U.S. Cyber Command.

[726] For original intent, see "Go Do" letter. For debate over MAJCOM or NAF, see Robert J. Elder, "Cyberspace Paper for COMACC." Secretary Wynne was the only one who wanted to see AFCYBER become a MAJCOM; once he was fired, the momentum stalled.

[727] Otto, Shanahan, Shwedo, interviews.

[728] STRATCOM received the cyber mission by default in 2002, when Sec Def Donald Rumsfeld directed the merging of USSPACECOM with USSTRATCOM. "History," STRATCOM.mil, accessed June 25 2018, http://www.stratcom.mil/About/History/.

The loss of the ICBM mission left a very real, very political need to fill this void with something else in order for space to justify retaining its four-star status.[729]

The move of AFCYBER to space command had significant implications for AFCYBER's development. First, it disrupted the natural and historic relationship between the cyberspace and intelligence communities. This was significant, because most of the Air Force's cyberspace expertise still resided within the SIGINT community, even after the move to space.[730] While the intel-cyber relationship had been jeopardized by the 2006 decision to put cyberspace capabilities underneath 8AF and the Air Combat Command, little about the relationship had changed at the level of day-to-day operations during that period.[731] This continuity in relationship was likely due in part to LTG Elder's decision to keep his geographically dispersed cyber forces where they were when he inherited them, and where they could retain the best mission support, rather than consolidate them all in one location for the purpose of centralized command and control.

In contrast, the movement of 24AF to space command effected a more lasting rift. With AFISRA reporting to the Air Staff A2, and AFCYBER reporting to U.S. Strategic Command through the AFSPC, the once unified disciplines of cyber and signals intelligence were split into distinct organizations, each with their own headquarters, their own chain of command, and their own operational priorities. For a time, the intelligence community continued to be involved with cyber after this divorce, often by providing personnel with the right expertise to fill certain cyber billets. However, this involvement was personality-dependent, the result of commanders who could work well with one another in spite of organizational constructs that neither required nor demanded it.[732] Friction between the two commands, each of whom naturally wanted to have full control over their own personnel, ebbed and flowed over time with the

---

[729] Elder, interview.

[730] Shanahan, interview.

[731] This seems to have been largely due to the management style of Elder, who allowed personnel to stay where the resources were that could support them.

[732] Shanahan, interview.

rotation of unit commanders. This split cyber/intel construct also created issues for manning joint cyber organizations later on. Air Force teams within the Cyber National Mission Force, for example, would often have a mix of personnel from different commands co-located on the same team.[733]

This friction between the intelligence and cyberspace communities reached a head in 2011, when the commander of Space Command — having realized the importance of signals intelligence to cyberspace operations — made a push to turn AFISRA's cryptologic component into a subordinate numbered air force. This effort to once again unify the intelligence and cyber components mimicked previous turf wars between Air Combat Command and the Air Intelligence Agency. Placing the Air Force intel component under Space Command would have helped the cyber mission, but keeping ISR where it was would allow it to continue to provide unified reporting to the NSA. The AFISRA commander believed that the two disciplines belonged together, but did not belong under the supervision of Space Command, and so he heavily fought the takeover from summer 2011 to spring 2012.[734] General Hayden's 2001 memo on the need to split Title 10 and Title 50 cyberspace operations was resurrected in this instance to justify keeping AFISRA independent.[735]

The move to Space Command also had implications for how cyberspace operations were organized. AFCYBER attempted to rectify its initial struggle to clearly delineate each cyber capability through the creation of Cyber Operations Mission Sets (COMS). These mission sets were roughly analogous to Space Command's central organizational concept of Space Mission Areas. They allowed AFCYBER to achieve early progress in a number of important areas, to include operations training, crew force standardization and evaluation, and mission operations procedures. However, while the COMS construct was modeled after space organization, it was not well-suited to enabling Space Command to properly organize, train, and equip the cyberspace mission because it did not fit into the broader Air

[733] Shanahan, interview.

[734] Otto, interview.

[735] Ibid.

Force's weapon system concept. This structural mismatch meant that cyberspace capabilities were effectively invisible to space leadership and led to several years of persistent resourcing challenges.[736]

Finally, the move of cyberspace to Space Command raised a number of significant cultural challenges that would have to be overcome for the two fields to work effectively together. The first of these challenges concerned the respective communities' tolerance for risk. Space command was responsible for launching and controlling satellites, a process which requires a slow, methodical, detailed approach to engineering, a long operational timeline, and an extremely low tolerance of risk. The consequences of failure when dealing with satellites — and, from 1993-2009, with intercontinental ballistic missiles — are at best expensive and at worst catastrophic. In planning and preparing for a satellite launch, space operators would rather accept lengthy delays than do anything which would increase the risk of mission failure. It was not uncommon for the command to wait ten years or more between the initial development of a satellite concept and its ultimate launch into space.

This ten year acquisition and development timeline means that a mistake in the process of controlling satellites could result in the potentially irretrievable loss of mission capability. The decision space of satellite mission crews is thus deliberately limited in order to reduce the possibility of human error that could lead to mission compromise. Space operators are not accustomed to having a lot of latitude or authority in day-to-day operations, and as a result they typically receive only a minimum amount of training.[737] Space operations are safeguarded by a reliance on inflexible methodologies, detailed checklists, and rigidly hierarchical decision-making. The resultant culture of Space Command is slow, procedural, heavily regulated, and extraordinarily risk-averse.

The cultural necessities of operating in space stand at odds with the cultural necessities of operating in cyberspace. In cyberspace, risk is defined by the window of relevance: the amount of time between the discovery of a vulnerability, the creation of an exploit for that vulnerability, and the discovery

---

[736] All taken from Dean Clothier, "Cyberspace Weapon System Briefing," script for the AFSCP CC Conference, April 27, 2011.

[737] Clothier, interview.

of a patch or security correction that limits the exploit's effectiveness. In other words, the effectiveness of a cyber weapon is typically inversely related to the amount of time that weapon is available for use. The resultant race condition — in which adversaries compete to build both offensive exploits and the defensive patches that mitigate their underlying vulnerability — runs counter to how weapons development works in the physical world, in which the objective destructiveness of a capability typically does not decrease over time.[738] The relationship between risk and time in cyberspace is therefore inversely proportional to the relationship between risk and time in space: risk in cyberspace is mitigated by moving quickly. This speed-oriented and risk-acceptant culture is supported by the fact that the losses that happen due to the compromise of a cyber weapon system are often small and reversible.[739] Outages can be restored, software can be rebuilt, and hardware can be replaced relatively quickly.

The relatively high level of risk tolerance within the cyber community, combined with the fundamentally creative nature of the coding and hacking that comprise the community's cultural core, results in a type of operations that can neither be confined to nor bound by a series of checklists or procedures.[740] Cyberspace is man-made, it is malleable, and it is dynamic; as such, it demands agile thinkers who are quick to adapt to changing circumstances. The potentially rapid pace at which cyberspace operations can unfold, combined with the need for continuous feedback between those who build weapons and those who use them, demands a flat organizational construct that provides maximal autonomy to cyberspace professionals and facilitates rapid decision-making during operations. Moreover, these professionals must be highly trained in order to perform the baseline functions of their career field,

---

[738] I am indebted to Dean Clothier for the insights contained in this paragraph

[739] By "loss" I mean either the compromise of a cyber weapon itself, as in the viral spread of the Stuxnet virus, as well as the collateral damage inflicted by a cyber weapon that hits an unintended target. Saying that these losses are typically small and reversible isn't to say that they cannot also be large and irreversible, but it is to say that they tend not to approximate the level of catastrophic damage approached by the loss of a multi-million dollar satellite or hitting the wrong target with a cruise missile. Cyber weapons are designed to be tailorable. Whereas a cruise missile will destroy what it hits regardless of whether it is launched at the right house, a well-made cyber weapon will typically have a limited effect on a system that it was not designed to target.

[740] Once again, this is a deliberate generalization that deserves additional explanation. Checklists and procedures have their place in cyberspace operations, just as they have their place in the more risk-acceptant conventional operations. However, the difference is that cyberspace is not *dependent* upon such safeguards in the same sense that, say, nuclear missile launch crews are. The relationship between cyberspace operations and the checklists that are typically used to prepare for them is far more interactive and dynamic than other, more slow-moving and risk-averse cultures would allow.

and highly educated in order to adapt to the type of creative problem-solving that their operating environment typically demands.

In spite of these cultural differences, space and cyber shared also shared certain cultural similarities. For one, both communities were accustomed to working with technology. While space leadership did not necessarily have a well-developed understanding of the practice of cyberspace operations, they did at least have an appreciation for the type of technological expertise and technological requirements that such operations demanded. Secondly, in contrast to the fliers of Air Combat Command, space operators did not need to see or touch their weapon systems in order to comprehend their potential. The fact that cyberspace operations are largely invisible did not change space command's perception of their value or effectiveness.[741] As a result, cyber leadership typically faced fewer challenges in justifying their need for resources under space command than they did under their previous regime, even while the aforementioned mismatching organizational constructs may have prevented said justifications from being realized.[742] The limited cultural overlap that existed between the cyberspace and space domains meant that cyberspace operations often received more senior leader attention while under space command than they had underneath the ACC.[743]

However, these limited cultural similarities were not powerful enough to overcome the more significant cultural misunderstandings between the cyber and space communities. The combination of mismatched appetites for risk and timeliness with a lack of reciprocal expertise, resulted in friction between 24AF commanders and their higher headquarters.[744] Space Command had neither the resident personnel to properly train a cyber cadre, nor the staff expertise to understand cyberspace operations. As a result, AFCYBER struggled to develop the right talent while its higher headquarters struggled to properly manage or support the mission. An attempt to remediate the expertise problem with contractors

[741] Clothier, interview.

[742] Ibid.

[743] Ibid.

[744] Elder, interview.

proved insufficient.[745] Resourcing and equipping the cyber mission also became a challenge.[746] To provide one of the more compelling examples, as late as 2014 the space command headquarters did not have any top secret network systems in their command center — in other words, they lacked access to the very systems necessary to properly monitor cyberspace operations.[747]

FIRST CYBERSPACE DOCTRINE: AFDD 3-12

In spite of these difficulties, the Air Force published its first cyberspace operations doctrine in 2010 in *AFDD 3-12: Cyberspace Operations*. Only 60 pages long, this doctrine discusses cyberspace fundamentals; command and organization; and a robust chapter on the design, planning, execution, and assessment of cyberspace operations. It remains informed by joint concepts while taking a unique Air Force perspective, as when it applies the "tenets of airpower in relation to cyberspace operations" or affirms the need for cyberspace operations to be "commanded by an airman who takes a broader view of war, unconstrained by geographic boundaries."[748]

Shortly after the release of AFDD 3-12, the Air Force provided another update to AFDD 1: *Basic Doctrine*. This represented a significant doctrinal update from the previous 2003 version. Information warfare was eliminated as a doctrinal term, and cyberspace superiority was added as one of twelve core Air Force functions. Following with the theme of effects integration that drove the intent of placing AFCYBER underneath 8AF in 2006, the document presented airpower as a unitary concept that equally encompassed air, space, and cyberspace. This conceptual shift was intended to overcome previous presentations of the Air Force as a "collection of tribes broken out in technological stovepipes" in order to

---

[745] Otto, Shanahan, interviews. One former commander described AFSPC as a "structural pass-through," while another described AFCYBER as an "appendage" underneath space command rather than a valued subordinate command.

[746] One former commander of the 67th Network Warfare Wing spent his first year in command under the 8AF/ACC, and his second year under space command. He stated that they had no problem with resourcing under ACC, but began to run into issues after the transition into space.

[747] Otto, interview.

[748] Headquarters, Department of the Air Force, *Air Force Doctrine Document 3-12: Cyberspace Operations* (Washington, D.C.: Headquarters, Department of the Air Force. July 15, 2010), 14, 17.

facilitate the integration of capabilities across all domains.[749] AFDD 1 also attempted to distinguish its own cyber component from those of the Army and Navy by arguing that "the Air Force uses air, space, and cyberspace capabilities to create effects, including many on land and in the maritime domains, that are ends unto themselves, not just in support of predominantly land or maritime force activities."[750]

These doctrinal updates were complimented by a new organizing concept that sought to normalize cyberspace operations to the broader Air Force, and in so doing solve the resourcing problems that stemmed from the previous COMS organizing principle.[751] In the Air Force, nearly all mission capabilities that serve a direct warfighting purpose are defined, organized, trained, and equipped within the weapon system construct.[752] Consideration for program-associated funding stagnates without this weapon system designation.[753] An Air Force weapon system includes mission equipment, a combat-ready crew, and mission support personnel, and mission essential supplies, and provides one or more specific operational capabilities.[754] The absence of any clearly defined cyber weapon systems meant that cyberspace capabilities were effectively invisible to AFSPACE resourcing mechanisms, even while they received increased senior leader attention in comparison to their experience in Air Combat Command.

In order to better posture cyber capabilities to compete for funding and manpower, in 2013 the Air Force approved an AFCYBER request to redefine its cyberspace capabilities as individual weapon systems.[755] The Air Force identified six cyberspace operations weapon systems: Air Force Cyberspace Defense, Cyberspace Defense Analysis, Cyberspace Vulnerability Assessment/Hunter, Cyber Command

---

[749] Headquarters, Department of the Air Force, *Air Force Doctrine Document 1: Air Force Basic Doctrine, Organization, and Command* (Washington, D.C.: Headquarters, Department of the Air Force, October 14, 2011), 12.

[750] Ibid., 13.

[751] Dean Clothier, "Cyber Weapon Systems," Powerpoint briefing, April 20, 2011, slide 2.

[752] Clothier, "Cyberspace Weapon System Briefing Script."

[753] Mark A. Welsh III., Memorandum for HQ AFSPC/CC,"Weapon System Designation Request for Cyberspace Operations Systems," March 24, 2013.

[754] Clothier, "Cyber Weapon Systems," slide 7.

[755] Joseph Wingo et al., "Revamping the Cyberspace Professional Training Model — The Weapon System Construct," *Cyber Compendium: Professional Continuing Education Course Papers* Vol 2 Issue 1 (Spring 2015): 26-33.

and Control Mission System, Air Force Intranet Control, and Cyber Security and Control Systems.[756] This designation allowed the Air Force to more effectively think about, invest in, and resource cyberspace capabilities, and as such had long-term implications for how the Air Force managed its cyberspace operations.[757]

24th Air Force remained under space command until July 2018, when it, along with 25th Air Force and several other direct reporting cyber assets, were moved under Air Combat Command.[758] With cyberspace now a warfighting domain on equal footing with air and space — at least organizationally and doctrinally — it made sense to move the unit responsible for cyberspace effects and the unit responsible for intelligence underneath the command that serves to integrate ISR with combat forces.[759] The effects of this move remain to be seen, but it effectively ended the decade-long schism between Air Force cyber and intelligence forces. In 2019, in a further effort to join the two fields, the Air Force announced that it would merge the 24th and 25th Air Forces into a single, Information Warfare numbered Air Force.[760]

SUMMARY: 2005-PRESENT

The above history suggests three distinct phases of Air Force cyberspace operations. The first, from roughly 1993 to 1999, was an intelligence-led information warfare phase, a largely experimental period in which the Air Force began its initial exploration of doctrine, organizations, and capabilities. The second, from roughly 1999 to 2005, was the information operations phase, still intelligence-led but marked

---

[756] Welsh, "Weapon System Designation Request."

[757] Clothier, interview.

[758] R.J. Biermann, "24th Air Force Joins Air Combat Command, Welcomes New Commander," AF.mil, July 18, 2018, https://www.af.mil/News/Article-Display/Article/1577754/24th-air-force-joins-air-combat-command-welcomes-new-commander/. Direct reporting assets that moved included the Cyber Support Squadron, Network Integration Center, and Spectrum Management Office, which all reported directly to AFSPC, per "Air Force Transfers Cyber Responsibility to ACC," AF.mil, June 7, 2018, https://www.af.mil/News/Article-Display/Article/1544072/air-force-transfers-cyber-responsibility-to-acc/.

[759] The ACC was chosen because it is where the Air Force integrates ISR with combat forces. Per Colin Clark, "Air Force Mulls Merging Cyber, ISR Troops," Breaking Defense, September 20, 2017, https://breakingdefense.com/2017/09/air-force-mulls-merging-cyber-isr-troops/.

[760] "Air Combat Command Announces 24 and 25 AF Merger," Air Combat Command, April 4, 2019, https://www.acc.af.mil/News/Article-Display/Article/1805297/air-combat-command-announces-24-and-25-af-merger/.

by a redefinition of the information space and its relevance to Air Force operations. This phase was accompanied by the creation of updated doctrinal publications and the reorientation of a number of intelligence units to be more information-centric and more responsive to operational needs. The third, from 2006 to the present, was marked by the firm distinction of cyberspace as a warfighting domain, the increasingly aggressive pursuit of autonomy in cyberspace operations and organizations, and the creation of a dedicated cyberspace career field. The third phase culminated in the 2018 consolidation of Air Force cyber and ISR units underneath Air Combat Command, followed by the 2019 decision to merge the 24th and 25th Air Forces into a single Information Warfare Numbered Air Force.[761]

[761] Mark Pomerleau, "How A Merger Will Expand the Air Force's Cyber Edge," Fifth Domain, April 4, 2019, https://www.fifthdomain.com/dod/air-force/2019/04/04/how-a-merger-will-expand-the-air-forces-cyber-edge/?fbclid=IwAR3eW1AWbSfRddkTp9qoVYNIwHz3ki_0r-gntJet-hslavDsELq0zlhktk8.

Table 6. Air Force Cyberspace Organizations 1953-2019

Unit	Date of Formation	Mission	Subordinate To
Air Force Special Communications Center	24 July 1953	A subcomponent of USAFSS which took on the Air Force electronic warfare mission in 1967.	USAFSS
Air Force Electronic Warfare Center (AFEWC)	1 July 1975	A redesignation of the Special Communications Center which expanded the EW mission in the Air Force.	USAFSS/ESC
Air Force Computer Emergency Response Team (AFCERT)	1988	Created in response to the Morris Worm incident of 1988.	Electronic Security Command
Air Force Information Warfare Center (AFIWC)	10 Sep 1993	Formerly AFEWC. Develop IW tools, tactics, and techniques that could be transferred to warfighting commands. Combined EW and cryptologic security functions.	Air Intelligence Agency
609 Information Warfare Squadron	1 Oct 1995	Conceive, develop, and field IW capabilities in support of a numbered air force. Defend the 9AF and central command from information attacks. Deactivated June 1999.	9th Air Force (AFCENT)
67th Information Operations Wing	1 Aug 2000	Executed the global IO mission for the AIA	Air Intelligence Agency
67th Network Warfare Wing	5 July 2006	Formerly 67th IO Wing	Air Combat Command
Air Force Information Operations Center (AFIOC)	1 Oct 2006	Formerly AFIWC	Air Intelligence Agency/AFISRA
AFCYBER (P)	1 Nov 2006	Provide forces to conduct offensive and defensive operations through the electromagnetic spectrum; fully integrate with air and space operations.	8th Air Force/Air Combat Command
Air Forces Strategic (AFSTRAT)	18 Aug 2009	Formerly AFCYBER(P). Deliver full-spectrum, global cyberspace capabilities for the Air Force, the joint force, and the nation.	Air Force Space Command
24th Air Force (AFCYBER)	7 Dec 2010	Formerly AFSTRAT. Deliver full-spectrum, global cyberspace capabilities and outcomes for the Air Force, the joint force, and the nation.	Air Force Space Command
688th Cyberspace Wing	13 Sep 2013	Formerly AFIOC. Dedicated to tactical communications, engineering and installation capabilities, defensive cyber operations, and network operations across the Air Force.	AFCYBER
67th Cyberspace Wing	1 Oct 2013	Formerly f 67th Network Warfare Wing. Conduct network operations, defense, attack, and exploitation in support of the Air Force, combatant commands, and national agencies.	AFCYBER

Cyberspace Personnel Development

How did the Air Force manage its cyberspace personnel through each of these distinct periods of reorganization? Until the creation of a dedicated cyber career field in 2009, personnel assigned to cyberspace units were managed on an individualized basis at the unit level, rather than by any central Air Force strategy.[762] For example, those assigned to the 609 IWS were hand-selected from a cross-section of disciplines, to include communicators, engineers, intelligence personnel, and even pilots who were expected to ground the new field of information warfare in an operational perspective. The transfer of 609th capabilities into various intelligence organizations after the unit's disbandment in 1999 resulted in a cyber mission that was populated largely, if not entirely, by signals intelligence professionals. However, the lack of a specialty code for what were then called information operations meant that there was no way to centrally manage the Air Force's cyber talent. Absent a standard talent management system, commanders often relied upon grassroots recruitment efforts to identify and then assess qualified airmen from units across the Air Force.[763] Airmen who successfully passed these assessments, and who could secure release from their host units, were able to transfer into a temporary cyberspace operations assignment.[764]

This individualized approach allowed for the identification of appropriately high quality talent, but it did not allow units to retain this talent for very long.[765] Since cyber assignments were not part of a traditional intelligence career path, qualified airmen would eventually have to return to a more standard job. The lack of a cyber career field thus affected not only talent management at the individual level, but

---

[762] Lynn M. Scott et al., "Human Capital Management for the U.S. Air Force," (Santa Monica, CA: RAND Corporation, 2010), 16.

[763] One former commander of the 67th Network Warfare Wing, for example, would screen prospective candidates through an interview, followed by an aptitude test sent to their home station. Those who achieved a sufficiently high score on the aptitude test were sent to the National Security Agency for a second, more rigorous test. If they passed, they were brought into the unit through a by-name request.

[764] Of note, the transition of many of these intelligence organizations into information operations squadrons in the early 2000s led to some discussion as to whether the Air Force should create an information operations career field. Such discussion was marred by a general inability to agree upon the balance to be struck among the cognitive and technical components of what the Air Force understood to comprise information operations. From Timothy P. Franz, et al., "Defining Information Operations Forces: What Do We Need?" Air and Space Power Journal, Vol 21 No 2 (Summer 2007): 53-67.

[765] Paul D. Williams, "USAF Cyber Capability Development: A Vision for Future Cyber Warfare & A Concept for Education of Cyberspace Leaders" (Thesis, Air University, 2009), 4.

continuity of expertise at the unit level, which made it difficult for cyber units to develop any long-term depth in mission proficiency.

A CYBER CAREER FIELD AND TRAINING PROGRAM

In 2006, in order to address this problem, the Secretary and Chief of Staff directed the Air Force Headquarters personnel section to develop a plan for the creation of a cyber career field.[766] This directive resulted in the creation of the aforementioned *Roadmap for the Development of Cyberspace Professionals* in 2008, whose recommendations ultimately never materialized. Simultaneous to the effort to outline the skills that would be required for a professional cyber workforce, the Air Force began to develop a cyber training program. At the time, the closest thing the Air Force had to any formalized cyber training was Basic Communications Officer Training, a communications qualification course for those in the 33S career field. Originally three months long, progressive funding cuts combined with the increasing consolidation of communication specialties reduced the course to a scant five weeks by 2008.[767]

Since a five week, substantively empty communications course was insufficient to train the next generation of cyberspace experts, the Secretary of the Air Force directed the creation of a new cyber officer cadre with new operations-centric qualification training.[768] The result of this directive was Undergraduate Network Warfare Training (UNWT). Created in 2007, the course was intended to standardize proficiency among all personnel assigned to the cyber mission — officers, enlisted, and civilians alike, regardless of their underlying Air Force specialty.[769] It was initially run by the 39th Information Operations Squadron out of Hurlburt Field, Florida due to insufficient cyber expertise within the Air Force's Air Education and Training Command (AETC). The course was five months long, highly

---

[766] Moseley and Wynne,"Establishment of an Operational Command for Cyberspace."

[767] Clothier, interview. Also, the continuous consolidation of Air Force communications specialties into singular, over-generalized officer career fields dramatically reduced the need for substantive technical training. See Golembiewski, "From Signals to Cyber."

[768] Clothier, interview.

[769] Matthew G. Beach, "Managing Cyber Operator Training Curriculum" (Thesis, Air University, 2010), 21.

technical, and partially classified. It was intended as a practical, hands-on introduction to the skills necessary for cyberspace attack, defense, and reconnaissance.[770] In 2008, UNWT transitioned into the Undergraduate Cyber Training course (UCT). The UCT was officer only, and it was now run by the AETC, which allowed for more resources and a greater personnel throughput.

On 1 November 2009, the Air Force unilaterally transferred 43,000 enlisted airmen and 8,800 civilian personnel from the communications field into a new Air Force Specialty Code for cyberspace.[771] This move was not so much the bottom-up creation of a new cadre of cyber specialists as it was the semantic rebranding of an existing career field. All 3,000 33S officers became 17-series cyber officers overnight, with the intent that each would complete cyber-specific retraining no later than 2011.[772] With this move, the Air Force became the first of the military services to have its own dedicated cyber warfare career field.

Officers

The Air Force currently has five career fields most closely associated with the cyber mission: 14N, 17D, and 17S for officers, and 1N4 and 1B4 for enlisted. Of note, the Air Force does not have warrant officers, a population which the Army has relied upon heavily for its cyberspace and technical expertise.[773] While the 14N, 17D, and 17S career fields all make contributions to cyberspace, there are significant differences in the purpose, culture, and management of each.

As Air Force intelligence officers, 14Ns are trained to be generalists first, with the opportunity to specialize in one of six intelligence disciplines over the course of their career: human intelligence,

---

[770] Beach, "Managing Cyber Operator Training Curriculum."

[771] Rita Boland, "Military Branch Undertakes Massive Troop Conversion," Signal Magazine, Feb 2, 2010.

[772] 3,000 officers taken from Katrina A. Terry, "Overcoming the Support Focus of the 17D Cyberspace Operations Career Field" (Thesis, Air Force Institute of Technology, 2011), 1. That each would complete retraining by 2011 taken from Boland, "Military Branch Undertakes Massive Troop Conversion."

[773] The Army uses warrants to fill the expertise gap lost by its policy of maintaining a generalist officer corps. The Air Force, given that it expects its officers to be technical experts already, has maintained the position that it has no such need for the warrant officer function. The high technical requirements of the cyberspace mission have challenged the Air Force position on warrants, particularly given the lack of incentives for technically-qualified enlisted to continue to do their jobs.

geospatial intelligence, measures and signatures intelligence, open source intelligence, technical intelligence, and signals intelligence.[774] 14N initial training takes place with the 17th Training Wing at Goodfellow Air Force Base, Texas. Training provides a broad overview of the intelligence career field with separate blocks on each intelligence discipline. While the 14N specialty code does indicate an Airman's skill level in a particular discipline — with a 14N3 rated higher than a 14N1, for example — it does not indicate which of the six disciplines an Airman has mastered. Furthermore, there is no separate discipline for cyber-related intelligence. Officers receive a two-day segment on cyberspace out of a six month total course with 1,049 hours of instruction. By comparison, the air block of instruction — comprising study of air forces, surface-to-air forces, and integrated air defense systems — lasts four weeks, or 174 total hours. The broad, overview nature of the course makes it difficult to assess cyber aptitude for follow-on assignments.[775] Only 2.9 percent of 14N officers have a cyber-related degree, and roughly two-thirds have degrees outside of the hard sciences.[776]

Those 14Ns who do receive a cyber-related assignment, particularly those en route to Cyber Command, will undergo an additional year's worth of on-the-job training before being mission qualified to conduct intelligence activities in the cyber domain. 14Ns are permitted to attend higher level hacking courses later in their careers, but the lack of a skill identifier for these courses prevents higher USAF from tracking who has attended these courses while simultaneously lowering the incentive for intelligence professionals to pursue them. While cyber-skilled intelligence officers are manually tracked by the 25th Air Force, the lack of a cyber skill identifier, combined with an institutional preference for broadly trained 14Ns who are prepared for future leadership, can and does lead the Air Force Personnel Command to move these officers elsewhere after only one tour in cyberspace.[777] In other words, cyber-savvy intelligence

---

[774] Brauner et al. "Improving Development and Utilization of U.S. Air Force Intelligence Officers."

[775] Panayotis A. Yannakogeorgos and John P. Geis II, *The Human Side of Cyber Conflict: Organizing, Training, and Equipping the Air Force Cyber Workforce* (Maxwell Air Force Base, AL: Air University Press, 2016), 93.

[776] Ibid.

[777] Clothier, interview.

officers are managed according to the best interests of the intelligence community, which are not always congruent with the best interests of cyber.

Air Force cyberspace officers, on the other hand, are tracked in one of two specialty codes: 17S cyber warfare operations officer, and 17D cyberspace operations officer.[778] 17Ds are more akin to classic communications officers with general information technology expertise, and they comprise the bulk of the Air Force's 17-series career field.[779] As such, they build, maintain, and defend Air Force networks, and are usually assigned at or near operational flying units. In contrast, 17Ss work in support of joint, national, and broader Air Force cyberspace objectives, and are rarely co-located with fliers. Both the 17S and 17D officers undergo the same initial qualification training before branching off into specialty, mission-specific training programs.[780] Training for 17Ss consists of the Undergraduate Cyber Training Course (UCT), which is 115 days of instruction (920 academic hours/24 weeks) at Keesler Air Force Base, Mississippi. The course is split between Air Force and joint instructional topics. Phase one of the course provides an introduction to fundamentals of the cyberspace domain; cyberspace operations; doctrine; organizations, roles, and responsibilities; network fundamentals; and deployed communications systems. Phase two builds on phase one with an increased focus on protecting and defending a network. A third phase with OCO- and DCO-specific instruction for 17S officers was added in 2015.[781]

After initial qualification training at UCT, 17S officers attend the eight week Intermediate Network Warfare Training course (INWT) at the 39th Information Operations Squadron (39 IOS), with

---

[778] Air Force cyber officers were managed within a single 17D AFSC for the first several years of their existence, with two possible "shreds:" 17DXA, or cyberspace operators, and 17DXB, or network maintainers. Only 8.5 percent of the original officer allocation fell into the former category of cyberspace operators, yet both shreds received similar initial training (Phillips, "Engendering Cybermindedness"). However, there was no distinction between offensive and defensive cyberspace operators, which meant that officers were rotated among different types of positions with the expectation that they would perform all equally well. The reality was described rather brutally by one 2015 study: "The 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." See Matthew T. Hyland, "Operationalizing the 17D Workforce," *Cyber Compendium: Professional Continuing Education Course Papers* Vol 2 Issue 1 (Spring 2015): 2-8.

[779] 89% of 17s are 17Ds, while on 11% are 17S. Yannakogeorgos, *The Human Side of Cyber Conflict*, 105.

[780] For detailed information on these training programs, see James E. McCarthy, "Training for Cyber Operations," Air Force Research Laboratory Report, April 2018.

[781] Robert M. Lee, "Disruptive by Design: Saving the Air Force Cyber Community," Signal Magazine, February 1, 2015.

follow-on system qualification as needed. The entire process for a 17S to become fully mission qualified takes at least 66 weeks, with an additional 44 weeks of coursework and on-the-job training for those assigned to CYBERCOM national mission teams. Like pilots, Air Force cyberspace operators face challenges in remaining operationally current, particularly after a non-operational assignment. As such, they must undergo keyboard requalification as needed.[782] As of March 2014, the 17-series career fields had 2,459 authorizations, of which 2,291 were filled.[783]

Enlisted

Enlisted cyberspace personnel are managed under one of two career fields: 1B4, which is the enlisted counterpart to the officers' 17S, and 1N4, which designates the Air Force's cyberspace intelligence specialists. The 1B4 career field is critical to the success of USAF cyberspace operations. Retention for this field is generally high, ranging from 93% among those with more than eighteen years of service to 71% among those with between six and ten years of service.[784] Retention issues usually arise when those on mission receive a routine off-mission assignment, such as to a staff headquarters or to serve as an instructor. The duplication of effort present between the 17S and 1B4 career fields causes additional retention issues by lowering the incentive for enlisted airmen to stay enlisted. The Air Force's propensity to employ officers as its technical operators — the "pilots" of cyberspace — means that enlisted airmen could commission as officers and be able to perform the same jobs that they previously enjoyed at a lower pay grade.

In contrast to the 1N4 intelligence field, 1B4 is a "retrain only" specialty, meaning it does not take initial entry personnel. Individuals wishing to switch into the 1B4 field must have prior Air Force experience in another field, with the 3D cyberspace systems field serving as the most popular source of

---

[782] This problem has been less relevant to Army cyber officers, since far fewer serve in "on keyboard" jobs as compared to the Air Force.

[783] Yannakogeorgos, *The Human Side of Cyber Conflict*, 97.

[784] Ibid., 67-68.

1B4 recruits. Initial training consists of a 12 unit program of 679 academic hours over 85 training days (16 total weeks). This training begins with an overview of skills needed for cyberspace defense, such as the theoretical principles of network warfare and information assurance. Trainees are also introduced to various operating systems, network exploitation, industrial control systems, and cyber threats and defense before progressing to a capstone event of fighting through a cyber attack.

After the initial course, students attend an eight week INWT at Hurlburt with the 39 IOS. This course helps students to build their foundation in network programming and operations through various blocks of instruction: how to build a virtual network, incident response and forensic analysis, master hacking and attacking techniques, cyber operations strategy and mission planning, responsibilities of the network warfare operations cell, offensive cyber operations against IP and functional networks, and understanding the chain-of-command for network defense. 1B4s then report to their gaining unit for up to two years of on-the-job training.[785]

While 1B4s serve the Air Force's enlisted cyberspace operations function, 1N4s, or Highly Specialized Cyberspace Intelligence Analysts, fulfill the Air Force's cyberspace intelligence needs. This specialty acts as the enlisted corollary to cyber-trained 14Ns, albeit with a dedicated cyber focus. The 1N4 specialty is open to direct accessions, and does not require prior Air Force experience to join. 1N4s undergo 106 days of initial training before the 120 day Joint Cyber Analysis Course (JCAC) at Corry Station, Florida, for a total of one year of training before they arrive at their first unit. The Air Force, like the other services, also sends language analysts to support CYBERCOM, but these individuals receive little additional cyber training. In addition to the above, the Air Force also has eleven cyber support specialty codes for its enlisted personnel. These Airmen receive a degree of cyber-familiarity in their training, but are not usually associated with the national cyber mission.

Personnel Backgrounds

---

[785] Yannakogeorgos, *The Human Side of Cyber Conflict*, 106-113.

How are these enlisted and officer cyber specialists shaped before they join the Air Force? Where do they come from, and what do they study? A 2015 study uncovered a severe lack of cyber-related degrees within the cadre of 17D network operations officers, 14N intelligence officers, and each of the 1B4, 1N4, and 3D enlisted career fields.[786] Of those assessed into the cyber career field over the time period of the study, only thirty five percent had a cyber-related bachelors degree. The majority of 17-series officers come from ROTC programs, with the U.S. Air Force Academy and Officer Training School (OTS) taking second and third. As of 2015, OTS produced about twenty seven percent of the Air Force's cyber officers, a number which has had a tendency to fluctuate in response to cycles of economic boom and bust. Furthermore, only twenty six percent of OTS accessions are from ABET-accredited schools, resulting in an inferior candidate pool from which to identify cyber aptitude.

This Air Force accessions pattern is the opposite of that found in the U.S. Army, where the blueprints for cyber branch were created in the Electrical Engineering and Computer Science department at West Point, and each of its first two cyber cohorts were comprised exclusively of West Point lieutenants. Furthermore, while many of the ROTC graduates who enter the cyber field have some background in computer science or electrical engineering, few of these officers have come from top universities. Between 2009 and 2013, for example, the Air Force received between just 2 and 5 accessions from top universities per year.[787]

While the Air Force Academy has been tasked to produce 50 17Ds per year, the Air Force itself has proven reluctant to provide explicit guidance on how these 17s should be produced. Electrical Engineering and Computer Science, the two most promising academic backgrounds for future cyber officers, are the third and fifth least popular majors at USAFA, respectively.[788] Those with a preference for

---

[786] Yannakogeorgos, *The Human Side of Cyber Conflict.*

[787] Ibid., 161.

[788] In contrast, computer science is a popular major at West Point. It's cyber-focused corollary, Cyber Science, is a similarly popular major at the Naval Academy.

17D generally have a lower GPA than other non-rated line officer career fields, and the 17D career field is among the last choices for non-rated officers.

One can speculate as to the cultural origins of this difference in distribution between West Point and USAFA cadets: whereas the Air Force encourages its pilots to have undergraduate technical degrees, the Army's cyberspace branch is one of the few options for cadets who are both technically proficient and operationally oriented.[789] In contrast, the cyber career field might appear as less of a unique operational opportunity to a service which has technological appreciation ingrained into its DNA. It is feasible to speculate that the cadets who branch cyber at West Point come from the same population — with a mix of both technological and operational leanings — that would otherwise become pilots at USAFA.[790] Furthermore, many USAFA cadets do not view the 17-series career field as a good long-term career choice. The Air Force's decision to consolidate the communications and cyber functions into a single career field, albeit one with two different alpha-numeric designations, has many cadets who desire to become cyber operators worried that they may get stuck as a squadron communications officer instead.[791]

On the enlisted side, the general difficulty of identifying the skills necessary to make a good hacker has caused the Air Force (along with the Army and Navy) to look for ways to augment the Armed Services Vocational Aptitude Battery (ASVAB), the test that determines job placement for recruits, in order to identify potential cyber operators. In 2014, the 711th Human Performance Wing developed a cyber test that emphasizes four content areas: networking and communications, computer operations, security compliance, and software programming and web development.[792] However, while this test can identify those with a knowledge base in computer science, it does not identify the more abstract qualities required for offensive and defensive cyberspace operations. As of 2015, the Air Force was in a joint effort

---

[789] Phillips, Jeffrey A. "Engendering Cyber-Mindedness in the United States Air Force Cyber Officer Corps," (Thesis, Air University, 2011).

[790] Panayotis A. Yannakogeorgos, telephonic interview with the author, September 26, 2018.

[791] Robert M. Lee, "The Failing of Air Force Cyber," Signal Magazine, November 1, 2013.

[792] Yannakogeorgos, *The Human Side of Cyber Conflict*, 53.

with the Army to develop just such a test.[793] More recently, the Air Force has undergone efforts to reach beyond the traditional cyberspace recruiting pools in order to identify those service members in other fields, such as logistics and maintenance, who might have the capacity to learn cyberspace operations.[794]

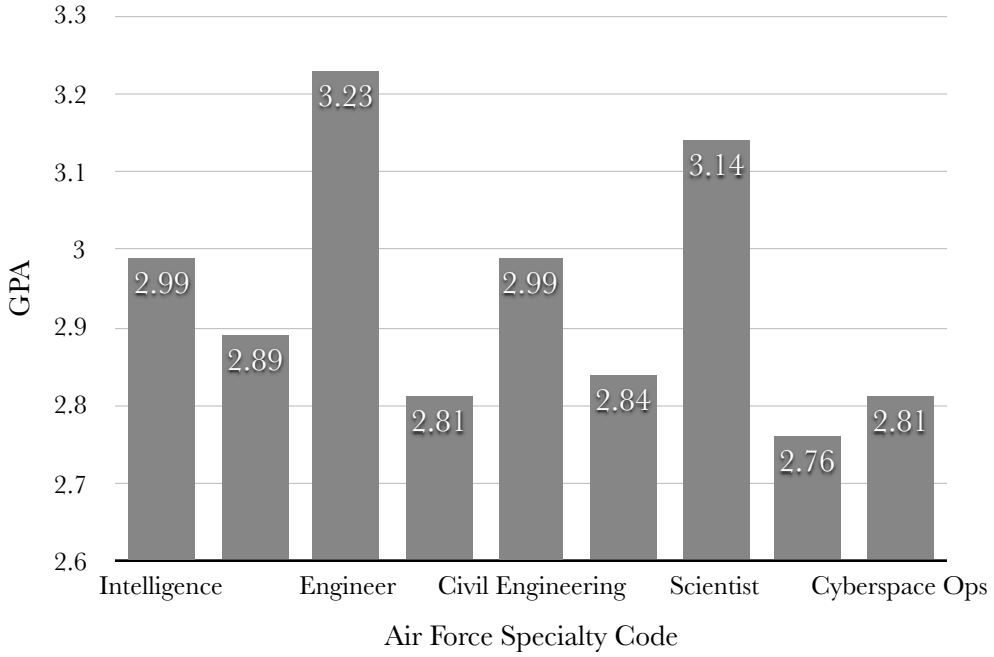

Fig 1. USAFA non-rated Preference AFSC and GPA, August 2014[795]

[793] Yannakogeorgos, *The Human Side of Cyber Conflict*, 54.

[794] Lauren C. Williams, "Air Force to Roll Out New Cyber Job Categories," FCW, April 3, 2019, https://fcw.com/articles/2019/04/03/usaf-cyber-job-categories.aspx?fbclid=IwAR2fEh2Cce71RfDPItFIr54YFvZcNsOE1VCVFIHKLx3Hi6YBLE_FIObRq1A.

[795] Data taken from Yannakogeorgos, *The Human Side of Cyber Conflict*.

CHALLENGES

What all of these accession patterns suggest is that the Air Force personnel management strategy in cyberspace has lagged behind its operational ambition.[796] As such, it is "losing the battle of perceptions with the other services" that have placed a greater emphasis on educating cyber professionals through things like cyber research centers at their service academies and institutes of higher learning.[797] The Army Cyber Institute at West Point, for example, was created in 2012 to provide strategic insight and advice on cyber-related issues affecting the Army, a full two years before the creation of an Army cyber branch. In contrast, the Air Force Academy did not establish its first cyber research center until 2015.[798] In another example, the Air Force Research Laboratory (AFRL) founded the ACE Cyber Security Boot Camp in 2003 to develop ROTC cadets into future cybersecurity leaders. However, this lab receives no Air Force funding — although it has received funding from the Army to work on Army issues.

The Air Force's perception battle extends to its own institutional self-perception of the cyberspace domain. The Air Force added "cyberspace" to its mission statement in 2005 and incorporated it into its core service doctrine as far back as 1997, but it still struggles to shake the notion of cyberspace as an enabling function rather than a fully operational domain of warfare.[799] The fact that the vast majority of cyberspace officers do not actually engage in cyberspace operations, but do the work of network maintainers, does not help the cause of attempting to place cyberspace on equal operational footing with air and space. This perception demoralizes cyberspace operators and disincentivizes properly qualified individuals from entering the ranks.[800]

---

[796] A 2015 study found that the 17D end strength faced steady reductions in the face of increasing cyberspace operational requirements. See Hyland, "Operationalizing the 17D Workforce."

[797] Yannakogeorgos, *The Human Side of Cyber Conflict*, 191.

[798] Ibid.

[799] Terry, "Overcoming the Support Focus."

[800] Yannakogeorgos, *The Human Side of Cyber Conflict*, ch. 7. Echoed in Lee, "The Failing of Air Force Cyber," and "Disruptive by Design."

The institutional challenges of accepting cyberspace as a domain on equal footing with air and space suggests that, in spite of its doctrinal rhetoric, there are certain technological frontiers which the service culture will be reluctant to cross. There is something real and compelling in the mythological image of a pilot taking to battle in the sky; anything which attempts to approximate this image, without the associated risk of personal danger, will be only reluctantly accepted by the dominant service community and the broader cultural norms which they dictate. This cultural phenomenon was evident in the service friction that accompanied the rise of remotely piloted aircraft, and it is being replicated in the Air Force's efforts to build a reliable cohort of cyberspace professionals. While the Air Force is a technologically-dependent service, it still retains a sense of itself as a warfighting service comprised of its own unique brand of warfighters. At its cultural core, it does not want to be seen as simply a service which operates technology, safe from the risks and dangers of actual combat.

The necessary efforts required to overcome these cultural frictions and to operationalize cyberspace as a credible career field have not been helped by the Air Force's decision to transition the communications career field (formerly 33S) into the 17XX career field.[801] While the DoD has three broad categories of cyberspace operations, with each requiring a different skill set — offense, defense, and network support — the Air Force merger of communications with cyber only enhanced the confusion over what constitutes a cyberspace operator. The merger of the communications and cyber communities did not eliminate the communications mission; instead, it assigned a single personnel community to fulfill two very different operational requirements without providing adequate training in operations or operational planning.[802] Evidence suggests that this transition did not effectively take into account the different demands of each mission and the different mindsets required to succeed in them.[803]

---

[801] Hyland, "Operationalizing the 17D Workforce."

[802] Joy M. Kaczor,"The Cyberspace Domain: Recommendations to Change Mindsets and Air Force Culture," *Cyber Compendium: Professional Continuing Education Course Papers* Vol 1 No 2 (Winter 2013): 98-104.

[803] As one author wrote in 2013, "this change did not effectively take into account that cyber and communications are two distinct fields and should be entirely separate communities." Lee, "The Failing of Air Force Cyber." See also Kaczor, "The Cyberspace Domain," and Jefferey A. Phillips, "Engendering Cyber-Mindedness in the United States Air Force Cyber Officer Corps" (Thesis, Air University, 2011).

Consider that only about fifteen percent of each UCT class of initial entry 17-series officers are assigned to an operational cyber mission, or two out of every fifteen students.[804] Because eighty-five percent of each course neither needed the in-depth technical understanding required for cyberspace operations, nor likely had the technical aptitude to understand it, the bulk of the course material was originally designed so that the majority of students who went on to communications missions could pass.[805] This dichotomy resulted in an ever-expanding quantity of Air Force personnel who were called cyber operators, but who lacked the technical skills which were expected of the name.[806] Rather than supporting the elevation of cyberspace as an independent warfighting function with its own separate warfighting class, the Air Force's decision to carve a cyberspace cohort from its communications population only furthered the long-held assumption that any Airman who touches a computer is automatically a cyberspace warrior.[807] The result was enhanced service-wide confusion over what constitutes a cyberspace operator.

In addition to inefficient training models and confusion over who possesses actual cyber skills, the merging of communications and cyber resulted in a paradigmatic clash over how best to prepare and promote leaders within the branch.[808] The Air Force has always held a distinction between its operational and its support personnel. In flying, there is a strong historical and cultural norm that treats mission proficiency as a prerequisite for leading a unit. If you cannot fly, you cannot lead. Since the Air Force considered space as much a part of its operational purview as air, it used this same model of technical proficiency first, leadership second, for the space command which eventually took over the Air Force cyber mission.[809] As a result, the Air Force applied the same expectation of technical proficiency to its

---

[804] McCarthy, "Training for Cyber Operations."

[805] Lee, "The Failing of Air Force Cyber."

[806] Hyland, "Operationalizing the 17D Workforce."

[807] Reiterated by John Chezem, "Air Force Cyber Mission Success Depends on Cultural Change," Signal Magazine, October 1, 2015.

[808] Clothier, interview.

[809] Ibid.

cyberspace officers as it always had to its pilots: if you are not qualified to be an on-net operator, for example, then you are not qualified to be a cyber mission team lead.

The impact of this framework can be seen in how the Air Force has managed its service billets in Cyber Command. While each service was given responsibility for manning, training, and equipping personnel for its designated cyber teams, they had wide latitude in how they selected and managed those team members, and in who they put in what positions. The Air Force's cultural and historical expectation that officer leaders must have technical proficiency led to a service decision to expand the number of officer billets on their cyber mission teams, relative to the other services, in order to cultivate the type of technical expertise that was expected of its eventual team leaders.[810] Thus, under the influence of space command and the aviation legacy that preceded it, the Air Force made the early decision to groom its cyberspace officers as they would any other operational line function, building them as technical experts first and leaders second.

This air-centric management style contrasts with the personnel management preferences found in the Air Force's mission support branches, such as the communications branch from which the cyber force structure was eventually created, and the intelligence branch which continues to feed select 14Ns into the cyber mission. The Air Force treats these mission support career fields much in the same way that the Army treats its officer corps more generally, wherein too much technical expertise is seen to detract from an officer's ability to maintain the broad perspective required to make decisions. In mission support fields, the officer is a manager who leads technical experts; he is not expected to maintain a high degree of technical proficiency himself, nor is he expected to pursue assignments that would otherwise cause him to specialize. Thus, both communications and intelligence officers are managed in a way that provides maximum exposure to as many different missions and to as many different major commands as possible in order to ensure a wide breadth of experience. This pattern is, of course, antithetical to how the Air Force operational core views leadership and officer development. These differences resulted in competing

[810] Clothier, interview.

paradigms over how best to prepare and promote leaders within the 17XX career field, as well as tension within the different cadres at the earliest iterations of the Air Force's cyber schoolhouse.[811]

Explaining Outcomes: The Role of Subcultures

INTELLIGENCE AND ELECTRONIC WARFARE

Why, then, did the Air Force choose to build its cyber population off the back of a less technical cadre of communicators? What led to the decision to use its network maintainers as the foundation for a branch of network destroyers, rather than the electronic warfare, intelligence, or space personnel who were equally involved in the Air Force's early history with information warfare? Furthermore, given the original proposals of the 2008 *Roadmap for the Development of Cyberspace Professionals*, what explains the absence of electronic warfare and intelligence personnel from the final cyberspace design?

The immediate answer to this question can be found in the aftermath of the Air Force's 2007 incident of nuclear mismanagement. This incident, and the pausing effect that it had on the Air Force's cyberspace momentum, presented an opportunity for the commander of Air Combat Command to reverse certain cyber-related decisions that were seen to detract from the command's combat power. Recall that the original plan for AFCYBER (P) would have required Air Combat Command to surrender its electronic warfare assets. While this move may have made sense to those who considered electronic warfare and the electromagnetic spectrum to be natural extensions of cyberspace, it was less intelligible to those for whom electronic warfare was the first line of defense for combat aircraft. When the Air Force halted further cyberspace development in order to get its nuclear house in order, Air Combat Command regained control over its electronic warfare assets and prohibited its electronic warfare officers from moving into the new cyber warfare career field.[812] These two moves dramatically reduced electronic warfare's involvement in future cyberspace development.

---

[811] Clothier, interview.

[812] Ibid.

The intelligence community, equally unhappy with the *Roadmap's* final arrangement, offered a similar scorched earth response. When the intelligence community's original proposal to take full control of cyberspace operations was rejected, leadership reluctantly accepted a counter proposal that entailed the transition of one intelligence squadron to AFCYBER (P) and 300-500 intelligence personnel into the new cyber warfare career field. When the nuclear incident halted cyberspace momentum, General John Kolziol, the then-commander of AFISRA, took the opportunity to reverse both of these decisions.[813] The intelligence squadron that was promised to AFCYBER (P) would remain in AFISRA, and the intelligence personnel who were previously identified to become cyber warfare officers would no longer be allowed to make the transition. Thus, an unintended consequence of Air Force nuclear mismanagement was the elimination of electronic warfare and intelligence community involvement with the process of cyberspace personnel development.

INFORMATION WARFARE

However, a more comprehensive answer to the question of why these two communities were so eager to withdraw in the first place requires more in depth historical analysis. Two places offer clues as to the final answer: in the relationship between cyberspace and the intelligence community, and in the history of the communications field itself. During and after Vietnam, when emerging technology included surface-to-air missiles and integrated air defense systems, the Air Force dramatically increased its investment in electronic warfare capability. This investment resulted in the creation of the Air Force Electronic Warfare Center in San Antonio, Texas.[814] While the organization was led by electronic warfare officers, the preponderance of AFEWC personnel came from the intelligence community in a reflection of the close relationship between the two fields.[815]

---

[813] Clothier, interview.

[814] See Price, *History Vol III,* for a comprehensive history of these and other decisions.

[815] Clothier, interview.

In 1993, the AFEWC became AFIWC, the Air Force Information Warfare Center, as the service expanded its original thinking on concepts of command and control warfare to encompass a broader set of capabilities.[816] Comprised of a mix of electronic warfare, intelligence, engineering, and communications personnel, AFIWC was kept under the administrative care of the Air Intelligence Agency. However, it was viewed as a distinctly non-intelligence organization that was left to its own devices and kept highly classified. The AFIWC thus became its own counter-culture within the Air Force operational universe.[817]

Tension between the AFIWC information warfare pioneers and the intelligence community that sheltered it centered around a single core question: is information warfare an extension of intelligence, or is it something completely different?[818] If it was something completely different, so the thinking went, then information warfare possessed the latent ability to change the nature of warfare itself by enabling what Alvin Toffler famously called "anti-war" to prevent full on nation state to nation state conflict.[819] The IW community believed in this vision, and so saw itself as a unique community that could potentially become the next profession of arms.

If, however, it was the former, and merely an extension of intelligence, then there was no need for a separate information warfare organization, complete with its own doctrine, capabilities, and operational independence. Whether or not those who served within AFIWC should be considered EW/intel/space/communications personnel with an information warfare specialty, or information warfare personnel in a field all their own, became the core question for each community involved in this early organization.[820] Fundamentally, this was a question of whether or not to treat information warfare as its own line-distinctive combat arms profession, equal in importance to the Air Force's pursuit of dominance in air and

---

[816] Healy, "From Cybernetics to Cyberspace."

[817] Clothier, interview.

[818] Ibid.

[819] Alvin and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century* (Little, Brown & Company, 1993).

[820] Clothier, interview.

space, or merely a support function that enabled such air and space dominance. This debate continued when the Air Force removed information warfare from its doctrinal lexicon and adopted the cyber terminology familiar today.[821]

SPACE

To be fair, this core versus support question was something that all services had to consider as they expanded into the cyberspace realm. However, the Air Force diverged from the other services in a substantial way when it chose to move cyberspace operations to Air Force Space Command in 2008. In early October 2008, still reeling in the aftermath of the 2007 nuclear incident, the new Air Force Secretary and Chief of Staff announced that USAF would establish a component numbered air force and assign it to AFSPC to "plan and conduct cyberspace operations in support of combatant commands and maintain and defend the Air Force enterprise network."[822] The result of this decision was the 24th Air Force, or Air Forces Cyber (AFCYBER). Space command became the home of AFCYBER for the next ten years.

The most important aspect of the 2008 organizational shake-up is the manner in which it completely divorced the cyber community from Air Force Intelligence. Moreover, the movement of cyber command underneath a space higher headquarters was something of an affront to the intelligence community that had spent so many years as the unheralded stewards of nascent Air Force cyberspace capability. While intelligence personnel remained in AFCYBER, and select cyber personnel remained in AFISRA, cyberspace operations nevertheless became completely distinct from intelligence in planning, execution, and chain of command. This created a unique AFCYBER culture that took its cues from the

---

[821] In 2003, the Air Force Doctrine Document (AFDD) 1, *Basic Doctrine*, was the last major doctrinal pub to use the phrase "information warfare." By this point, IW had become the more innocuous-sounding Information Operations, and was comprised of influence operations, electronic warfare, and network warfare. Information warfare was officially eliminated with the 2005 release of AFDD 2-5, *Information Operations*, which encompassed the Air Force's most specific doctrine of what were then called network operations to date. In 2010, the Air Force released its first doctrinal publication on cyberspace operations with AFDD 3-12, *Cyberspace Operations*.

[822] "History of the Twenty-Fourth Air Force and 624th Operations Center," 24th Air Force Heritage Pamphlet, 24 AF Office of History, January 17, 2014.

space community rather than from the intelligence community.[823] More importantly, this schism between cyberspace and intelligence created an opportunity for the communicator population to cross from mission support into core operations, which was the realization of a decades-long ambition to seek a more prominent operational role in the Air Force hierarchy.[824] The historical and cultural baggage of the communicator mission support background then became intertwined with existing cyber operational perspectives and management practices.

COMMUNICATIONS

Given the evident friction between the communications and cyber communities, what was it about the history of the communications career field that made it seem a suitable match for cyberspace? In the early days of the Air Force, communications emerged as a highly technical career field, in which officers were technical authorities who specialized in radio, radar, telephone, and computer systems. By 1945, for example, the communications officer family was comprised of 36 distinct military occupational specialties ranging from radar officer to telephoto officer to cryptographic security officer.[825]

The arrival of computers as a mainstay of Air Force operations in the 1960s led to a concurrent need for a new type of communication specialist, one who understood things like data automation and computer programming. However, the Air Force did not know where to house this new family of expertise. While the communications career field dealt with complex electrical systems, computers at the time were so specialized that each functional community often needed to grow its own specialists who were only familiar with the particular machines that they used. In the absence of a specific computer career field, the Air Staff decreed that "functional areas such as Logistics or Personnel would do their own automated systems design and be responsible for their own machine programming of the automated

[823] Clothier, interview.

[824] Ibid. Decades-long ambition taken from Golembiewski, "From Signals to Cyber," 6.

[825] Golembiewski, "From Signals to Cyber," 43.

systems."[826] Officers across a range of career fields who had demonstrated computer expertise were branded with a specific prefix to their Air Force Specialty Code. However, because these computer-savvy individuals were not specially or centrally managed, many saw this additional designator as potentially detrimental to their careers.[827] By 1963, it was clear that a more centralized focal point for computer expertise was needed to steer computer acquisitions and standardize system development.

A new Assistant for Data Automation position and data automation officer career field were stood up in 1963 as the Air Force computer focal point within the office of the comptroller — in other words, within the Air Force finance community. The data automation officer career field subsumed two previous computer specialties, the Electronic Data Processing Officer and the Data Systems and Statistics Officer, both of which were also contained under the Air Force comptroller.[828] At about the same time, the Air Force also introduced two new officer specialties: the Computer Systems Analyst and the Computer Systems Programming Officer. Unsure of where to house this expertise, each specialty was labeled as "interim" with an explanation that "proper career area location for this utilization field has not been determined."[829]

These interim methods of management proved inadequate to the long-term education, training, and retention of computer-skilled personnel. A 1970 report from the Air Force Select Committee on Computer Technology Potential cited "a shortage of educated and trained computer people assigned to the functional areas."[830] In August of 1970, the Air Force created a new Computer Technology career area by merging the data automation officers with the computer systems interim career fields of the early

---

[826]Golembiewski, "From Signals to Cyber," 57.

[827] Ibid., 58.

[828] The Electronic Data Processing Officer was formerly known as the Machine Accounting Officer, and the Data Systems and Statistics Officer was formerly known as the Statistical Services Officer.

[829] Golembiewski, "From Signals to Cyber," 57.

[830] Ibid., 58.

1960s. The new career area received an Air Force career designator of 51XX and consisted of five specialties. The field was renamed Computer Systems in 1977 and expanded from five to eight specialties.

More change came in 1982, when an Air Staff study concluded that the Air Force was no longer leading in the information technology realm.[831] In response, Air Force Chief of Staff General Charles A. Gabriel directed the consolidation of Air Force communications and data automation functions. Data automation units, previously a comptroller function, would be merged with base-level communications units to form information systems groups or squadrons under the Air Force Communications Command.[832] The merging of career fields followed soon thereafter: on 30 April 1985, the eight 51XX computer systems officer specialties joined with the five 30XX communications-electronics officer specialties to form six 49XX information systems officer specialties, comprising the largest non-rated officer career field in the Air Force, and the core of what would eventually become the 33SX communications branch.[833]

In 1986 the career field was renamed to cast officers as communications-computer officers, and the Air Force once again designated its information systems units as communications units. Six communications-computers officer specialties now replaced the previous 13 computer systems and communications-electronics officer specialties, and they all fell under the functional control of the Air Force Communications Command. By 1986, the Air Force Communications Command was the service's most widely dispersed command, with over 60,000 officer, enlisted, and civilian personnel assigned to 743 units at over 450 locations. The command centrally managed communications, air traffic control services, and now computer systems.[834]

This centralized model proved untenable to base operational commanders who wanted more power over their local communicators and the systems they maintained. In August 1989, at the urging of

---

[831] Golembiewski, "From Signals to Cyber," 59.

[832] Ibid., 60.

[833] Ibid.

[834] Ibid., 62.

then Commander-in-Chief of Pacific Air Force, General Merrill A. McPeak, Air Force Chief of Staff Larry D. Welch created a panel to consider Air Force Communications Command's future. McPeak argued that Air Force Communications Command was not needed, and that communications and computer systems personnel should be aligned under base mission commanders rather than under a distant functional command. In spite of the panel's recommendation against any significant changes, on 18 June 1990, General Welch announced that most communications units would be transferred to their host wings and major commands, effective 1 October 1990. Air Force Communications Command consequently shrank to less than 8,000 people. Air Force Communications Command lost further stature when then-Air Force Chief of Staff General Merrill A. McPeak converted it from a major command to a field operating agency on 1 July 1991. Soon after, the field operating agency was redesignated the Air Force Command, Control, Communications, and Computers Agency, and was reduced to about 900 people. In a further reduction of influence, the commander's billet was downgraded from a three-star general to that of a colonel.[835]

There are a number of reasons why the Air Force adopted a new decentralized approach, after spending decades developing a centralized management and control structure for communications. First, the end of the Cold War led to drastic cuts in defense spending. Cuts in spending and reductions in personnel meant that the Air Force would need to consolidate missions where it could, and many saw communications command as an additional bureaucratic headquarters that could be cut without jeopardizing operational missions. At the same time, the deployment of forces to the Middle East for Operation Desert Shield drove a requirement for robust, responsive communications that answered to mission commanders, as well a migration toward commercial-off-the-shelf communications products.[836] In the midst of these external requirements, General McPeak had voiced a concern that other operational commanders echoed: communications units should fall under and answer to their host wings in order to

---

[835] Golembiewski, "From Signals to Cyber," 63.

[836] Ibid., 64. On COTS migration, see Beach, "Managing Cyber Operator Training," 4.

strengthen unity of command for operational commanders, and to create a more readily enforceable structure for operations, maintenance, and system interoperability.[837] Furthermore, the migration to COTS systems led to a perceived reduction in the need for technical specialization within the communications career field.[838]

The Air Force went on to restructure its entire Air Force Specialty Code system of military personnel classification in 1993. While this restructuring had broad and far-reaching implications for many career fields, the communications-computer officer specialty was noticeably switched from 49XX to 33SX. Individual duty titles and descriptions were not significantly altered, though the Air Force eliminated specific specialty codes for communications staff officers. This move made base-level and higher-headquarters positions completely interchangeable, which served to further generalize the communications officer career field. This generalizing trend was exacerbated in 1995, when the service merged nearly 1500 officers in the information management and visual information career areas into 33SX communications-computers.[839]

The merger of visual information and information management with traditional communicators had the effect of further diluting the ability of the communications officer to specialize, and thus further diluted the incentive for him to cultivate specific technical skill. The responsibilities of visual information officers and information management officers had nothing to do with the management of electronic communications systems, yet the Air Force had committed to the position that the purview of a communications officer should extend to anything done on a computer.[840] Communications officers were now in charge of everything from filling Freedom of Information Act requests, producing installation decals, creating signage for official functions, photographing events, acting as executive officers and

---

[837] Golembiewski, "From Signals to Cyber," 63.

[838] Beach, "Managing Cyber Operator Training," 5.

[839] Golembiewski, "From Signals to Cyber," 69.

[840] Ibid., 71.

administrative assistants to Air Force leaders, and overseeing the traditional communications and computer systems operations and maintenance missions.

While this merger diluted the technical aspects of the communications officer career field, three sub-specialties still required technical expertise: electrical engineer, software engineer, and computer programmer/analyst. One snapshot of those numbers reported that of 4,648 communications officers, 318 were electrical engineers, 97 were software engineers, and 1,282 were programmer/analysts.[841] These numbers indicate that broad-based generalists comprised about two thirds of all communications officers, while only about one third of the career field were specialists focusing on specific technical mission areas. In 1998, however, the Air Force eliminated two of these specialties, as software engineers and computer programmer/analysts — two of the most important skill sets in cyberspace today — were absorbed into the core communications field. This left only electrical engineer as a specialized segment of the communications officer family. Most communications officers were now officially interchangeable, with the consequence that leaders increased their focus on broadening and career development over specialization and technical expertise.[842]

What accounts for the gradual death of the specialized communications officer? Concerns over promotion and retention likely drove this change. During its existence, Air Force Communications Command tended to have "well qualified and highly effective" officers who "managed complex systems vital to national defense, but for some reason this quality was not reflected in the promotion rates" which were typically below the AF average.[843] One can speculate that the junior officers who grew up in this period would conclude that the Air Force rewarded broad management and leadership experience over technical specialization, and would later work to shape the career field accordingly.

---

[841] Dina G. Levy et al., *Characterizing the Future Defense Workforce* (Santa Monica: Rand, 2001), 150.

[842] Golembiewski, "From Signals to Cyber," 72.

[843] Ibid., 73.

A 1976 Rand study supports this interpretation, and adds several additional observations as to why the Air Force failed to capitalize on its computer expertise.[844] First, decision makers lacked computer systems experience, and so had little understanding of the consequences of each iteration of career field changes and enterprise reorganizations. Second, the common practice of moving personnel to new jobs which were unrelated to their previous ones prevented the accumulation of in-depth experience and corporate knowledge over time. Third, voluntary separation rates for field-grade computer systems officers were significantly higher than for field-grades in general, making talent retention in the high ranks difficult. The Rand study concluded that field grade officers generally believed that specialization was bad for their careers, and a transition to a broader, more generalized career path for technical fields presented itself as one solution to the problem.[845]

As an example of the field's growing affinity for generalization, a 1994 communications officer career development plan warned, "A word of caution on specialization to the specialists—the Air Force needs technical specialists, but that need is limited." Specialization could "erode senior leadership's confidence in an officer's ability and flexibility … [impacting] … continued promotion at the field grade level where requirements for highly specialized and narrowly focused majors and lieutenant colonels are fewer."[846] Similarly, a 1999 communications officer professional development guide produced by the Air Staff sent a clear signal that for officers to be promoted "a broad spectrum of diversified jobs creates the best promotion recommendation form."[847] Further, it explained that the initial Basic Communications Officer Training course was not the specialized training of generations past; instead, its primary focus was "to provide a broad brush of basic communications fundamentals."[848]

---

[844] S.M. Drezner, The Computer Resources Management Study, (Santa Monica: Rand, 1976), 19.

[845] Interestingly, a 2005 Rand study noted a similar problem in a distinct shortage of captains and field-grade officers in the communications and information career field, but this study suggested the career field's diversity, or generalization, was a source of the problem. From Lionel A. Galway et al., *Understrength Air Force Officer Career Fields: A Force Management Approach* (Santa Monica: Rand, 2005), 42-47.

[846] Golembiewski, "From Signals to Cyber," 73.

[847] Ibid.

[848] Ibid.

By the early 2000s, several decades of career field reorganization had led to an interchangeable, generalist communications officer who held responsibilities across many different areas, but who specialized in none of them. Furthermore, the traditional communications mission had begun to change. The consolidation of network defense at AFNETOPS underneath 8AF in 2006 reduced mission demand for communicators at the squadron level.[849] The related difficulty of retaining officers past the rank of captain had led to talk of an increased reliance on contractors to fulfill certain routine communications functions.[850] Combined with Air Force personnel cuts, there was a growing sense that the communications field was becoming increasingly irrelevant and unnecessary.[851]

Meanwhile, while the intelligence community had proven historically eager to take over the cyber mission, they proved less eager when the time came to sacrifice billets for the creation of a cyber career field. The insatiable ISR demands prompted by Operations Iraqi and Enduring Freedom left the intelligence community overburdened and understrength, while the cyber-intel organizational schism of 2008 led to a break in the two fields' historically cozy relationship.[852] Additionally, the intelligence community's poor performance in Vietnam had created an undercurrent of suspicion between Air Force senior leadership — who had served in Vietnam as junior pilots — and Air Force intelligence organizations. There was a sense, however faint, among senior warfighters that they could not trust intelligence to deliver on a non-ISR mission, and consequently could not trust intelligence with cyberspace.[853]

The slow withdrawal of intelligence left communicators as the most opportune seed population for the new cyber career field. The historically close relationship between communicators and the

---

[849] Cothier, interview.

[850] Regarding the difficulty of retaining officers past captain, see Galway et al., *Understrength Air Force Officer Career Fields*, 44-47. Regarding the reliance on contractors: Shwedo, interview.

[851] Clothier, interview.

[852] Otto, Shwedo, interviews.

[853] Otto, interview. This point specifically referenced former Air Force Chief of Staff Larry D. Welch, who was raised as a pilot in Vietnam and retained suspicion of the intelligence community's ability to deliver ever since.

computational specialties they absorbed throughout the1980s meant that, from an outsider's perspective, communicators could be reasonably seen as the population which possessed the appropriate technical aptitude to pick up the cyber mission. Early iterations of the plan to man the cyber career field suggested transforming both communications officers and electronic warfare officers, but later iterations favored the the wholesale conversion of the 33SX career field alone.[854] Lieutenant General William T. Lord, Chief of Warfighting Integration under the Secretary of the Air Force, announced the service's new plan on 27 January 2010. The service's communications officers ceased to exist officially on 30 April 2010, "exactly 25 years after the merger between communications-electronics officers and computer systems officers."[855]

The selection of 17XX to designate the new cyberspace specialty carried a distinctive cultural significance, one which signaled an intention to break with the communicators' support tradition. The first character of an Air Force Specialty Code indicates a broad mission area. Any officer whose specialty begins with a 1 is considered operations, while a 3 indicates a support officer.[856] Communications officers have traditionally been considered support officers, but this new specialty code placed cyberspace operators, as the title suggests, squarely in operations — a move which technically puts former communications officers in the same prestigious cultural category as pilots, navigators, and space and missile operators. Eight years after the transition of the communications career field, the Air Force is still trying to strike the right cultural balance between the two very different populations that it contains.

---

[854] "Roadmap."

[855] Golembiewski, "From Signals to Cyber," 81.

[856] *Air Force Officer Classification Directory (AFOCD): The Official Guide to Air Force Officer Classification Codes,* Air Force Personnel Center. April 30, 2018. Other designators include 2 for logistics, 4 for medical, 5 for legal and chaplain, 6 for acquisition, 7 for special investigations, 8 for special duties, and 9 for special reporting identifies.

Table 7. Evolution of the Air Force Cyberspace Officer, 1945-2019

Year	Career Field	Summary	Number of Specialties
1945	Communications	A family of specialists within the Army Air Corps consisting of 36 distinct military operational specialties	36
1950s	Machine Accounting Officer Statistical Services Officer	Responsible for managing the computers that automated data processing within finance community	2
1954	Communications-Electronics (30XX)	Initially created from four specialties in 1954. Expanded to 7 specialties in 1970. Reduced to 5 specialties in 1981.	4
1961	Data Automation Officer Computer Systems Analyst Computer Systems Programming Officer	Three new career fields developed to provide a focal point for computer expertise.	3
1970	Computer Technology (51XX)	Merger of Data Automation Officer, Computer Systems Analyst, Computer Systems Programming Officer	5
1977	Computer Systems (51XX)	A renaming of Computer Technology with the addition of three new specialties	8
1985	Information Systems (49XX)	Merger of the five communications-electronics (30XX) and eight computer systems officer (51XX) career fields.	6
1986	Communications-Computer Officers (49XX)	Renaming of Information Systems	6
1993	Communications-Computer Officers (33SX)	Switched the alpha-numeric designation and eliminated specific specialty codes for staff officers.	6
1996	Communications and Information Officers (33SX)	Merged information management and visual information careers into communications-computers	4
2009	Cyberspace Operations (17XX)	Renaming of 33SX career field. Distinguishes between 17D cyberspace operations and 17S cyber warfare operations.	2

SUMMARY: CYBERSPACE PERSONNEL DEVELOPMENT

While the creation of the 17-series specialty code solved the career field problem, it did not solve the more pressing challenge of long-term talent development. The communications career field is a support function with a customer service mindset. As such, it does not breed "warfighters" of the type required to succeed in an operational, fighting domain. Moreover, the technical expertise required to build and maintain a network is not the same as the expertise required to either attack or defend it, with the latter carrying far higher demands of intellectual aptitude and technical acumen. These different operational demands have bred different cultures: communicators are largely risk averse generalists while their cyber counterparts must be risk-acceptant, technically creative specialists. The communications and cyber fields may both pertain to networks, but they require different skill sets, different talents, and different mindsets. Combining the two competencies into a single career field has arguably resulted in officers who are not terribly good in either, and has led to continued struggles to create the talent pool necessary for long-term cyber success.[857]

Furthermore, the adoption of the operational officer model has resulted in a cyber culture in which officers are bred as the technical experts, and are expected to hone their individual skill before stepping into leadership positions — akin to the model followed by pilots. This has resulted in an Air Force proclivity to use officers in its most highly technical cyber workroles, without an accompanying need to hasten them away from the keyboard and into leadership positions, as is most notably seen in the Army.[858] Predictably, Air Force cyber teams tend to be more officer-dominant than the identical teams of their sister services.[859]

---

[857] Lee, "The Failing of Air Force Cyber."

[858] Sydney J. Freedberg Jr. "Cyber Force Fights Training Shortfalls: NSA, IONs, and RIOT," Breaking Defense, September 27, 2018, https://breakingdefense.com/2018/09/cyber-force-fights-training-shortfalls-nsa-ions-riot/?fbclid=IwAR3Obpo7fW3N6emlfnGo_S6hrsbsxX2RkSqIrtPBJbVOutKmKJ2wEcyfYX0.

[859] Clothier, interview.

Conclusion

Returning to our original theoretical framework, the history described above allows us evaluate the primary motivating question of this dissertation: how do the organizational predispositions created by prior professional training, and the organizational decisions made in response to those predispositions, affect the ability of a service to deal with new challenges? How did the movement of cyberspace operations across subcultures — from intelligence, to nuclear strategic bombing, to space, to communications — affect the nature of Air Force cyberspace operations at any given time?

The Air Force recognized the value of cyberspace to military operations far earlier than any other service, but it struggled to develop a coherent organizational framework for how to effectively manage the capability. Ultimately, the theoretical innovation that was epitomized by the 1995 *Cornerstones of Information Warfare* was not matched by an adequate operationalization of that theory. Furthermore, the movement of cyberspace operations across different subcultures over time introduced a number of competing influences which prevented the mission from developing consistently. The brief inclusion of cyberspace operations into an operational numbered Air Force via the 609th Information Warfare Squadron from 1995-1999 led to a number of offensive and defensive innovations that were focused on providing theater-level, tactical support to 9th Air Force operations. Furthermore, the deliberately mixed personnel composition of the 609th, with equal parts intelligence, engineers, communicators, and warfighters, encouraged a high level of unconstrained innovation along with a service-centric focus of cyberspace support.

The movement of cyberspace operations into the intelligence community following the dissolution of the 609th resulted in a predictably homogenous unit personnel composition that was heavily reliant on the skills and expertise of Air Force signals intelligence. The desire to make intelligence more responsive to the needs of the operational Air Force resulted in the redesignation of intelligence units as information operations squadrons and the subordination of the AIA underneath Air Combat Command. However, cultural misunderstandings between intelligence professionals of the Air Intelligence Agency and the combat pilots of Air Combat Command led to recurring issues in the areas of resourcing and

mission prioritization. Both communities attempted to lobby for more control over the Air Force cyber mission without strongly articulating in which direction that mission should go. Doctrinal updates that occurred during this period likewise affirmed the centrality of cyberspace to the Air Force's core mission set, even while mainstream Air Force communities struggled to accept or understand what this might mean in practice.

What were the consequences of the Air Force's 2005 embrace of cyberspace as a core warfighting domain, and its subsequent attempt to integrate cyberspace into the dominant service culture? The initial placement of the new AFCYBER provisional command within the 8th Air Force, and the subsequent redesignation of 8AF as the Air Force global effects integrator, led to initial mission successes that were quickly stalled after the service's nuclear accountability failure in 2007. 8AF, as a command comprised of both nuclear strategic bombers and intelligence, surveillance, and reconnaissance aircraft, was uniquely suited to the type of global perspective that the Air Force's intent for cyberspace demanded, even while the command's lack of specific cyberspace expertise proved an initial disadvantage. Internal 8AF planning documents suggest that this global perspective was not shared by other components of the Air Force.[860] One can speculate that the theater-centric, rather than global approach with which 8AF had to compete began during the Gulf War and was influenced both by the Air Force's ongoing support to the Global War on Terror, and the natural inclinations of the non-bomber pilot communities: a fighter pilot, for example, will be naturally less inclined to think in terms of global strategic effects than would a pilot trained to fly nuclear aircraft.[861] This much is evident in the theater-centric focus of the 609 IWS while it was subordinate to the 9th Air Force.

However, in spite of the natural overlap in strategic orientation, AFCYBER (P) faced considerable difficulty in advocating for itself in a command that was still ultimately filled with pilots. In contrast to

---

[860] Elder, "Go Do One Year Report." The effort to convince the Air Force population to redefine Airpower to include the cyber domain "has been difficult because the Air Force does not see itself as a global force; instead, most Airmen view what we do in a purely theater context."

[861] Elder, email.

cyberspace operators, pilots were accustomed to being able to see both the weapon systems under their charge and the effects that those systems created. It was understandably difficult for this community to comprehend a weapon's value — and thus to argue for its continued resourcing — absent such physical reassurance. No such issues followed the movement of cyberspace operations into space command. Because space personnel are used to working with high tech systems that they can neither see nor touch, the conceptual integration of cyberspace operations into the space mission was relatively seamless. However, significant cultural differences in regards to risk, timeliness, and the need for continued training posed challenges to operational integration and mission prioritization. Moreover, the fact that cyberspace operations failed to fit into the Space Command resourcing construct led to resource and acquisition challenges that persisted in spite of the increased senior leader attention that the new command afforded.

Finally, the decision to populate the new cyber warfare career field with communicators — a support branch comprised of technical generalists — rather than with intelligence or electronic warfare personnel as originally planned caused a cultural stagnation within the cyber branch itself. As the Air Force struggled to fully articulate what cyberspace as warfighting capability meant, the personnel in the cyberspace career field struggled to demonstrate their operational worth due to a combination of insufficient training and their general support mentality. While the Air Force remains unique in its bifurcation of the intelligence and cyber communities, it has made steps toward integration and cultural assimilation with its 2018 decision to move 24th and 25th Air Forces underneath Air Combat Command.

The Air Force cyber story demonstrates that, while subcultural effects are strongest during periods of high uncertainty about the nature of an innovation, they are not necessarily eliminated once that uncertainty recedes. On the contrary, attempts to integrate a once-peripheral innovation into the core of a service's identity can spark a new type of intra-service competition, one that is less concerned with the mechanics of how an innovation is implemented than it is with how to maintain the balance of institutional prestige and influence in the face of a new competitor. Thus, while the introduction of strong central direction from service senior leadership might eliminate the subcultural competition for control of

an innovation's theoretical development, it does not eliminate traditional bureaucratic posturing for resources and power.

CHAPTER 5 | **Cyberspace Development in the U.S. Navy**

The preceding chapters on the Army and Air Force have supported the theoretical assertions of this dissertation: that the shape of an innovation is driven by patterns of behavior ingrained in service subcultures, that the influence of these subcultures is higher during periods of uncertainty, and that competing interpretations will resolve themselves in a way that aligns with the dominant service culture. In the Army, no fewer than five independent subcultures advanced their individual notions of cyberspace operations for the first fifteen years of the field's existence. These actions occurred against a backdrop of senior leadership whose uncertainty over the capability's relevance disinclined them to mediate intra-service disputes over how best to employ it. As the importance of cyberspace began to emerge with greater clarity in the late 2000s, spurred by joint momentum and increasingly clear real world examples, the Army resolved tensions between these competing interpretations by first separating cyberspace from its previous subcultural stewards, and second by shifting its focus from strategic matters to the level of tactical maneuver.

In the Air Force, early recognition of cyberspace's importance to air operations did not prevent the proliferation of institutional confusion over how best to manage it. Likewise, the sophisticated theoretical understanding of cyberspace which the Air Force developed well in advance of the other services was not followed by an adequate operationalization of these concepts. Over an approximately twenty year period, responsibility for cyberspace operations moved across the operational, intelligence, and space communities before settling into its most recent home underneath the Air Force's central operational command, Air Combat Command. These frequent reorganizations prevented the cyberspace mission from developing with consistency, and in some instances even undid the progress that had been established in previous years. Furthermore, while the Air Force was arguably the first service to establish a separate cyberspace operations career field, the ingrained cultural influences of the communications

community that was responsible for it had a stagnating effect on this career field's early development.[862] The movement of cyberspace operations across different sub-communities over time — and, in particular, the contrasting perspectives among these communities as to how cyberspace operations should develop — ultimately contributed to the mission's uneven patterns of growth.

Given the above, how should we expect subcultural patterns to manifest themselves in the development of cyberspace operations in the U.S. Navy? The history of cyberspace development in the Navy is less a story of inter-subcultural feuds than it is of a single subculture fighting with the dominant service culture for acceptance and validation of its new ideas. Heavily dependent on a network of global signals intelligence to protect its fleet abroad, the Navy forged a uniquely strong cadre of cryptologic professionals through an early investment in and partnership with the national cryptologic enterprise. This cadre of cryptologic warfare officers formed the nucleus of the Navy's early cyberspace development.

However, the primacy of fleet operations and the need for assured communication at sea — combined with the service desire to avoid alienating the national intelligence enterprise — prevented the Navy from developing an operational concept for cyberspace that was independent of the SIGINT community from which it had emerged. On the contrary, cyberspace came to be seen as a single component of an overarching theory of information dominance whose conceptual origins were derived from the signals intelligence successes of World War II. While a strong tradition of signals intelligence provided the Navy with an early advantage in the development of cyberspace operations, it was the very strength of this tradition, coupled with the operational imperatives of warfare at sea, that prevented the later emergence of an independent conceptual framework for what the other services had come to unequivocally label a new warfighting domain. The model that the Navy ultimately adopted for cyberspace was not, therefore, driven by cyberspace itself, but by the subordination of cyberspace to the

[862] I use the word "arguably" here because, as this chapter will show, the Navy was actually the first service to create an enlisted cyber-focused career field with its Cryptologic Technician-Networks (CTN) rating in 2004. However, the CTN rating was then and is now an extension of the larger community of cryptology, and cannot be fairly considered an independent cyber career field akin to what exists in the Air Force and Army.

broader concept of information dominance, and the subsequent elevation of that concept to a core service warfare area.

The Navy

ORIGINS, HISTORY, AND CULTURE

As with the Army and Air Force, Navy service culture is shaped by the domain in which it fights.[863] The maritime domain — defined as "the oceans, seas, bays, estuaries, islands, coastal areas, and the airspace above these, to include the littorals" — is vast, connected, featureless, and inhospitable.[864] The sheer size of this domain, and the consequently great distances over which the Navy must operate, have made the task of communication at sea a historically difficult one.[865] This difficulty of assured communication resulted in a level of operational independence among navy sea captains that is unique among the military services and is a Navy cultural hallmark.[866] As Carl Builder writes:

> Independent command of ships at sea is a unique, godlike responsibility unlike that afforded to commanding officers in the other services. Until the advent of telecommunications, a ship "over the horizon" was a world unto itself, with its captain absolutely responsible for every soul and consequence that fell under his command.[867]

---

[863] "The Navy's most obvious distinguishing characteristic is simply the maritime domain in which it operates." Zimmerman et al., *Movement and Maneuver*, 47.

[864] Lesa A. McComas, *The Naval Officer's Guide*, *12th Ed.* (Annapolis, M.D.: Naval Institute Press, 2011), 6.

[865] Zimmerman et al., *Movement and Maneuver*, 53: "Before the advent of wireless radio, when ships went to sea, they were not able to communicate with higher authority. Captains and commodores received broad mission orders and were expected to exercise their best judgment in the specific scenarios they encountered. There was no possible way to ask for further direction and guidance even had they wanted to."

[866] Ibid.

[867] Builder, *Masks*, 18.

While modern technology has largely eliminated the communications problem, its cultural legacy is such that the Navy values operational independence and self-sufficiency to a far greater degree than the other two services.[868]

The world's oceans are also defined by their uniformity of surface.[869] Unlike the contours, hills, and valleys which shape the reality of terrestrial warfare, the oceans are noteworthy for what they lack. On the one hand, the absence of terrain, vegetation, or man-made structures of any kind means that ships may go where they please without leaving record of where they have been. On the other, it means that surface naval forces rarely have anywhere to hide. Instead, the very vastness of the sea serves as a ship's most reliable form of concealment: the size and opacity of the maritime environment can make it difficult to find an enemy whose position cannot be deduced by a terrain-based process of elimination.[870] This fact has made maritime surveillance and reconnaissance vital to the conduct of naval warfare.

The featureless uniformity of the ocean's surface also affords a marked disadvantage to inferior navies. While a technologically inferior fleet can attempt to hide in the vastness of the sea, it cannot exploit terrain for positional advantage or to offset weakness once found.[871] Victory in a naval engagement will therefore often depend upon the pure balance of capability between the two engaged forces. The importance of this raw balance of capability helps to explain the Navy's dependence on technological superiority as well as its focus on platforms as an indicator of institutional health.[872] Furthermore, it also suggests that new technologies can have a more dramatic effect on fleet tactics than would an equivalent disruption on land.

---

[868] Zimmerman et al., *Movement and Maneuver.* The importance of operational independence and self sufficiency was further reinforced in interviews with past and current Navy leadership.

[869] Ian Speller, *Understanding Naval Warfare* (New York: Routledge, 2014), 16.

[870] Ibid., 24-25.

[871] Ibid., 26. The same is not true of submarine forces, who are able to exploit the geography of the seabed to hide from pursuit.

[872] Zimmerman et al., *Movement and Maneuver*, 49.

In addition to being large and featureless, the oceans are also connected and open. This continuity offers a level of global mobility and agility for maritime forces that has no parallel on land. Furthermore, while states have sovereignty over portions of the sea that extend out a fixed distance from their shorelines, the vast majority of the world's oceans are politically free and accessible to anyone who can get there. A ship may largely sail where it wants, when it wants, without crossing any borders or infringing on the sovereignty of another state. This relatively costless global mobility affords navies access to areas that are either physically or politically unavailable to land or air forces, and allows navies to represent the potential of force without its imminent or necessary application.[873] This flexibility of response allows navies to fulfill uniquely important roles in support of foreign policy and non-coercive diplomacy.[874]

Maritime openness also creates a unique type of complexity that derives from the status of the sea as global commons. While the sea is expansive, it can also be crowded, and so navies must contend with a maritime terrain that encourages regular encounters with merchant ships and other navies.[875] Furthermore, because the global connectivity of the maritime domain also serves as the basis of world trade, there is an implicitly economic dimension to naval activity that is less pronounced in the air or on land.[876]

However, while the oceans may provide a medium free from political control, they are not unregulated.[877] The nature of the sea as a shared domain, transited by military and civilian ship alike, makes it vital for a naval commander to understand the norms, laws, and agreements which govern maritime operations. Naval commanders must always be able to recognize the implications of their

---

[873] Speller, *Understanding Naval Warfare*, 83.

[874] Ibid., 83.

[875] In reflection of this principle, "Naval Operations Concept 2010: Implementing the Maritime Strategy" describes "comprehensive maritime domain awareness" as the foundation of global maritime security. Achieving maritime domain awareness requires an architecture that collects, fuses, analyzes, and disseminates large amounts of data regarding vessels, cargo, people, infrastructure, maritime areas of interest, and ongoing maritime security operations.

[876] By some estimates, over 90 percent of the world's goods travel by sea. (Naval Operations Concept 2010).

[877] Speller, *Understanding Naval Warfare*, 23.

actions within the context set by this legal framework. The familiarity with international law that is required of ship captains, combined with the inherently economic dimensions of maritime activity, lends a uniquely strategic tone to naval operations. Thus, naval officers — trained to operate in a vast global commons which is not delineated by rigid geographic demarcations, and accustomed to regular interactions with other nations and other navies — tend to be implicitly strategic minded, even if they are not explicitly taught to think in strategic terms.[878]

Finally, the sea is inhospitable. This inhospitable nature means that man cannot survive on the oceans unassisted. Instead, like the air forces above them, naval personnel are dependent upon their platforms for survival as much as for they are for warfighting. This dependence results in a platform-centric perspective that shapes the focus of all activity at sea.[879] The platform-centric nature of the navy, when combined with the inherent openness of the sea, allows the navy to adopt a persistent expeditionary posture. Whereas land-based forces traditionally reside in domestic garrisons and deploy abroad only in the event of a war or crisis, the default posture of the Navy is to be forward, continually engaged with global partners, ready to provide domestic leadership with the freedom of maneuver needed to influence world events.[880] As the U.S. Naval Operating Concept states,

> For the Naval Service, 'expeditionary' is not limited to 'being an armed force organized to accomplish a specific objective in a foreign country.' Rather, *being* expeditionary is one of our defining characteristics — we are ready to fight when we 'leave the pier,' persistently forward postured, and self-sustaining through our deployments.[881]

---

[878] By this I mean that the nature of naval operations forces an inherently strategic perspective that the the nature of air and land operations do not. However, as I will later discuss, the Navy is also possessed of a reluctance to encourage deliberate strategic education in its officer professional development, believing that time in the classroom is less important than time spent forward deployed.

[879] Speller, *Understanding Naval Warfare*, 18.

[880] Naval Operations Concept 2010. See also Zimmerman et al., *Movement and Manewer*, 53: "The real essence of the Navy is forward deployments. That's what makes us unique and sets us apart from the other services — that even during peace time we are always out doing the Navy's mission. […] The Navy has been forward, far from the homeland, ever since its creation 241 years ago."

[881] Naval Operations Concept 2010.

The mobility, agility, and self-sustainability of naval platforms that is captured in this service mantra of "forward presence" allows the Navy to gain access to places that other forms of military power cannot.[882] This access has historically allowed the Navy to serve in diplomatic roles that extend beyond the traditional military functions of coercion or deterrence.[883] Activities such port calls, contributions to multi-national engagement, humanitarian support, and simple presence in various regions around the globe are as much a part of the navy's core purpose as is fighting and winning in combat. As a result, the Navy is far more frequently employed to prevent conflict than to engage in it, with prevention activities constituting the most likely application of naval power.[884]

> The familiar attributes of an oceanic navy — inherent mobility, tactical flexibility, and a wide geographical reach — render it particularly useful as an instrument of policy even in the absence of hostilities. Land-based forces, whether ground or air, can also be deployed in a manner calculated to encourage friends and coerce enemies, but only within the narrow constraints of insertion, feasibility, and with inherently greater risks, since the land nexus can convert any significant deployment into a political commitment, with all the rigidities that this implies.[885]

The above principle is also evident in U.S. naval strategy, which states,

> For in this modern world, the instruments of warfare are not solely for waging war. Far more importantly, they are the means for controlling peace. Naval officers must therefore understand not only how to fight a war, but how to use the tremendous power which they operate to sustain a world of liberty and justice, without unleashing the powerful instruments of destruction and chaos that they have at their command.[886]

---

[882] Naval Operations Concept 2010.

[883] The six core capabilities of the Navy today, according to the current revision of Naval Doctrine Publication 1 (NDP 1), are forward presence, deterrence, sea control, power projection, maritime security, and humanitarian assurance/disaster relief. (Naval Doctrine Publication 1, *Naval Warfare* (Washington, D.C.: U.S. Navy, March 2010), 31).

[884] Naval Operations Concept 2010, 8: "We believe that preventing war is as important as winning, and that prevention activities will constitute the most likely application of naval power."

[885] Spellman, *Understanding Naval Warfare*, 80.

[886] Naval Operations Concept 2010, 44.

To conclude, the physical properties of the maritime domain give rise to particular political, economic, and legal dimensions that color naval strategy and shape the thinking of those who participate in it. For the Navy, accustomed to operating in a global commons transited by civilian and military ship alike, the prevention of conflict is as important as the ability to prevail in it. The prevention of conflict, in turn, depends on a type of persistent forward presence whose sustainability and flexibility is unique to the Navy alone, and which demands a global intelligence and communication network to sustain it. The global perspective derived therein has unique implications for how the sailor thinks about war: naval power is preventative and enduring in both application and reach; it is flexible in the range of diplomatic and military options it affords; and its proper application is contingent upon a global maritime domain awareness that both feeds and demands a strategic approach to sea control and power projection.

CULTURAL IMPLICATIONS

One can derive several conclusions about Navy culture from the descriptions given above. First, Navy culture is marked by a strong sense of independence that is derived from the historic difficulty of communication at sea. Sea captains received mission orders and were expected to exercise their best judgment in the execution of those orders once they left the harbor. This valuation of independent action and initiative persists to the present in the form of the doctrine of command by negation, in which a subordinate is expected to take action until instructed to stop.

> Faced with a situation that might require additional guidance or direction, rather than asking, "What should I do?" the typical Navy officer will instead inform his or her superior of the action he or she intends to take, understanding that the superior officer will either agree or provide alternative direction.[887]

Second, the Navy is a service which values the platform above all. The fact that a sailor cannot survive without his ship means that the individual naval platform — whether surface, subsurface, or

[887] Zimmerman et al., *Movement and Maneuver*, 53.

airborne — is both the key to power projection at sea and the nucleus around which service life revolves.[888] Accordingly, the sublime focus of a sailor's life is to maintain the fighting platform. Rear Admiral James Winnefield captures this principle well:

> The airman conquers his environment; the sailor survives it. The soldier shapes and exploits his environment; the sailor must adjust to it. The soldier depends on "combined arms;" the sailor must rely on himself and the world defined by his ship. The soldier may advance or retreat; the sailor must stand and fight. In modern times, even the release of surrender is beyond the reach of the sailor; he fights and dies with his ship — even if it is a blazing wreck or sinking beneath his feet. These forces imbue the sailor with a unique combination of qualities: self-reliance, a special respect and regard for the person who is in charge of his vessel, and absolute accountability. […] It is "his" ship against the environment, the enemy, and even sister ships.[889]

Whereas in land warfare, the individual soldier is the weapon, and thus the loss of an individual soldier entails the degradation of a unit's fighting capacity, individual sailors at sea are are the first thing that will be sacrificed, and readily, when the larger and far more important fighting organism is put at risk. This harsh reality of life at sea also underpins many of the seafaring traditions that serve to uniquely differentiate, and to uniquely stratify, officers from enlisted sailors.[890]

The platform-centric focus of war at sea means that naval battles tend to involve larger component pieces than land battles, and that naval power, as a result, tends to be disaggregated into fewer individual units. These natural limitations allow for the concentration of more control in the hands of a single commander than would be possible on land.[891] In contrast to land warfare, in which tactical

---

[888] Zimmerman et al., *Movement and Maneuver*, 49.

[889] James A. Winnefield, "Why Sailors Are Different," *Proceedings* Issue 121 (May 1995).

[890] Two aspects of naval personnel culture are worth highlighting here. The first is the relative detachment with which navy leaders must be willing to dispense with a sailor's life in order to save the ship. This detachment is operationally necessary when the alternative is to lose the ship and everyone on it, but it nevertheless stands in stark contrast to the decision-making calculus of the average Army officer, for whom manpower is the ultimate measure of combat strength — and for whom grunts hold an unmistakable grasp on the service imagination. The second aspect is the rigid distinction that the Navy maintains between its officers and its enlisted, a distinction which is partially attributable to the aforementioned dispensability of the average enlisted sailor, and partially attributable to the need to artificially impose a sense of separation on a ship's cramped quarters. Accordingly, enlisted and officers sleep in separate quarters, eat in separate messes, and generally maintain a level of formality in their interactions that would be foreign to the average infantry platoon or company. (Zimmerman et al., *Movement and Maneuver*, 47-48)

[891] Spellman, *Understanding Naval Warfare*, 27.

execution is decentralized across a large number of subordinate commanders who are each empowered to develop the local situation as they see fit, the focus at sea is on the effort of the entire crew to place the ship, which is the primary combat instrument, in the control of the directing mind of the commander. This concentration of power in the hands of the ship's captain leads to a hierarchical decision-making structure which is epitomized in the naval saying, "the captain is the ship."[892] Thus, the dominant decision-making unit in the Navy is the commander of a naval platform.

The independence of the average platform commander, while somewhat attenuated by modern technology, has given rise to another cultural idiosyncrasy: the Navy's aversion to written doctrine.[893] The Navy is alone among the services in its reluctance to embrace doctrine.[894] While the service has a limited number of doctrinal publications, those publications do not possess nearly the level of institutional prominence or preeminence that they do in either the Air Force or the Army. Operations at sea are typically fluid, change quickly, and have a greater variety of methods available to achieve them than do operations on land, which tend to be oriented towards the possession of terrain. The speed at which naval operations can unfold in this environment only magnifies the need for a ship's captain to possess complete freedom of action. The ongoing, if unfounded, naval fear is that written doctrine could potentially curtail this freedom.[895]

The importance of the naval platform also shapes the Navy's approach to technology. While the Army values its people above all, and the Air Force is possessed of a singular fixation on the quality of its technology, the Navy lies somewhere in between. On the one hand, the Navy has been historically

---

[892] Spellman, *Understanding Naval Warfare*, 27.

[893] Scott Hastings, "Is There a Doctrine in the House?" *Proceedings* Issue 120 (April 1994). The Navy's aversion to doctrine was also affirmed by a number of current and retired naval officers I interviewed, to include RADM Steve Parode, VADM (R) Jan Tighe, Winsor Whiton, Mark Hagerott, and others.

[894] Consider that the service's first center for doctrinal development did not officially open until March 1993. Hastings, "Is There a Doctrine in the House?"

[895] Hastings, "Is There a Doctrine in the House?" An additional challenge to the creation of naval doctrine is the fact that the Navy, as a persistently forward force, is always operationally engaged. The Army typically writes its doctrine in between wars when it has had time to reflect on lessons learned. The Navy's default posture of being constantly at sea affords little chance for similar reflection. (Jan Tighe, telephonic interview with the author, October 30, 2018.)

distrustful of technologies which threaten the independence of a ship's commander.[896] On the other, the absence of maritime terrain, and thus the absence of opportunities to offset weakness, means that victory at sea depends to a great extent on the quality of one's ships and the technological sophistication of one's weaponry. Thus, superior technology is welcomed in the service as a bulwark against potential naval defeat.

However, in order to defeat an inferior ship, one must first find it, a task which can be exceedingly difficult in the vast expanses of open ocean. The challenges inherent to the sprawling distances of maritime warfare, as well as the inherent vulnerability of a ship derived from the lack of mitigating surface features, have lent the Navy a historic fondness for technologies which allow it to communicate great distances and to see things over the horizon. This fondness helps to explain the Navy's strong heritage in the fields of cryptology, communication, intelligence, surveillance, and reconnaissance. Thus, the Navy can be said to have a moderate dependence on technology that lies somewhere in between the technological aversion of the Army and the technological fixation of the Air Force, with an institutional emphasis on technologies related to surveillance and communication.

Finally, the Navy's focus on platforms also serves as the source of its most contentious intra-service divisions. Who a naval officer is is defined by what he does, and what he does is bound to the platform community to which he belongs. The first and broadest distinction within naval communities is between those who command platforms at sea, and those who cannot. Members of these command-eligible platform communities, called unrestricted line officers, comprise the Navy's warfighting class.[897]

These platform communities are further subdivided by platform type into surface warfare officers, submariners, and aviators.[898] Significant cultural distinctions exist between these platform communities,

---

[896] Arleigh Burke once famously said, "Going to sea used to be fun and then they gave us radios." (Gary Roughead, remarks delivered at the Center for Strategic and International Studies. "Information Dominance: The Navy's Initiative to Maintain the Competitive Advantage in the Information Age," October 1, 2009)

[897] Zimmerman et al., *Movement and Maneuver*, 48.

[898] Special operations and explosive ordnance disposal are also members of the unrestricted line community, but have traditionally not held the same levers of power as the "big three" since their missions represent such a small fraction of overall maritime operations.

even while they enjoy relative equity in terms of institutional power and influence.[899] Broadly speaking, aviators and submariners tend to be more insular than surface warfare officers. The inherent limitation of undersea sensors, combined with the secretive nature of submarine missions, give the sub community a single-ship mindset that tends to be naturally averse to information sharing. In contrast, pilots are an engagement-oriented community that is singularly concerned with the air domain. Meanwhile, beholden to an array of sensors and operating in a three-dimensional battlespace, the surface warfare community must maintain an inherent awareness of the other platforms that results in a more integrative operational mindset.[900] While these communities do compete with one another for resources, evidence suggests that there is neither a vast disparity between them nor an enduring hierarchy of power and influence.[901]

The cultural differences within the platform communities are far less important than the cultural differences between the platform and non-platform communities. The platform communities are considered the warfighters of the Navy. The non-platform communities, called restricted line officers and prohibited from command at sea, are considered warfighter support.[902] Restricted line officers were created out of a demand for specialized expertise that could not be satisfied through simple assignment cross-detailing.[903] For example, until the creation of the Navy's information professional community in 2001, all afloat communications functions were performed as an additional duty by surface warfare

---

[899] Zimmerman et al., *Movement and Maneuver*, 48. As with the differentiation among pilot types in the Air Force, several divisions exist within platform communities as well. Aviators are divided between the F-18 "single seat master race," maritime patrol multi-engine, reconnaissance, and rotary-wing. SWOs are divided by ship type between fighters, transporters, and mine sweepers. Submariners tend to be the most homogenous of the bunch, as the officer corps is all nuclear trained and can switch between attack subs and missile subs. (Phil Pournelle, interview with the author, September 27, 2018)

[900] Ibid., 50. The challenges of coordinating between the multiple domains in which the Navy operates — air, surface, subsurface, and littorals — lend the Navy more multi domain familiarity than either the Army or the Air Force. This remark was echoed by Mark Hagerott and Phil Pournelle in interviews.

[901] Zimmerman et al., *Movement and Maneuver*, 49. Since December 1945, the breakdown of Chiefs of Naval Operations by warfare community are as follows: seven aviators, eight SWOs, and seven submariners.

[902] Ibid., 48. Restricted line communities include intelligence officers, foreign area officers, information professionals, and engineering duty officers. The Navy also maintains a separate staff corps comprised of active duty professionals such as doctors, nurses, dentists, lawyers, and chaplains.

[903] Henry Stephenson, "Masters or Jacks?" *Proceedings* Issue 140 (October 2014).

officers who were augmented by more technically focused enlisted sailors. The Navy created a restricted line community for communications in response to a demand for more well-managed technical expertise.

This broad division between warfighters and warfighting support has implications for how the Navy approaches career development. Unrestricted line officers are bred to be generalists who are capable of commanding mixed maneuver units that are comprised of a variety of different force types.[904] Restricted line officers, in contrast, are trained to be specialists in a particular support discipline. Broadening assignments are typically seen as counterproductive to the development of the type of specialized skill that the community as a whole exists to provide.

A noteworthy commonality between both restricted and unrestricted line communities, however, is the relative balance each places on classroom versus on-the-job training. With a few notable exceptions, the Navy training model tends to disregard classroom instruction in favor of on-the-job training. This applies to both the initial schooling of new officers and to professional education throughout an officer's career.[905] More so than the other services, the Navy places a far greater emphasis on operations experience at sea than other forms of professional development, to include postgraduate education and strategic broadening assignments.[906] Furthermore, the Navy's valuation of science and technology degrees at the expense of broad education in the humanities — with the majority of Naval Academy and ROTC graduates expected to be STEM majors — has arguably led to a decline in how the Navy approaches the formulation of strategy in comparison to the other services.[907] These contrary career models will have implications for the future Navy cyber story.

---

[904] Stephenson, "Masters or Jacks?"

[905] Pournelle, interview. Exceptions to this rule are made for high skill disciplines. For example, aviators must still attend flight school, and nuclear submarine officers must attend the Navy's rigorous nuclear power school. However, the general disdain for formalized professional education still holds across the service.

[906] Zimmerman et al., *Movement and Maneuver*, 50.

[907] Ibid., 51. 85% of Navy ROTC scholarships are granted to students who select an engineering, math, or science program. These scholarships can be rescinded if the student chooses to change his or her major. Beginning with the USNA class of 2013, at least 65% of graduates must complete academic majors in a STEM field.

NAVY SUBCULTURES

The Navy is comprised of a number of functional subcultures, each with its own purpose, mission, and culture. As described above, the broadest distinction is between those who can command at sea — the service's traditional platform-based warfighting communities — and those who cannot. Members of this unrestricted line community unquestionably hold the most power and influence in the Navy.

In addition to the restricted and unrestricted line distinction, there are three specific sub-communities that have interacted to affect the outcome of Navy cyberspace operations: cryptology, intelligence, and communications. However, the overwhelming extent to which cryptology dominated Navy cyberspace development, coupled with the unique manner in which that development concluded, makes the four dimensions of cultural variation I have previously established — tolerance of risk, delegation of decision-making, mission orientation, and technical aptitude — far less relevant to this chapter's empirical analysis. I will therefore forgo an evaluation of each of the sub-communities along these dimensions in favor of a more general description of the sub-communities' character.

Cryptology

Cryptology, was born out of the Navy's code-breaking efforts in World War II. Today, it exists to intercept and analyze enemy communications signals. With this purpose, it is similar in orientation to the signals intelligence communities of the Army and Air Force. However, cryptologists enjoy a unique position of institutional reverence in the Navy due to aforementioned importance of communication at sea, and to the community's herculean effort in exploiting that communication to lead the Navy to victory during key battles of World War II.[908] The Navy's substantial World War II investment in cryptology,

[908] Consider that the Navy celebrates exactly two holidays service-wide: the Navy's birthday, and the Battle of Midway (Winsor Whiton, telephonic interview with the author, January 8, 2019). One of the most important naval battles in history, the outcome of the Battle of Midway was decided by the cryptologists who broke the Japanese communication codes, thereby allowing the U.S. to identify the location of the Japanese fleet. Admiral Michael Rogers also emphasized the importance of the Battle of Midway to the service's institutional memory during our interview.

coupled with the singular importance of code-breaking to a service that is beholden to long-range radio-frequency (RF) communication, contributed to the service's decision to develop it as a separate career field from the broader practices of naval intelligence and communication from which it arose. The Navy is alone among the services in maintaining a professional distinction between these two fields. Furthermore, the historic inclusion of electronic warfare with the field of cryptology has lent the community an operational mindset that stands in contrast to what would be expected of a traditional intelligence field. Cryptologists tend to consider themselves more operationally-minded, more forward-leaning, and more focused on problem solving than their intelligence peers.[909]

After a six week basic course that is divided, if unequally, among signals intelligence, electronic warfare, and cyberspace operations, naval cryptologists spend their first tour of duty at one of the main National Security Agency field sites.[910] They there have eighteen months to meet the Navy's cryptologic warfare qualification standards. After this first tour, cryptologists alternate between sea- and shore-based assignments, with the expectation that regardless of where they are, they are always engaged in the practice of cryptologic warfare. The Navy's practice of sending its junior cryptologic officers to an assignment with the National Security Agency, rather than straight to the fleet, serves to ensure that said officers are grounded in a robust understanding of the national signals intelligence enterprise. This practice also speaks to the Navy's uniquely close service relationship with the NSA.[911]

Intelligence

Standing in contrast to cryptology, the intelligence community is comprised of restricted line officers whose purpose is to provide fleet and national decision-makers a thorough understanding of the maritime operational environment and the potential threats contained therein. The community is defined

---

[909] Tighe, interview.

[910] Brandon Karpf, "Train Navy Officers for Cyber Lethality," *Proceedings* Issue 146 (February 2019). Regarding the unequal curriculum distribution, cryptologic warfare officers receive six weeks of basic officer training before their first assignment, with one week on cyberspace.

[911] The Army and Air Force do not have similar assignment policies for their SIGINT personnel.

by a culture of operational intelligence that emphasizes the discipline's predictive value for the warfighting end user.[912] As with cryptology, naval intelligence established a strong reputation in World War II which only increased through the community's extraordinary contributions during the Cold War.[913] However, the Cold War left a significant cultural imprint on the community's self-perception that proved difficult to overcome when handed a new set of geopolitical circumstances with its own unique type of intelligence demands. The naval intelligence community's struggle to adapt to the post-Cold War informational landscape of the 1990s and 2000s would come to cost them critical influence during a period of of rapid institutional change.[914]

Naval intelligence officers attend a six-month Naval Intelligence Officer Basic Course (NIOBC) that introduces them to critical thinking and analytic tradecraft.[915] After initial training, these officers progress through the traditional alternation of sea- and shore-based assignments. While ashore, they typically serve in operational intelligence centers that provide focused intelligence to a geographically aligned fleet. As with cryptologists, the expectation is that intelligence officers will always be in the business of practicing their craft, whether ashore or afloat.

Almost as important as understanding the culture of these communities individually is recognizing the historic tension that exists between them.[916] As the intelligence and cryptologic communities began to specialize during the early years of the Cold War, the natural boundaries between

---

[912] Alfred Turner, telephonic interview with the author, January 16, 2018 and David J. Dorsett, telephonic interview with the author, January 12, 2019.

[913] Dorsett, interview.

[914] It is important to note that the entire Navy struggled to adapt to the post-Cold War world. Cold War maritime strategy envisioned an offensive fight against the Soviet navy at sea in order to gain control in areas adjacent to, and to launch strikes into, the Soviet rear and flanks during a war in central Europe. This strategy inspired the push for a larger and more capable 600-ship fleet. When the Cold War ended and the Soviet navy fell out of the picture, there no longer existed a foe capable of contesting the U.S. for sea control or control of shipping lanes. This new geopolitical context called into question the very relevance of the Navy's traditionally accepted roles and missions, and led to much institutional introspection to determine how, exactly, the Navy would fit into 21st century defense strategy. The Navy's first post-Cold War service strategy, "…*From the Sea,*" emphasized the Navy's expeditionary flexibility and self-sustainability as ideally suited to providing the type of flexible response options to unpredictable geopolitical issues that the U.S. would need in a world that had lost the stability of bipolarity. See Zimmerman et al., *Movement and Maneuver*, 62-63, 71.

[915] William N. Murray, "Reimagine Intelligence Officer Training," *Proceedings* Issue 145 (January 2019).

[916] The existence of this inter-community tension, particularly at the bureaucratic level, was echoed in nearly every interview I conducted with former cryptologists and intelligence officers.

them grew into a rivalry over what each side could or could not bring to the fight.[917] This rivalry produced a palpable friction between intelligence officers and cryptologists. While the friction between communities was often less evident aboard ships at the operational level, it had a notoriously disruptive influence on bureaucratic decisions.[918] Furthermore, because Navy fighting staffs held separate positions for each discipline — with independent cryptologic and intelligence officers each reporting their part of the intelligence picture to a single operational commander — cooperation or conflict between the two was more often the chance product of personalities than of any built-in structural mechanism.[919]

Communicators

Standing in contrast to both intelligence and cryptology are the Navy's communicators. Despite the importance of long-range communication to maritime operations, the Navy did not have a truly independent communications career field until the creation of the Information Professional community in the early 2000s. Until that point, staff communication functions at sea were performed by regular unrestricted line officers, most of whom had received minimal appropriate training and who would return to a regular line job afterwards.[920] Ashore, positions were filled by an eclectic collection of various communities, ranging from limited duty and engineering duty personnel to a General Unrestricted Line community (GURL) that, until the removal of Title IX restrictions in 1995, was comprised primarily of the Navy's female officers who were prohibited from serving in combat.[921] However, these eclectic fields

---

[917] This divergence and subsequent rivalry is interesting given that the cryptologic communities two greatest World War II heroes, Rochefort and Layton, were both intelligence officers, not cryptologists.

[918] *"And I Was There"* by Layton, Pineau, and Costello provides good historic context on the World War II origins of the cryptologist-intelligence rivalry.

[919] Turner, interview. This is an important point, because measures taken during the reign of Admiral Jack Dorsett as Chief of Naval Operations were explicitly designed to eliminate personality as an operational variable.

[920] The surface warfare community did have a five week basic communications course in Newport, Rhode Island, for some of its officers. However, the course lacked comprehensive technical content, and was not designed to create subject matter experts. From Danielle Barrett, "Developing a Community of C4IW Professionals," *Proceedings* Issue 126 (June 2000).

[921] The GURL community was created to allow Navy females a place to serve before the removal of restrictions that prohibited women from combat units. From Janice Graham, "Does the Navy Need the 1700 Community?" *Proceedings* Issue 125 (Feb 1999).

had neither a single community manager nor a single career path to ensure that their skills were used effectively.

In 1997, the Navy took the first step toward rectifying this discrepancy when it merged the historic Radioman enlisted rating with the Data Processing Technician to form the enlisted Information Technician (IT).[922] ITs were designed to serve as the Navy's primary experts in digital networks.[923] This move was followed shortly thereafter by the creation of the Information Professional (IP) officer community in 2001.[924] As communicators, IPs are similar to their Army and Air Force counterparts in that they manage communication requirements for the broader force. This entails a responsibility to build, maintain, defend, and restore networks of all kinds and at all levels, which in turn leads to a culture that is oriented towards providing a service rather than conducting operations. However, as the youngest of the communities that were involved in the evolution of naval cyberspace operations, Navy communicators did not possess the same level of cultural or institutional maturity as did their intelligence and cryptologic peers, and thus had a limited ability to influence the cyberspace trajectory.

---

[922] "Enlisted Rating Insignia," Navy.mil, updated June 28, 2009, https://www.navy.mil/navydata/nav_legacy.asp?id=262.

[923] ITs perform core and specialty functions of communications operations, message processing, network administration, and cybersecurity; secure, defend and preserve data, networks, net-centric capabilities, and other designated systems; implement security controls and defensive counter-measures; establish, monitor, and maintain Radio Frequency (RF) communications systems; perform spectrum management to support Joint, Fleet, and tactical communications; handle, store, and retrieve incoming and outgoing messages; build, configure, deploy, operate, and maintain information technology, networks and capabilities; perform network system administration, maintenance and training; manage, plan and coordinate unit-level Information Systems Security (ISS) and integration across platforms, fleets, and services; and ensure the proper security, handling, accounting, reporting, and control of Communications Security (COMSEC) materials, systems, and equipment. From "IT Career Path," Navy.mil, updated August 2018, https://www.public.navy.mil/bupers-npc/enlisted/community/crypto_it/Documents/IT%20career%20path.pdf.

[924] "Navy Information Professional: Connecting the Global Force," United States Naval Academy Informational Brochure, https://www.usna.edu/CyberCenter/_files/documents/idc/NavyIPCommunityBrochure.pdf.

Electronic Warfare

Notably absent from our discussion of naval cyberspace operations is the field of electronic warfare. In spite of the Navy's proud tradition of electronic warfare, it has never had a true electronic warfare personnel community. Electronic warfare in the Navy has been principally an enlisted technical community with no permanently assigned officers. Functional responsibility for electronic warfare systems was distributed among the platform communities to which those systems belonged. Surface warfare, for example, would have responsibility for the electronic warfare systems that were designed for surface warfare ships, while aviation would be responsible for the EA-18 Growler electronic attack platforms. However, the pilots who flew electronic attack aircraft identified themselves as pilots first, and so from a cultural standpoint were more akin to the rest of the aviation community than to any independent electronic warfare tribe. In 2003, the Navy's enlisted electronic warfare technicians were merged with the cryptologic technician-technical (CTT) to fully and formally integrate electronic warfare into the cryptologic community.[925] This move was also intended to provide electronic warfare with adequate senior level oversight to ensure that it would not be forgotten in the push to improve the Navy's disposition in the information domain.[926]

CULTURAL SUMMARY

What does the above exploration tell us about Navy culture, and what might that culture reveal about the Navy's later approach to cyberspace? The Navy is a platform-centric organization whose primary purpose is to project power abroad through forward presence at sea. This maritime focus lends itself to a strategically-minded force in which the potential for power — economic, diplomatic, and

---

[925] CTTs perform a variety of specialized duties associated with the collection and processing of airborne, shipborne, and land-based radar signals. They operate electronic intelligence receiving and direction finding systems, digital recording devices, analysis terminals, and associated computer equipment. The systems they operate also produce high-power jamming signals used to deceive electronic sensors and defeat radar guided weapons systems. From "Cryptologic Technician-Technical," Navy Personnel Command, accessed January 18, 2019, https://www.public.navy.mil/bupers-npc/enlisted/community/crypto_it/Pages/CTT.aspx.

[926] Winsor Whiton, telephonic interview with the author, January 8, 2019.

military — is as important as its application, and which implicitly concentrates immense authority in the hands of the independent naval commander. Furthermore, the unique characteristics of the sea, and the subsequent great distances over which the Navy must operate, make the complementary acts of communication and over-the-horizon surveillance of supreme operational importance. Consequently, as a globally distributed force, the Navy must maintain a continuous level of global connectivity in order to conduct routine operations.

Given these cultural proclivities, we can expect the Navy to draw upon its storied traditions of communication and cryptology for the early development of cyberspace capabilities and concepts. The lack of a commensurately powerful rival sub-community will dramatically reduce the possibility that the cryptologist conception of cyberspace will face competition from alternate interpretations. However, the Navy's understanding of cyberspace will undergo a radical shift as it is assimilated into the dominant warfighting service culture. Specifically, the informational imperatives of warfare at sea, derived from the need to assimilate massive amounts of sensor information from a complex battlespace, will prevent the further development of cyberspace as an independent operational concept. Instead, cyberspace will only become relevant to fleet operations if it is subsumed into a broad doctrinal framework that adequately accounts for the importance of communication, connectivity, and intelligence to naval operational effectiveness. Within that framework, we can expect the Navy's approach to cyberspace to focus on defense and connectivity rather than offensive effects.

Communication at Sea and the Digitization of the U.S. Navy

One can interpret the Navy's approach to cyberspace operations — in particular, its subordination of cyberspace to the broader idea of information dominance — as a contemporary manifestation of the service's historic challenges of assured communication at sea. In this first section, I will briefly describe the history of how the Navy has met these communication challenges, and summarize what that portends for its future approach to cyberspace. Three important themes will emerge from this

history: first, the importance of communication at sea, and the consequent effort to adopt new technologies that enable it; second, the challenges of command and control and information management that have occurred as a result; and third, the primacy of the cryptologic community to Navy warfighting.

The Navy's adoption of computing technology was in response to a series of operational problems that stemmed from the nature of the maritime domain. The first of these problems concerned the matter of reliable ship-to-ship communication. Before the advent of radio technology, naval ships were reliant upon visual signaling techniques such as flags, flares, and lights to convey basic messages to one another. Limitations in the range and reliability of visual signals during the age of sail resulted in a necessary delegation of autonomy to individual ship captains, epitomized by the words of Admiral Horatio Nelson: "In case signals can neither be seen or perfectly understood, no captain can do very wrong if he places his ship alongside that of an enemy."[927]

The introduction of steam power in the 19th century rendered visual signals inadequate for the new distances and speeds at which ships could travel. Furthermore, the maneuverability that was afforded by steam power enabled the ships within a fleet to operate more easily as a single system rather than as a collection of independent vessels.[928] As the commander's ability to direct the individual components of his fleet grew in importance, the autonomy that was championed in previous eras began to erode. These developments encouraged a shift in the role of the naval commander from one of leadership by example to one of the mind of the entire fleet, able to control large groups of geographically dispersed warships that could act in concert against a determined foe.[929] The resultant command and control challenge would require the development of more advanced communications technology.

---

[927] Timothy S. Wolters, *Information at Sea: Shipboard Command and Control in the U.S. Navy, from Mobile Bay to Okinawa* (Baltimore: Johns Hopkins University Press, 2013), 20.

[928] Ibid., 20.

[929] Ibid., 19. "Now that, through the agency of steam, war has become not less a science at sea than on land; when the ocean is a great chess-board, upon which the skillful looker-on sees many a move not apparent to the contestants, whose brains have become heated with the strife, the *role* of the admiral approximates to that of the general, and he should, like the latter, take post whence, without being an active participant in it, he may overlook the whole *sea of battle,* and signal to the fleet such formations as he shall find necessary. He should, in other words, be the *mind* of the fleet."

In response to this operational challenge, naval officers worked hard to develop rapid, reliable, and secure signaling systems during the latter half of the 19th century.[930] The Navy began to experiment with wireless technology in earnest during the first decade of the 20th century, having purchased more than fifty sets of radio equipment by the end of 1903.[931] This experimentation became more urgent after the 1916 Battle of Jutland, a World War I engagement between the British and the Germans which offered the first demonstration of the new complexity of naval warfare, and of the subsequent command and control difficulties that modern fleet commanders would face.[932] "Lack of adequate information" was seen as a key contributor to the tactical defeat of the numerically superior British fleet.[933] As such, Jutland reinforced the conclusion that the U.S. Navy would need better methods of command and control.

The Navy made a number of internal reforms in response to lessons learned from both the Battle of Jutland and its annual fleet exercises that followed. In the 1920s, the Navy created shipboard communications departments to ensure that a single officer on each warship held responsibility for coordinating all methods of communication, from flags and lights to radio and underwater sound signals.[934] The 1930s saw the first official report for a fleet problem that contained a substantial entry under the heading "information" in order to incentivize better information management practices during what were increasingly three dimensional naval engagements.[935] The Navy also began to experiment with underwater sound signaling and high frequency radios, the latter of which enabled longer-range communications through its ability to bounce radio waves off the ionosphere.[936] Feedback from the U.S. Navy's Fleet Problem Five in 1925 highlighted the extent to which communications dominated the Navy's

---

[930] Wolters, *Information at Sea*, 38.

[931] Ibid., 43.

[932] Ibid., 83.

[933] Ibid., 108.

[934] Ibid., 120.

[935] Ibid., 133.

[936] Ibid., 123.

operational consciousness during the inter-war years, with one fleet commander stating that the exercise was "as much a problem of communications as it is a scouting problem and the success or failure of the whole maneuver will depend largely upon the radio personnel of the fleet."[937]

The command and control difficulties faced by naval commanders, as well as the resultant need for accurate, timely, and secure information, were exacerbated by the arrival of the aircraft carrier. The introduction of aircraft to the naval fleet meant that commanders had to control and defend against an increasing number of discrete units who were capable of attacking from multiple directions. Furthermore, the speed of these aircraft in comparison to the ships they attacked meant that commanders often had much less time to make critical decisions than they had in the past.[938] Subsequent information challenges related to the volume and speed of aircraft attacks were compounded by the inherent vulnerability of the carriers themselves. The ability to protect information about their location became crucial to success in the increasingly complex field of naval warfare.

Key to both the coordination of these disparate forces — surface, subsurface, and air — and to ensuring their survivability was the acquisition of timely, reliable, and accurate information about friendly and enemy activity. The need to rapidly acquire and communicate information drove the development of several related technologies in the decades leading up to World War II. First, the near exclusive reliance of naval forces on wireless radio transmission opened up the electromagnetic spectrum as a rich intelligence resource. The development of radio as a communication tool led to the development of radar to exploit that communication, which in turn led to direction finding and increasingly sophisticated methods of signals interception. The vulnerability of these signals created a need to secure them, which led to advances in the fields of cryptology and cryptography that emerged as the defining contest of naval intelligence during World War II. Each of these new technologies helped lessen the burden of the Navy's

[937] Wolters, *Information at Sea*, 122.

[938] Ibid., 134.

command and control challenges.[939] However, at the nexus of each of these technological advances stood an imminent new problem whose solution would ultimately propel the Navy into the digital era: information saturation.

In July of 1941, the Secretary of the Navy approved a joint recommendation that major combatant ships would be equipped with a radar plot that would serve as the "brain of the organization which protects the fleet or ships from an air attack."[940] While radar greatly improved the Navy's system of air defense, the amount of data that radars were able to produce quickly overwhelmed existing systems of information management. Combat experience in the Pacific led many American naval officers to conclude that there was an urgent need for a shipboard facility that could process all types of tactical information, from routine data on navigation and weather to updates from radar and direction finding systems. Largely in response to radar difficulties at the Battle of Midway, in late 1942 Pacific Fleet commander Admiral Chester Nimitz directed the creation of the Combat Operations Center, later the Combat Information Center (CIC), on all ships as a place where "information from all available sources can be received, assimilated, and evaluated with a minimum delay."[941]

CICs greatly improved fleet performance by streamlining the process of information management.[942] However, the introduction of Japanese kamikaze attacks in late 1944 revealed the fatal flaw of the CIC by highlighting the limits of what a manual tracking system could accomplish. The sheer number of targets that kamikaze attacks presented overwhelmed both the radar systems' ability to detect new data points and the human mind's ability to process them. Even when the CIC plotting teams were

---

[939] Radio made it possible for a remote commander to maintain near real-time awareness of events at sea, and dramatically improved his ability to control geographically dispersed forces. Meanwhile, radar made it possible for a commander to see what was happening in a broad battlespace. Encryption allowed a commander to send and receive secure messages over the great distances that his fleet was expected to travel.

[940] David L. Boslaugh, *When Computers Went to Sea: The Digitization of the United States Navy* (Los Alamitos: IEEE Computer Society, 1999), 20.

[941] Wolters, *Information at Sea*, 205; Midway from Paul Nagy, "Network-Centric Warfare Isn't New," *Proceedings* Issue 127 (September 2001).

[942] At the Battle of the Philippine Sea in June 1944, for example, the CICs of the U.S. fleet vectored defending fighters so effectively that they massacred the attacking Japanese naval air arm. Four major attacks were all intercepted some fifty to sixty miles from the carriers, and no fighters got through. (Wolters, *Information at Sea*, 212-213 and Norman Friedman, *Network-Centric Warfare: How Navies Learned to Fight Smarter Through Three World Wars* (Annapolis: Naval Institute Press, 2009), 59.

able to generate an accurate picture of the tactical situation, the speed with which kamikaze attacks progressed offered inadequate time to direct a ship's weapon systems for a defensive response. By the end of World War II, the Navy had begun to recognize the imminent need for a system of automated data management and missile response as a way to improve fleet survivability against rapidly improving attack technology.[943]

In the early 1950s, all three services were trying to find workable solutions to the discrepancy between radar's prolific output and the limited processing power of combat direction organizations.[944] The solution to the Navy's air defense challenges would come from the convergence of several technologies created to solve three different computational demands, the first of which was in the field of cryptology. The rise of radio communication at sea led to the realization that intercepted radio transmissions could be a fruitful source of information about the disposition and intention of other naval forces. In response, the Navy built a radio intercept and codebreaking organization that far overshadowed similar Army efforts.[945] By the outbreak of World War II, the Navy's Communications and Intelligence Section, OP-20-G, was the dominant U.S. military organization in communications intelligence. OP-20-G had a full-time codebreaking wing called the Communications Supplementary Activities, Washington (CSAW).[946]

What the cryptologists at CSAW ultimately sought was a high speed, general purpose machine that could be retargeted to new coding problems with minimal time and effort.[947] Two other computing

---

[943] Boslaugh, *When Computers Went to Sea*, 56-58 and 69-70.

[944] All three services sponsored research work that sought to apply the emerging technology of digital computers to the problem. Recall from chapter 4 that, by 1953, the Air Force had completed testing on the prototype of what would later become the SAGE Air Defense System.

[945] Ibid., 71. What explains the Army's lack of interest in code making and codebreaking during the interwar years? Land armies could rely on hardwired telegraph and telephone communications for their long distance messaging, whereas forces afloat had to rely exclusively on radio. In reflection of this fact, between 1921 and 1941, the Navy spent three to five times as much on radio intercept and codebreaking activities as did the Army.

[946] Ibid., 71-73.

[947] Ibid., 77. See also David L. Boslaugh, *First-hand: No Damned Computer is Going to Tell Me What to Do — the Story of the Navy Tactical Data System*, from Engineering and Technology History Wiki, last edited February 27, 2017, chapter 2, https://ethw.org/First-Hand:The_Navy_Codebreakers_and_Their_Digital_Computers_-_Chapter_2_of_the_Story_of_the_Naval_Tactical_Data_System.

projects, one in the Army and one in the Navy, would provide the technological breakthroughs to make this wish a reality. The first such development was called the ENIAC, or Electronic Numerical Integrator and Computer.[948] Built in December 1945 to solve the increased demand for ballistic range tables for Army artillery, the ENIAC eventually became the even more general purpose EDVAC, or Electronic Discrete Variable Computer, which in 1948 became the Universal Automatic Computer, or UNIVAC.[949] The ENIAC, EDVAC, and UNIVAC led to an increased awareness within the defense scientific establishment of the potential for digital computers to solve other pressing defense problems.

The second development concerned the Navy's need for flight simulator that could simulate the dynamics of a newly designed aircraft without having to build and fly the airplane. While this flight simulator was originally intended to be an electronic analog computer, the Army's ENIAC machine convinced the program engineers that a digital computer would provide a better solution.[950] The project, called WHIRLWIND, was approved in 1946 at an estimated cost of $1.2 million.[951]

The twin computing achievements of WHIRLWIND and the EDVAC provided the inspiration for the development of a general purpose Navy codebreaking machine.[952] In August 1947, the Navy assigned a contract for the development of a machine called the Atlas, a new codebreaking computer that would be patterned on the WHIRLWIND's architecture. The Atlas I was delivered to CSAW in December 1950. When the CSAW and Army Security Agency merged to form the Armed Forces Security

---

[948] Boslaugh, *When Computers Went to Sea*, 78. See also John W. Mauchly, "Mauchly on the trials of building ENIAC," *IEEE Spectrum*, Vol. 12, No. 4 (Apr. 1975): 70-76.

[949] Ibid., 79-81. Ballistic range tables calculated how far a projectile would travel for given angles of gun elevation based on adjustments in variables such as projectile weight and powder charge, and served as essential references for artillerymen. However, the slow process of performing manual calculations, even with large teams of "human computers," meant that by early 1943, new guns were being deployed to theater without completed range tables. It could take up to a month to produce a range table by hand. From Scott McCartney, *ENIAC - The Triumphs and Tragedies of the World's First Computer* (Walker and Company, New York, 1999), 53-54, 101.

[950] N. Metropolis, J. Howlett, and Gian-Carlo Rota, eds., *A History of Computing in the Twentieth Century* (Orlando: Academic Press, 1980), 365.

[951] Boslaugh, *First-hand*, ch. 2. While the Navy nearly scrapped the project in 1949 due to an increase in cost and a decrease in demand, the 1949 Soviet detonation of an atomic bomb caused the Air Force to look to WHIRLWIND as the digital foundation for a continental air defense system. WHIRLWIND thus became the heart of the Air Force's development of SAGE.

[952] Ibid., ch. 2.

Agency in 1951, and later joined the newly formed National Security Agency in 1952, the Navy's Atlas code-breaking computer was chosen to serve as the backbone of the nation's joint cryptologic efforts.[953]

Inspired by the technological achievements of WHIRLWIND, EDVAC, and Atlas, the Navy began to envision a system which could automate both the radar plotting functions of the Combat Information Center and the weapons assignment function of the fighter direction team. The proposed system was called the Naval Tactical Data System (NTDS). The NTDS was to collect data from a number of shipboard sensors, and to then correlate it with target data received from other units to present as a clear picture of the air tactical situation.[954] By April 1960, the Navy had established a computer programmer school to train a cadre of military programmers ready to man the new system.[955] By late 1961, the *USS Oriskany* became the first aircraft carrier to receive the new NTDS.[956]

Reception of the system was initially lukewarm, if not outright negative. During testing, an informal survey showed that naval officers opposed the system by a margin of 20 to one. The source of officers' resistance was twofold: a poor understanding of what the NTDS was designed to do, and a fear of the potential loss of autonomy that would occur should an officer have to share his command authority with a computer. In a reflection of the extent to which independent command at sea remained ingrained in the service psyche, there was a palpable sense among commanders that "no damned computer was going to tell me what to do," and "no damned computer was going to fire my missiles."[957] However, by 1964, when the first five NTDS-equipped ships went into operation, some of the senior officers who had used NTDS began to speak favorably of the new system.[958]

---

[953] Boslaugh, *When Computers Went to Sea*, 98.

[954] Ibid., 183.

[955] Ibid., 208.

[956] Ibid., 213.

[957] Ibid., 243.

[958] Ibid., 259.

From 1961 to 1969, led by the NTDS, digital computers were being introduced to an increasing number of shipboard systems.[959] By 1980, NTDS operational capabilities had grown substantially. A system which was originally developed to support anti-air warfare was also supporting anti-submarine warfare, anti-surface warfare, electronic warfare, and amphibious missions.[960] The ability of the NTDS to automate and synchronize routine naval functions, and to dramatically increase naval warfighting performance as a result, later inspired the idea for the Aegis advanced surface missile system program. Initially begun in the late 1960s, the Aegis project was concerned about fast moving, low-flying aircraft or missiles that might hit a target ship mere seconds after detection. It therefore demanded a higher degree of automation than what was provided by the NTDS — namely, by feeding targets directly into the fire control computer upon detection, rather than processing all targets through a separate threat evaluation function before assigning them to a weapons system. NTDS functions were eventually pulled into the Aegis system. This process turned Navy warships into floating, computerized, and largely automated weapon systems that have proven highly effective since the system was first introduced in 1974.[961]

SUMMARY: COMMUNICATION AT SEA AND THE DIGITIZATION OF THE U.S. NAVY

The above history suggests that computers and computing technology were introduced into the Navy as a way to solve a series of operational problems that were unique to the nature of war at sea. The first such problem concerned the need to develop a system of reliable communication that was capable of transmitting messages over the increasingly vast distances that ships, and later aircraft, could travel. This led to the development of RF technology that could transmit signal wirelessly. Radio technology quickly evolved into radar technology, which made it possible for a commander to maintain awareness of events

[959] Boslaugh, *When Computers Went to Sea*, 368.

[960] Ibid., 388.

[961] Boslaugh, *First-hand*, ch. 9.

in an increasingly broad battlespace just as aircraft began to shrink the time scale and expand the range scale of maritime warfare.

The introduction of radar presented the Navy with new information management problems that were exacerbated by simultaneous improvements in attacking technology.[962] The need to manage this information overload led first to the Combat Information Center in the 1940s, and then to the digitized and automated Naval Tactical Data System in the 1960s. The task of information management has remained a central service challenge at the center of U.S. naval operations ever since.

Concurrent to the development of radio was the development of ways to exploit it. The vulnerability of signals in transit led to the growth of cryptology and cryptography, which in turn drove the need for automated methods of code breaking during and immediately following World War II. Moreover, the critical role that cryptology played in the Navy's World War II successes, particularly at the Battle of Midway, marked the beginning of a rich heritage and historical legacy for the cryptologic community that has continued to the present day. Navy cryptologists, and the intelligence community from which they arose, have since enjoyed a level of institutional prestige in the Navy that their peers in other services do not.

Several critical breakthroughs in computing technology were driven by the needs of the cryptologic community, and enabled the later development of the Naval Tactical Data System. However, the gradual embrace of computers that resulted, and that culminated in the later adoption of the Aegis combat system, was not without its challenges. Foremost among these challenges was the fact that naval officers, raised in a tradition of independent command at sea, were reluctant to cede autonomy to a system they did not understand. It took the highest levels of naval leadership to make the NTDS vision a reality.

What insights might the above history provide about the Navy's eventual approach to cyberspace? First, the development of computers and computing technology affirms the Navy's institutional emphasis

---

[962] Boslaugh, *When Computers Went to Sea*, 56.

on, and operational need for, the principles of assured communication at sea, reliable command and control, and effective information management. Each of the technologies described above emerged in response to one of these three problems. While these challenges are not unique to the Navy as a military service, the extent to which modern maritime operations are contingent upon resolving them is such that they continue to exert an outsized influence on central service thinking. Second, the development of computers in the Navy was intimately tied to the emergence of a strong naval cryptologic community. The strength and influence of this community — both inside and outside of the naval service — would play a significant role in the trajectory of later cyberspace operations development.

Naval Information Theories of the Post Cold War

SPACE AND ELECTRONIC WARFARE

The development of increasingly complex and independent sensors and communication systems in the aftermath of World War II led to a need to network these systems together. The resultant networking efforts, epitomized in the NTDS and Aegis weapon system, allowed the entire fleet to function as a single networked and increasingly automated organism rather than as a collection of individual ships. Communications platforms connected sensors and intelligence fusion centers to the fleet task force, which used these assets to expand the range of effective surveillance and command and control capabilities. By the early 1980s, enabled by improvements in computer and satellite technology, the product from these national and naval sensors began to flow seaward. By the last two decades of the twentieth century, the growth and proliferation of the microprocessor computer, combined with the sophistication of shore-based sensors, had finally made global surveillance and electronic warfare a possibility for naval forces.[963] With that possibility came more concerted efforts to develop the C3I architecture to support it.[964]

---

[963] Recall that the terminology for command and control in the 1980s and 1990s moved from command, control, communications, and intelligence (C3I) to command, control, communications, computers, and intelligence (C4I).

[964] Michael S. Loescher, "Copernicus Offers a New Center of the Universe," *Proceedings* Issue 117 (January 1991).

These technological changes are aptly summarized in a report published by the Office of Naval Research in 1988. Called "Navy 21: Implications of Advancing Technology for Naval Operations in the 21st Century," the report discussed how advances in technology would impact the next thirty to fifty years of naval warfare. The report argued that the routine nature of global military surveillance would cause the battle space for naval forces to continue to expand, such that forces would have to cover more area while becoming more tightly integrated through an interconnected information system. As a result of this expanded battle space, the central command and control challenge for blue water navies would become less the mechanical process of communication itself, as it had been for the preceding decades, than the act of buying space and time through early indications and warnings of enemy activity. Intelligence fusion and over-the-horizon targeting — the ability to identify and engage with platforms well beyond line-of-sight — were thus expected to assume a central role in future sea control.[965] Accordingly, the report predicted that "the contest for information will dominate maritime warfare" over the next several decades.[966]

The convergence of these technological changes only increased the importance of surveillance, counter-surveillance, and combat information systems to naval operations. In other words, the operational consequences of technological change increased the sense of urgency behind the Navy's need to properly harness the riches of the information environment. In a sense, it could be said that these emerging technologies took the same problems that were endemic to naval warfare during World War II and simply expanded them to a much larger geographic area.

In an effort to take advantage of both the pitfalls and the potential of the information environment, in the late 1980s the Navy developed a concept called Radio-Electronic Battle Management (REBM), later redesignated Space and Electronic Warfare (SEW). SEW referred to the use of space and the electromagnetic spectrum to target enemy decision-making systems and disrupt adversary command

---

[965] "Implications of Advancing Technology for Naval Operations in the Twenty-First Century Volume 1: An Overview (Navy-21)," (Washington DC: National Academy Press, 1988), 43.

[966] Ibid., 21.

and control. As such, it encompassed a variety of functions, from intelligence and command and control to communications, electronic warfare, and targeting.[967] The advent of SEW represented a primitive recognition that the information domain demanded its own set of operational principles, and that the Navy would need to learn how to operate both offensively and defensively within it.[968]

In 1989, the Chief of Naval Operations formally designated SEW as a Navy warfare mission area — a designation which, in theory, granted operations in space and the electromagnetic spectrum the same sense of institutional urgency as the Navy's traditional warfare areas of surface, subsurface, and aviation operations.[969] Organizational changes followed shortly on the heels of this new designation. On 1 August 1991, the Navy's Space, Command, and Control Directorate, OP-094, was renamed the Space and Electronic Warfare Directorate. Vice Admiral Jerry O. Tuttle, who had directed OP-094 since May 1989, and who was long considered a visionary in the field of information warfare, remained in charge of the organization. The creation of the Space and Electronic Warfare Directorate was intended to structurally reaffirm the 1989 declaration that space and electronic warfare were considered a new warfighting area on par with surface, air, and undersea warfare. Importantly, the move also gave SEW an organizational home and a high-powered advocate. The stated goal of OP-094 was to improve the Navy's ability to conduct over-the-horizon targeting by creating the systems and architecture necessary to transmit processed data to fighting units at sea. The organization's proposed architecture would enable the simultaneous and continuous fusion of targeting data both ashore and afloat.[970]

---

[967] Doctrinally, SEW referred to the integrated use of OPSEC, surveillance, C4I, signals management, MILDEC, counter-surveillance, counter-C4I, and electronic combat to target both enemy decision-makers and the systems they relied upon. In this integration, it was similar to other theories of command and control warfare.

[968] Michael S. Loescher, "Space and Electronic Warfare: A Navy Policy Paper on a New Warfare Area," (Washington DC: Director, Space and Electronic Warfare, June 1, 1992).

[969] Ibid.

[970] The system in use at the time transmitted large quantities of unprocessed data to ships, with the (unreasonable) expectation that ships would be able to effectively process the data themselves. John F. Morton, "Space and Electronic Warfare Comes of Age," *Proceedings* Issue 117 (January 1991).

The Navy followed this staff realignment with the creation of a new billet at sea under the composite warfare commander (CWC) concept.[971] Called the Space and Electronic Warfare Commander (SEWC), the billet allowed a single naval officer to serve as the principle advisor to the battlegroup commander for friendly and enemy use of the electromagnetic spectrum. The SEWC was responsible for force emissions control restrictions, monitoring intelligence and surveillance sensors, and developing operational deception plans as appropriate.[972] The SEWC was an evolution of the electronic warfare coordinator position of the 1970s, and later evolved into the C2W commander in the mid-1990s.[973] This position was eventually elevated to a captain's billet, thus putting it nominally on par with the other warfare commanders who reported to the battlegroup commander.

INFORMATION WARFARE

The post Desert Storm period also saw a shift in terminology from space and electronic warfare to information warfare. However, there was significant disagreement over what this new term actually meant. In 1995, Commander George Kraus Jr. argued that the Navy suffered from the lack of a coherent organizational approach to offensive and defensive considerations for information warfare. In dealing with information warfare, Kraus argued, the armed forces had adopted an approach that was akin to "polishing the stovepipes," or working to improve performance elements within the current organizational structure rather than considering new capabilities that might not fit within that structure. Tellingly, he offered that "The military has viewed information services as supporting inputs to the actual warfare

---

[971] The CWC concept is the command structure used to govern the various assets found within a Navy strike group. The CWC concept takes the most critical missions of warfighting at sea and divides them among O6 commanders, all of whom report to the overall strike group commander. The model relies upon command by negation, in which subordinate commanders are empowered to act as needed within their respective mission unless told otherwise. For example, the commander of an air defense cruiser would typically receive the CWC designation of air warfare commander, with responsibility for all aspects of air defense for the formation in addition to his duties commanding his own ship. Likewise, the SEW commander would have responsibility for all aspects of both offensive and defensive use of the EMS within the strike group. See "Ready-for-Sea Modular Course and Handbook," (San Diego: Naval Reserve Intelligence Program, April 9, 1999), 51-53, https://fas.org/man/dod-101/navy/docs/rfs4/ready.pdf. and Annex 3-04 Countersea Operations. "The Navy Composite Warfare Commander," Curtis E. LeMay Center for Doctrine Development and Education, November 7, 2014.

[972] "Ready-for-Sea," 54.

[973] "Comments and Discussion," *Proceedings* Issue 122 (November 1996). The C2W billet was usually filled by a cryptologist (William Leigher, telephonic interview with the author, November 13, 2018).

functions of fire, maneuver, and strike. But information warfare might not always be a supporting function; in some future campaigns, it might take a leading role."[974]

A 1996 article advanced this sense of disagreement with its argument that, "There is no universally agreed-upon definition of information warfare. An underlying foundation of most definitions is that information warfare is conflict in which information is the resource, the target, and the weapon, all at the same time."[975] In 1997, another author criticized the lack of systemic understanding of information warfare that stemmed in large part from the use of "expansive metaphors" that muddle efforts to establish a clear definition.[976] Perhaps the most scathing indictment came from John L. Peterson, who argued that "much of the thinking about future information warfare looks like little more than traditional military missions embellished with new information technology. Essentially, future warfare is seen as using the extraordinary characteristics of information technology to do a better job of breaking things and killing people."[977]

Unlike the Army and Air Force, however, the Navy did not publish any authoritative doctrine in the post Gulf War period to resolve these debates. However, this dearth of doctrinal development regarding the new concept of information warfare did not keep the Navy from making progress

---

[974] George F. Kraus Jr., "Information Warfare in 2015," *Proceedings* Issue 121 (August 1995).

[975] William E. Rohde, "What is Info Warfare?" *Proceedings* Issue 122 (February 1996).

[976] Robert D. Gourley, "The Devil is in the Details," *Proceedings* Issue 123 (September 1997).

[977] John L. Petersen, "Info War: The Next Generation," *Proceedings* Issue 123 (January 1997).

organizationally.[978] In the early 1990s, the Navy created a small organization within its service cryptologic element called the Naval Information Warfare Activity (NIWA).[979] Embedded within the Naval Security Group, NIWA was headquartered at Fort Meade, Maryland and was closely linked to the National Security Agency.[980] The organization began as a small, informal cadre of hand-selected technical personnel who were assigned to work on a highly classified strategic problem.[981] The production of real capability in response to this and other challenges led to the organization's eventual establishment as a separate entity within the Naval Security Group. By the early 2000s, NIWA had grown in size to between 400 and 500 people, many of whom were officers selected for their technical backgrounds.[982]

As a result of a unique designation that allowed it to circumvent ordinary defense acquisition and regulatory processes, NIWA had an unusual level of flexibility that made it an invaluable player for Navy cryptologic research and development.[983] In its role as the service's chief technical agent for the pursuit of information warfare-related technologies, NIWA was responsible for designing solutions to some of the

---

[978] Recall that the post-Gulf War years saw the creation of FM 100-6, *Information Operations*, in the Army and *Cornerstones of Information Warfare* in the Air Force, both of which helped to influence the development of the first joint doctrinal publication on information warfare, JP 3-13.1, *Joint Doctrine for Command and Control Warfare*. Why did the Navy's doctrinal development on information warfare lag behind that of the other services in the post-Gulf War period, given that all were involved in the same conflict and ostensibly drew similar joint lessons? One could partially attribute the service's conceptual lag to its service-wide reluctance to embrace doctrine in general. Culturally, the Navy has long harbored a fear that doctrine would curtail freedom of action at sea by constricting what a ship's captain could or could not do. Operationally, the nature of naval warfare — towards freedom or denial of use rather than possession of terrain — inclines officers to rely more upon the strategic foundations of their service rather than the tactical ones. Thus, a naval officer will be more inclined to cite Mahan or Corbett than he will Naval Doctrine Publication 1. It is telling, for example, that the Navy did not establish a center for doctrine development until September 1992, which opened in March of 1993. Consider also the Navy's unique relationship with the idea of jointness. Unlike the Army and the Air Force, "joint" to the Navy means that it provides support to the other services but does not (or cannot) receive the same support in kind for its engagement in maritime warfare. Thus, jointness to the Navy is seen as something of a one way street. (Zimmerman et al., *Movement and Manewer*, 74). Finally, the nature of the Navy's participation in Desert storm was such that it "served as a reminder of their diminished relevance in a world where U.S. adversaries were rogue states with small or nonexistent navies." The service's resistance to the joint approach fostered by Goldwater Nichols led to its lackluster contribution to the air campaign in Desert Storm. (Zimmerman et al., *Movement and Manewer*, 198).

[979] I was unable to obtain the official date of NIWA's creation. Former NIWA veterans speculated that a secretive precursor to the organization began sometime in the 1980s. The lineage of Naval Information Operations Center (NIOC) Suitland, which NIWA became on 1 October 2005, places the origins of NIWA in July 1994. It is possible that this date marked the organization's unclassified founding, with a classified history extending several years prior.

[980] "Naval Information Warfare Activity Was Established in July 1994," Station Hypo, accessed January 22, 2019, https://stationhypo.com/2017/07/22/navy-information-warfare-activity-was-established-in-july-1994/.

[981] Early details of the organization's creation, to include the date it was founded and its original purpose, remained unobtainable through unclassified means.

[982] Whiton, Tighe, interviews.

[983] Whiton, interview.

service's harder technical problems in the realm of cryptology and information warfare.[984] One such prototype in the late 1990s was a dual-use SIGINT system, eventually adopted Navy-wide, that allowed for cryptologic exploitation and attack from surface, subsurface, air, and land platforms.[985] Over time, NIWA evolved into what is today the Navy Cyber Warfare Development Group (NCWDG), which holds the preponderance of the Navy's Cyber Warfare Engineers and the bulk of its cyberspace development capability.

In addition to its close partnership with the National Security Agency, NIWA collaborated with two other Navy organizations that were important to the early years of naval information warfare. The first was the the Navy Space and Naval Warfare Systems Command (SPAWAR).[986] SPAWAR was established on May 9, 1985 as the Navy's acquisition command for systems related to C4ISR, space, and information technology.[987] SPAWAR was the redesignation of an organization called the Naval Electronic Systems Command (NAVELEX).[988]

Whereas NAVELEX focused on the development, testing, operation, and maintenance of naval electronics, SPAWAR assumed an expanded responsibility for all aspects of the Navy's information warfare mission, with a focus on designing systems for the total battle force instead of just individual platforms and weapons.[989] As such, SPAWAR conducted large-scale acquisition for the types of

---

[984] On NIWA's roles and responsibilities, see "Comments and Discussion," 1996, and "Naval Information Warfare Activity Was Established in July 1994." NIWA was designated as a "reinvention laboratory" during the Clinton years, which afforded it special funding opportunities (Whiton, interview).

[985] Michael D. Brown, telephonic interview with the author, January 3, 2019 and Tighe, interview.

[986] In June 2019, SPAWAR changed its name to NAVWAR, for Naval Information Warfare Systems Command. See Barry Rosenberg, "Why is SPAWAR Now NAVWAR? Networks and Cyber Warfare," Breaking Defense, June 5, 2019, https://breakingdefense.com/2019/06/why-is-spawar-now-navwar-networks-cyber-warfare/.

[987] "Space and Naval Warfare Systems Command History: 1966 to 2007," January 23, 2019.

[988] Ibid., 2. NAVELEX was created on 20 June 1966. It exercised overall program responsibility for the development, testing, operation, and maintenance of shore electronics; shipboard electronics; airborne navigational, meteorological, and communications equipment; satellite communications and space surveillance systems; shore-based strategic data systems; and general purpose electronic test equipment. NAVELEX was especially useful for the Navy's small space program, which was responsible for maintaining their space surveillance and satellite navigation system.

[989] Ibid., 4. See also "Records of the Naval Electronic Systems Command," National Archives, accessed January 28, 2019, https://www.archives.gov/research/guide-fed-records/groups/345.html.

information warfare prototypes that were developed in NIWA labs.[990] As more and more hardware for the fleet was purchased through commercial-off-the-shelf vendors, SPAWAR developed a close partnership with the commercial industry.[991] This partnership allowed it to play an instrumental role in the fielding of later Navy network initiatives, to include IT-21, NMCI, and ForceNet.[992] In the words of one former commander, "From the bottom of the oceans to the edges of space, SPAWAR provides an integrated web of sensors and communications systems that supply the warfighter with the information superiority needed to win."[993] However, the mission of SPAWAR made it a lucrative target for computer attacks in the late 1990s, with almost a dozen computer attacks a day and a March 1998 denial of service attack that hit about 100 SPAWAR computers.[994]

The second organization with which NIWA maintained a close relationship was called the Fleet Information Warfare Center (FIWC). In its capacity as an interface to the operational fleet, FIWC would take the capabilities developed by NIWA and acquired by SPAWAR and figure out how to employ them fleet-wide.[995] Created in response to the reluctance of the service cryptologic enterprise to fully embrace the information warfare mission set for the long term, FIWC began in 1994 as a handful of contractors and naval officers.[996] Out of 30 personnel spots initially requested, only three were granted; this number had grown to eleven by March of 1997.[997] FIWC had a number of assigned missions that were focused on operationalizing both the concepts and technologies that comprised the Navy's nascent information

---

[990] "Comments and Discussion," 1996.

[991] "Space and Naval Warfare Systems Command History: 1966 to 2007," 12.

[992] Ibid., 10-12.

[993] Ibid., 12.

[994] Ibid., 9.

[995] "Comments and Discussion," 1996.

[996] "Reluctance of the service cryptologic enterprise" from Andrew Singer, telephonic interview with the author, December 12, 2018. "Handful of contractors and naval officers" from Jim Grainger, telephonic interview with the author, September 12, 2018.

[997] Grainger, Weatherford, interviews. That only three of thirty slots were granted came from U.S. Government Accountability Office, *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*, GAO/AIMD-96-84, (Washington, D.C., 1996), 38.

warfare capabilities. These missions included the development of information warfare tactics and doctrine, training information warfare staffs, fielding realistic opposition forces for fleet exercises, the remediation of computer incidents, and operating a defensive computer protection laboratory. However, in a reflection of the lack of doctrinal certainty on what did and did not comprise information warfare, FIWC also had responsibility for an eclectic group of missions that included the Navy's electronic warfare libraries, unmanned systems, and psychological operations planning.[998]

From a network support standpoint, FIWC was primarily concerned with system security and information assurance, though it did conduct limited support to offensive missions through joint and interagency task forces.[999] In support of its network security mission, FIWC became the parent organization for the Navy Computer Incident Response Team (NAVCIRT) in October of 1995. Like FIWC, NAVCIRT was another organization with humble beginnings: it started with five people in the information warfare-defensive division of FIWC and eventually grew to 250 people before its 2003 merger with the Navy Component Task Force-Computer Network Defense (NCTF-CND).[1000] FIWC also worked with other service, agency, and commercial incident response teams to conduct intrusion detection and incident reporting, and provided assistance to Navy network administrators to secure their networks through vulnerability testing and patch fielding. Of note, FIWC maintained a close partnership with Naval reserve forces to maintain the security of publicly accessible websites. Select reservists would use their scheduled drill periods to access and review each of the Navy's over 1500 public websites every year. These reviews encompassed administrative, privacy, and OPSEC requirements, and used web tools to generate automatic deficiency notices that allowed webmasters to correct problems in real time.[1001]

---

[998] Leigher, interview.

[999] Grainger, interview.

[1000] "Navy Cyber Defense Operations Command Celebrates Past, Present, Future," Navy.mil, February 11, 2016, https://www.navy.mil/submit/display.asp?story_id=93055.

[1001] U.S. Congress, House, Armed Services Committee, *Information Technology: An Examination of DoD Network Vulnerabilities*, May 17, 2001.

The Navy's decision in 2002 to establish Information Operations as a primary warfare area reinforced the importance of FIWC as the service's warfare center of excellence for information operations.[1002] Concurrent to this announcement, control of FIWC realigned from the Naval Security Group to the newly established Naval Network Warfare Command (NETWARCOM). In 2005, following the merger of Naval Security Group with NETWARCOM, FIWC merged with the Navy's signals intelligence center in Norfolk, Virginia to create the Naval Information Operations Command (NIOC) Norfolk.[1003] NIOC Norfolk remains the service's center of excellence for information operations and information warfare.

The structural reorganization exemplified by the creation of NIWA and FIWC also carried over onto the Navy staff. In 1992, the Navy replaced its OP codes on the OPNAV staff with N codes. This realignment led to the creation of the N6 Directorate of Space and Electronic Warfare and the N64 Directorate of Information Warfare. The new structure was designed to replace competition among resource sponsors with cooperation and dialogue in order to enhance the Navy's approach to the information space.[1004] These reorganizations also led to the creation of the N3/N5 Strategy and Concepts Branch, which would serve as home to some of the cryptologic community's efforts to operationalize computer network operations in the late 1990s.[1005]

[1002] Roughead, interview.

[1003] "NIOC Norfolk's History," U.S. Fleet Forces Command, accessed January 16, 2019, https://www.public.navy.mil/fltfor/iwtgnorfolk/Pages/NIOCNorfolkHistory.aspx.

[1004] "Comments and Discussion," 1996. OPNAV underwent significant structural reorganization in 1992. In keeping with joint staff practice, all "OP" codes were changed to "N" codes, and the staff was reorganized to reflect more fully the so-called "Napoleonic" staff-code usage of the U.S. Army and the Joint Staff. This realignment led to the creation of the N6 Director for Space and Electronic Warfare, underneath which emerged the N64 Directorate of Information Warfare. The new staff model was intended to foster cooperation and dialogue among the different resource sponsors, rather than competition. "We designed the structure to build operations and consensus," ADM William Owens, OPNAV N8 1992-1994. See Peter M. Swartz and Michael C. Markowitz, "Organizing OPNAV (1970-2009)," report prepared for the Department of the Navy Naval History and Heritage Command by CNA Analysis and Solutions, 54, https://www.cna.org/cna_files/pdf/D0020997.A5.pdf.

[1005] Swartz, "Organizing OPNAV," 62.

NETWORK-CENTRIC WARFARE

By the late 1990s, the combination of new information theories and increasingly sophisticated information technologies converged into the concept of network-centric warfare. First articulated as a distinct concept by Vice Admiral Arthur K. Cebrowski in a 1998 *Proceedings* article, network-centric warfare was based upon the premise that interconnected communications technology would enable warfighters to achieve information superiority on the battlefield.[1006] Cebrowski defined information superiority as the state in which relevant, accurate information arrives in the hands of those who need it faster than it would for one's adversaries.[1007]

The theory of network-centric warfare regarded interconnected networks not simply as combat support systems, but as weapon systems in and of themselves.[1008] Several first principles emerged from this theory that would influence the Navy's subsequent approach to both information in general and network technologies in particular. First, network-centric warfare was predicated upon the notion that information superiority had become a precursor to military power. Thus, network-centric warfare sought to translate an information advantage, enabled by superior information technology, into a competitive advantage through the robust computer networking of geographically dispersed forces.

However, in order to enact this transition from raw information to competitive advantage, network-centric warfare demanded a shift in naval thinking from the massing of platforms to the massing of effects. Information-age technological advancement meant that industrial-age measures of military might would no longer provide sufficient indication of military effectiveness. Instead, the sophistication of the new communications systems that linked these traditional military platforms, and that thus dictated the speed with which information could travel from sensor to shooter, would prove far more important to

---

[1006] Arthur K. Cebrowski and John H. Garstka, "Network-Centric Warfare: Its Origin and Future," *Proceedings* issue 124 (January 1998). See also Nagy, "Network-Centric Warfare Isn't New" and Friedman, *Network-Centric Warfare.* For earlier iterations of similar ideas, see Loescher, "Copernicus."

[1007] U.S. Congress, House, Armed Services Committee, *Network-Centric Warfare and Information Security*, February 23, 1999, (statement by Vice Admiral Arthur K. Cebrowski, President, Naval War College).

[1008] "Space and Naval Warfare Systems Command History: 1966 to 2007," 22.

determining one's combat potential than raw kinetic power. Network-centric warfare thus demanded a balance of sensor, shooter, and information-based command and control capabilities that would allow the right information to arrive at the hands of the right people at the right time.[1009] It was not, importantly, about the generation of more information, but about the movement of information.[1010]

Executing network-centric warfare in practice required a high-performance information grid,comprised of linked communication and information systems that would enable the rapid transmission of tactically relevant sensor data between decision-makers and the weapons they employed.[1011] These requirements inspired a number of changes to the Navy's communications architecture throughout the late 1990s. The first, called IT-21, was a network initiative that sought to bring IP connectivity to all Navy units, both afloat and ashore. IT-21 began in early 1997 as an initiative to enhance U.S. Pacific Fleet communications through the introduction of networked personal computers.[1012] As the joint planning network for the Navy, IT-21 would enable faster cycles of command and control through the provision of a common network operating environment that would facilitate distributed collaborative planning.[1013] Vice Admiral Cebrowski described IT-21 as the Navy's umbrella strategy for enabling the underlying IT elements of network-centric warfare.

A second initiative that took its inspiration from network-centric warfare theory was the Navy Marine Corps Intranet, or NMCI. In October of 2000, Secretary of the Navy Richard Danzig announced the award of a six billion dollar contract to Electronic Data Systems Corps (EDS) to build and

---

[1009] James R. Fitzgerald, Raymond J. Christian, Robert C. Manke, "Network-Centric Antisubmarine Warfare," *Proceedings* Issue 124 (September 1998).

[1010] U.S. Congress, House, Armed Services Committee, *Network-Centric Warfare and Information Security*, February 23, 1999, (statement by Vice Admiral Arthur K. Cebrowski, President, Naval War College).

[1011] Fitzgerald et al., "Network-Centric Antisubmarine Warfare" and Cebrowski et al., "Network-Centric Warfare."

[1012] "Space and Naval Warfare Systems Command History: 1966 to 2007." Cebrowski's key contribution to the development of the Navy's approach to information was to collate emergent ideas into a coherent operational theory. The pieces behind these ideas were in place, albeit in dislocated form, well before the publication of Cebrowski's article, which is why IT21 can be called an offspring of Network-Centric Warfare theory even though its implementation preceded the theory's actual written articulation.

[1013] Robert M. Nutwell, "IT-21 Intranet Provides Big 'Reachbacks,'" *Proceedings* Issue 124 (January 1998), and J.M McConnell and Edward J. Giorgio, "Building Information Security Layer by Layer," *Proceedings* Issue 124 (December 1998).

maintain a department-wide intranet.[1014] The contract formed the basis of an effort to fix the Navy's fragmented network enterprise system, which had no standardization of either operating protocols or security measures across various Navy and Marine Corps network infrastructure. NMCI led to the consolidation of hundreds of individual Navy shore networks into a small number of core enterprise intranets.[1015] Control of network operations moved from individual local network providers to regionally operated network operations centers (NOCs), located at either a Naval Computer and Telecommunications Area Master Station (NCTAMS) or at one of the smaller Naval Computer and Telecommunications Stations (NCTS) that supported numbered fleet commanders.

In their respective efforts to expand the Navy's networking coverage and overhaul its network management, NMCI and IT-21 presented two sides of the same network-centric warfare coin. Whereas IT-21 was primarily a fleet-driven effort to improve ship-to-shore and ship-to-ship communication, NMCI focused on the Navy's regional shore communications infrastructure.[1016] Both, however, sought the same endstate: to improve naval operational effectiveness through seamless interconnectivity between the sources of information and their users.

A final network initiative was called ForceNet. ForceNet had its roots in the work of the Chief of Naval Operations' Strategic Studies Group, based at the Naval War College in Newport, Rhode Island. The group defined ForceNet as "The operational construct and architectural framework for naval warfare in the information age that integrates warriors, sensors, networks, command and control, platforms, and weapons into a networked, distributed combat force that is scalable across all levels of conflict from seabed

---

[1014] "Space and Naval Warfare Systems Command History: 1966 to 2007," 11. The Navy's decision to outsource NMCI management and maintenance to contractors was a reflection of the service's lack of a dedicated communications community (Steve Parode, interview with the author, September 25, 2018).

[1015] Charles L. Munns, "A Global Navy Needs a Global Network," *Proceedings* Issue 129 (January 2003).

[1016] Archie Clemins, "It's More Than E-mail," *Proceedings* Issue 126 (February 2000).

to space and sea to land."[1017] In other words, ForceNet was to serve as the final implementation of the theory of network-centric warfare.[1018]

NETWORK-CENTRIC PERSONNEL CHANGES

The proliferation of new network initiatives demanded a new type of network expertise. The Navy attempted to create this expertise with the Information Professional (IP) officer community and the enlisted Information Technician (IT) rating in the late 1990s and early 2000s. Prior to its founding, the Navy did not have a dedicated cadre of communications specialists, nor did it have a systematic method of identifying, training, or retaining communications talent. Instead, it relied upon an eclectic group from various communities to fulfill communications functions both afloat and ashore.[1019]

Before the Navy lifted its restrictions on women in combat in 1995, shore communication duties fell largely to members of the General Unrestricted Line Community (GURL). At its founding, the GURL community was the primary place where female officers were able to serve, and it consisted of three professional core competencies: logistics support; manpower, personnel, and training; and space and electronic warfare, which encompassed the management of naval communications and information systems.[1020] Communications duties ashore remained largely within the purview of this community after its redesignation as the restricted line in January 1995.

Afloat, communication duties were often performed as an additional duty or an additional tour of duty by warrant officers, limited duty officers, and unrestricted line officers — few of whom received any formal training in the management of communication systems. While there were some notable efforts to cross-train officers in communications, such as the surface warfare community's five week basic

---

[1017] Richard W. Mayo and John Nathman, "ForceNet: Turning Information into Power," *Proceedings* Issue 129 (February 2003). Robert Bebber, "Cryptology at a Crossroads," *Proceedings* Issue 141 (March 2015).

[1018] "Space and Naval Warfare Systems Command History: 1966 to 2007." It is important to note that all services were undergoing upgrades to their communications infrastructure at the same time; the Navy was not unique in this regard.

[1019] Barrett, "Developing a Community."

[1020] Graham, "Does the Navy Need the 1700 Community?"

communications course at Newport, Rhode Island, such courses were not intended to create subject matter experts, and were not required by members of other warfighting communities.[1021] This ad hoc approach to communications management resulted in the development of small pockets of specialization across a broad spectrum of designators. However, there was no central ownership of these specializations as a whole, nor were there centralized training mechanisms to ensure standardization of expertise.

In November 1999, the Navy attempted to rectify this deficiency through the redesignation of the Radioman (RM) rating to the Information Systems Technician (IT).[1022] The rating consisted primarily of former radiomen and data systems technicians, and was designed to create a cadre of network systems engineers who could properly steward the Navy's substantial network overhaul initiatives.[1023] This was followed shortly thereafter by the creation of the information professional officer community in 2001. Comprised of restricted line officers, the community was responsible for operating, maintaining, and securing Navy networks.[1024]

SUMMARY: NAVY INFORMATION THEORIES OF THE POST COLD WAR

The experience of Desert Storm in 1991 reinforced many of the Navy's ideas on the importance of information, and on the subsequent need for the service to develop ways to conquer space and the electro-magnetic spectrum.[1025] The resultant conceptual evolution from radio-electronic battle management to space and electronic warfare to network-centric warfare shows how Navy senior

---

[1021] Barrett, "Developing a Community."

[1022] "Space and Naval Warfare Systems Command History: 1966 to 2007," 10.

[1023] 2000 Comments and Discussion; scope of duties from "Information Systems Technician," Navy.mil, updated February 2, 2019, https://www.public.navy.mil/bupers-npc/enlisted/community/crypto_it/Pages/IT.aspx.

[1024] "Comments and Discussion," *Proceedings* Issue 126 (July 2000).

[1025] William A. Dougherty, "Storm from Space," *Proceedings* issue 118 (August 1992). One Navy commander wrote in 1992 that "just as overall command of the air is a precondition for taking and holding enemy territory, overall command of the electromagnetic environment is a precondition for taking and holding enemy airspace" (William J. Luti, "Battle of the Airwaves," *Proceedings* Issue 118 (January 1992). Another author argued in 1993 that Desert Storm offered a clear demonstration of the principle that information would be the service's most potent weapon in the future (John Peterson, "Info Wars," *Proceedings* Issue 119 (May 1993). Many of the articles written on information during this post-Gulf War period were written by members of the Navy's traditional warfighting communities. In this way, conceptual development within the Navy on the subject of information warfare paralleled that which was taking place in the other services.

leadership approached the intersection of information and naval operations during the last two decades of the twentieth century. Each of these warfare theories led to structural changes in how the Navy organized for network operations and in how it managed its network-savvy personnel. Furthermore, the theory of network-centric warfare in particular led to a substantially renewed interest on networks as a source of connectivity. That connectivity, in turn, became the epicenter of how naval strategists thought about naval power. In this regard, digital networks were simply the latest solution to the challenges of information saturation and information management that had faced the Navy since World War II.

The earliest intimations of cyberspace operations were hidden within the secretive Naval Information Warfare Activity under the auspices of the Naval Security Group. Similar to the Army's Studies and Analysis Activity, NIWA was originally founded to explore technical solutions to highly classified strategic problems against a nation-state adversary under the theoretical framework of command and control warfare. This mission made NIWA a natural repository for some of the Navy's top technical talent. As NIWA's mission evolved and its technological expertise accumulated, the Navy cryptologic community began to funnel its newly-minted computer network operators into the organization in the early 2000s, thus making NIWA the primary source of Navy support to national computer network operations. NIWA's initial emergence as an outgrowth of the cryptologic enterprise demonstrated the close relationship between signals intelligence and offensive information warfare in the Navy, and would hint at the later inseparability of cyberspace from the cryptologic community.

In addition to and separate from NIWA was the Fleet Information Warfare Center. FIWC emerged in 1995 as the answer to the Navy's question of where to put information warfare for the long term, after the service cryptologic element rejected an offer for responsibility of something whose definitional boundaries they had lost the ability to confine. With information warfare now separated from its initial cryptologic home, the focus shifted from offensively-minded command and control warfare to defensively-minded network security. As such, FIWC became the parent command for the Navy's Computer Incident Response Team, which was responsible for the detection and remediation of

computer incidents. It worked with fleet commanders and battle group commanders to perform aggressive red team efforts during joint task force exercises, and partnered with Navy reservists to maintain the security of the Navy's publicly accessible websites. It was thus in FIWC that the emergence of computer network operations as such grew most explicit, albeit in a primitive and largely defensively-oriented form.

However, in a reflection of the general conceptual confusion that surrounded the service's understanding of information warfare, FIWC also had responsibility for portions of an eclectic mission set that included Navy unmanned systems, electronic warfare, space operations, and psychological operations. It was the Navy's failure to adequately define or conceptually unify the practice of information warfare — thereby allowing it grow boundlessly and encompass an ever-expanding set of functions — that cast the final vote on FIWC's, and by extension IW's, overall institutional irrelevance.

The Influence of Navy Cryptology

Concurrent to the theoretical development and organizational restructuring described above, in the late 1990s, the naval cryptologic community began a slow embrace of computer network operations in response to the natural technological migration of the practice of signals intelligence. This embrace mimicked a similar shift in the national cryptologic enterprise, to which, as the next section will show, the Navy had hitched its own service cryptologic element.[1026] The influence of this community on cyberspace operations development can be divided into roughly three phases. The first phase, spanning from the mid-1990s to 2001, was a period of realization hastened by certain visionary leaders who began to awaken to the realities of a changing technological landscape.[1027] The emergence of new communications

[1026] Initial exploration into the cyberspace realm at the national level also fell under the rubric of information warfare and later information operations. This exploration began most notably under the reign of Ken Minihan, who was a strong advocate for the development of a national information operations capability as DIRNSA in the late 1990s (Minihan, interview). This initial exploration focused mainly on the development of intelligence-related tools and capabilities rather than on the development of concepts or doctrine (Richard C. Schaefer, telephonic interview with the author, February 12, 2019).

[1027] This period really began in the early-to-mid 1990s, in line with a similar awakening that took place within the National Security Agency. However, it was not until roughly 1998 that leaders within the cryptologic community began to take concerted action to enact change.

technologies resulted in a need for new methods to exploit them. These new methods, in turn, would demand a new set of skills, which the commander of the Navy's service cryptologic element sought to develop through an expanded partnership with the National Security Agency. However, efforts to convince senior naval leadership of the importance of computer network operations, along with efforts to push related structural change, ultimately failed due to lack of interest in the capability and lack of understanding of what it could do.

September 11th, 2001 marked the beginning of a second phase of influence. In the years immediately following 9/11, the demand signal for computer network operations increased, even while widespread understanding of the capability did not. National counterterrorism efforts led to an increased appetite for all things digital, from the exploitation and attack of digital communication systems to new methods for processing the vast amounts of data that such exploitation amassed.[1028] The subsequent operational imperatives of the global war on terror provided the critical impetus that the naval cryptologic community needed in order to win over senior leadership. Discussions that had been circulating within the cryptologic community for several years — about the need for a cyberspace-focused career path, training program, capabilities, and units — began to gain traction both inside and outside of the community.[1029] It was during this period, from roughly 2001 to 2008, that the service created the first enlisted rating for cyberspace operations, the first training course, and the first cyberspace operations units. It was also during this period that the cryptologic community changed its name to information warfare in order to better reflect the operational focus that these new technologies demanded.

The third phase began in 2009, initiated by a series of significant structural reorganizations that were pushed by the Chief of Naval Operations himself. These reorganizations were intended to break the paradigm of the platforms by elevating information to a commensurate warfare area, thus forcing a reorientation of the Navy's operational focus. This period saw the creation of Fleet Cyber Command and

[1028] Sandra Brooks, telephonic interview with the author, January 16, 2019. The latter refers to the development of RT10 and RTRG.

[1029] Brown, interview.

Tenth Fleet, the consolidation of five separate communities into the Information Dominance Corps, and the merger of the Deputy Chief of Naval Operations for Intelligence, N2, with the Deputy Chief of Naval Operations for Communication, N6, into a single three star N2/N6 organization. However, while these major structural changes marked the beginning of new period of senior leader support for cyberspace and information operations, it also coincided with a waning cryptologic influence on how these changes would proceed: the Navy ultimately chose to subordinate cyberspace, as a subcomponent of cryptologic warfare, to a holistic concept of information dominance rather than elevate it as a separate warfighting domain that was deserving of its own cohort of technological warfighters.

PHASE 1: 1998-2001

In the early 1990s, as the technical landscape continued in its shift from analogue to digital, there proceeded a gradual recognition within the cryptologic community that the nature of signals intelligence collection was beginning to shift as well. Talk of information operations began to bleed into talk of computer network operations, followed by a realization that the cryptologic community would be best positioned to take ownership of this new mission due to its technical expertise and its natural familiarity with information technology infrastructure.[1030] By the late 1990s, discussion proceeded apace on how to develop the skills necessary to exploit the cryptologists' new operating environment.[1031]

In 1998, Admiral Winsor Whiton assumed command of the service cryptologic element, the Naval Security Group. A career cryptologist who had served as Ken Minihan's principle deputy at the National Security Agency, Whiton had been influenced by the preceding decades of thinking on how to exploit enemy communication systems.[1032] These theories had fallen under numerous titles throughout the years, from offensive electronic warfare in the late 1970s, to command, control, and communications

[1030] Brown, interview.

[1031] Ibid.

[1032] Whiton, Leigher, Minihan, interviews.

countermeasures (C3M) in the 1980s, to information warfare in the 1990s.[1033] Whiton had also been influenced by similarly revolutionary thinking within the national cryptologic enterprise. This thinking emphasized the active collection of intelligence at communication endpoints rather than passive collection at the midpoints.[1034]

Recognizing the prescience of many of these new ideas, in 1998, Whiton began an initiative designed to increase the Navy's investment in the national cryptologic enterprise. The intent of the initiative was to build Navy expertise in computer network operations by partnering with the national organizations that had the resources, access, and capability to execute those operations. What it meant in practice was that the Navy began to send more sailors to fill joint billets at the National Security Agency.[1035] Many of these sailors supported the NSA's information assurance mission through service on red teams, blue teams, and other aspects of active defense.[1036] This investment was substantial enough that one former information assurance director called Whiton's cryptologic sailors the backbone of NSA active defense.[1037]

Also in 1998, the Navy stood up an org in N3N5 that was focused on information operations. However, the majority of the organization's policy and doctrine work focused on computer network operations.[1038] Concurrent to Whiton's investment in the NSA were the aforementioned capability development efforts that were ongoing at NIWA, the bulk of which focused on how to make ships into cryptologic attack and exploit platforms.[1039] Thus, by the late 1990s, the cryptologic community was

---

[1033] In an interview, Whiton attributed the lack of clarity in thinking about these concepts to the lack of consistency in naming them.

[1034] Leigher, Whiton, interviews. Whiton had been Ken Minihan's principle deputy when Minihan was the DIRNSA.

[1035] Whiton, Brown, Leigher, Schaeffer, interviews.

[1036] Why the defensive investment? Combination of desire to increase proficiency in active defense with the fact that defensive money was what was available. These investments were funded by ISSP money, which focuses on information assurance and defense, rather than CSSP money, which fuels the active cryptologic enterprise (Brown, interview).

[1037] Michael J. Jacobs, telephonic interview with the author, January 11, 2019.

[1038] Brown, interview.

[1039] Leigher, interview.

engaged in a two-pronged effort to improve both its capabilities — through NIWA — and its expertise — through partnership with the NSA — in the new realm of computer networks.

By 1999, Whiton had developed a vision for how the Navy could best align itself to the demands of the current and future information environment. This vision entailed the consolidation of information-related communities and capabilities in a manner similar to what would transpire over a decade later with the creation of Fleet Cyber Command, the Information Dominance Community, and the consolidation of N2/N6. However, the problem of information operations was insufficiently pressing to convince Navy senior leadership of the need for significant structural changes, and Whiton's proposals fell flat. The rejection of the proposed structural changes stemmed largely from an immature understanding of the natural nexus that was forming between information-related fields. In spite of the information theorizing of the preceding two decades, the majority of naval leadership did not yet see the close overlap between cryptology, changing information technology, and traditional naval operations, and so could not see a justification for the type of change that would bring these fields into closer alignment.[1040]

In 2000, Whiton offered a briefing to the Chief of Naval Operations on the nascent field of computer network operations. In step with the thinking that had emerged within the National Security Agency, the cryptologic community had begun to define computer network operations as a single mission consisting of three separate components: offense, defense, and exploitation. Whiton argued that the Navy would need to improve its proficiency in each of these three components, with particular attention given to the offensive element, and that the cryptologic community was best suited to assume responsibility for this task. Senior leadership once again rejected the idea: with an insufficient understanding of computer network operations, they could see little need to divert limited resources to an unfamiliar and unproven capability. Undeterred, Whiton and his compatriots continued to build up their community's investment in the national cryptologic enterprise.[1041]

[1040] Brown, interview.

[1041] Contents of paragraph taken from an interview with Brown.

One of the most critical such investments came in the form of the Navy Remote Operations Center (NROC), which was a naval platform for Title 10 computer network operations built inside of an NSA facility.[1042] Around the year 2000, the closing of a handful of NSA bases and facilities resulted in the elimination of 450 service cryptologic billets. The cryptologists on OPNAV staff who had been working the computer network operations problem saw the 450 billets as exactly the opportunity for resources that their own service leadership had twice denied. The cryptologic community convinced the then-NSA Director General Michael Hayden to give these billets to the Navy. In exchange, the Navy would develop a cadre of sailors who were proficient in network operations through a substantial personnel investment in NSA work centers.[1043] Sailors would be individually assessed into these billets based on demonstrated technical aptitude and an analytical mind.[1044]

A portion of the resultant personnel investment went to a group called Tailored Access Operations (TAO), which at the time was the NSA's primary organization for computer network operations. This arrangement allowed sailors to gain proficiency in Title 50 computer network operations through their support to TAO, and TAO to reap the benefit of talent that they did not have to fund. However, the arrangement also made the Navy beholden to NSA processes and authorities, which were characterized by a high level of risk-aversion and a reluctance to employ tools in the service of anything that was not a national intelligence priority. These restrictions, and the Title 50 authorities from which they derived, were seen as unduly limiting to a service that was determined to create its own cyberspace capability for the independent prosecution of military targets. In response, the Navy's cryptologists struck a deal: in exchange for free manpower to support Agency operations, TAO allowed the Navy to set up its own, separate operations center called the NROC. The NROC provided the Navy with a separate infrastructure and launching platform in the event of an opportunity for a Title 10 cyberspace

[1042] Similar platforms were later built by the other services.

[1043] Contents of the paragraph taken from an interview with Amber Ryan.

[1044] Brooks, interview.

operation.[1045] In other words, it allowed the Navy to execute its own cyberspace operations with its own tools and infrastructure without risk of compromising national intelligence assets or priorities.

From roughly 1998 to 2001, cryptologic community efforts in cyberspace consisted of three components. The first was the effort of visionaries within the OPNAV N3N5 to define policy for naval computer network operations. The second was the service's investment in computer-network oriented billets in the National Security Agency. The third could be found in NIWA, whose flexibility to think and act creatively led to substantial advancements in cyberspace-related capability.[1046] While all three components of the cryptologic community's approach would prove important, their investment in billets, training, and personnel allowed the Navy to develop a close relationship with the NSA that was unique among the military services. This relationship gave the Navy access to expertise, infrastructure, and operational processes that allowed them to leverage real cyber capabilities in support of operations enduring and Iraqi freedom after 9/11.[1047]

[1045] Amber Ryan, telephonic interview with the author, January 7, 2019. Each of the services would eventually go on to create similar service-owned platforms.

[1046] There was also a parallel capability development effort within the OPNAV N9 in the late 1990s, but most information on that effort is not publicly available (Brooks, interview)

[1047] Ryan, interview and Stephanie Helm, telephonic interview with the author, December 28, 2018.

PHASE II: 2001-2008

The attacks of September 11th, 2001, led to an increased appetite for computer network operations among senior naval and joint leadership in support of overseas counterterrorism efforts. In 2002, using the expertise gained from working in TAO and using the NROC as launching infrastructure, Navy cryptologists conducted a Title 10 computer network operation in direct support to Central Command.[1048] The operation was personally supervised by the Secretary of Defense, who provided guidance on what could or could not be done as the operation progressed in real time.[1049] The operation also provided the first demonstration to Navy senior leadership that Title 10 computer network operations were useful.[1050] As such, it led to a two-fold realization among Navy senior leaders. First, that computer network operations provided valuable capability to military operations, and as such would be an instrumental component of 21st century warfare. Second, that because of its previous investment in the national cryptologic enterprise, the Navy was positioned to lead the services in the pursuit of computer network operations.[1051] Senior leaders finally began to recognize that its CNO-trained Navy cryptologists were providing critical support to a national level effort. This recognition led to increased support for CNO investment as well as to an expanded interest in how the capability could be used to support the Navy.[1052]

However, discussion over how best to expand the Navy's cyber capability quickly ran into the bureaucratic challenge of how to fund it. In matters of funding, the Navy's close relationship with the NSA proved to be a double-edged sword: while investment in the NSA allowed the Navy to develop both

---

[1048] Actual details of the operation remain classified. Its existence is not, as evidenced in an unclassified unit award for the Naval Information Warfare Activity.

[1049] This real-time guidance was not due to any claim of expertise by the SecDef, but simply the result of the fact that the operation was the first of its kind.

[1050] One leading Navy officer stated that the manner in which the team that conducted this operation switched from Title 50 to Title 10 authority was informed by his background as a surface warfare officer: they announced a change of cyber control as an officer of the deck would announce to a commanding officer.

[1051] Ryan, interview.

[1052] Brown, interview.

the expertise and the infrastructure to conduct cyberspace operations, it also acclimated senior naval leadership to the notion that cyberspace was a national enterprise that should be funded exclusively by national resources. From the perspective of the big three warfighting communities, there was little justification to divert Navy dollars away from aircraft carriers and submarines to spend on something that the NSA was already funding.[1053] Given the highly restrictive authorities that surrounded cyberspace operations at the time, there was also an immense skepticism that the Navy would ever get the necessary legal approval to conduct their own cyberspace operations. For many, this skepticism rendered moot any ideas of naval cyberspace independence.[1054]

While Navy leadership was content to continue with the status quo — in which the Navy relied upon preexisting national funding, national infrastructure, and national expertise to build capacity in cyberspace — the cryptologic community had a different perspective. On the one hand, it was far more operationally expedient and far more cost effective to rely upon the NSA than it would be to build an independent service infrastructure. In the short term, partnership with the NSA was still seen as the most effective method of building up service expertise.

In the long term, however, using NSA infrastructure required adherence to NSA rules, which meant the Navy could only pursue targets that reflected national intelligence priorities, and could only do so in a manner that fit within national intelligence calculations of risk. Reliance on the national cryptologic enterprise would ultimately limit the ability of cyberspace operations to prove their relevance to the warfighting Navy. The cryptologic community was faced with a dilemma: how to grow a service cyber capability that could be leveraged independently of the national infrastructure without severing the

[1053] Brown, interview.

[1054] Helm, interview.

national relationship that the service had relied upon thus far.[1055] Finding a way to resolve this dilemma became a primary focus of cryptologists on the OPNAV staff.[1056]

Between 2004 and 2005, the Navy allocated $38 million dollars to the expansion of the Navy's computer network attack mission.[1057] The cryptologic community went from having no money to having to a substantial amount of money, and with that came the need to prove that cyberspace was worth the investment. But how to demonstrate the worth of something that had no unifying service strategy to govern it? While the Navy had developed a sizable cadre of cyber-savvy sailors within the Naval Security Group — most of whom by that point still resided in the Naval Information Warfare Activity — their manner of employment was neither uniform nor unified, nor was it particularly focused on service-related priorities.[1058] Most of these personnel were scattered across various NSA work centers and performed work in support of NSA needs.

In 2006, in an effort to bring unity to the Navy's cyber investments, the Naval Security Group — by now called Naval Network Warfare Command (NETWARCOM) — implemented a concept called Navy Cyber Attack Teams (NCATs).[1059] While the NCATs were created in part to provide operational cyberspace capability, their ultimate intention was a bureaucratic one: NCATs served to inform naval leadership on just how much it would cost in money and manpower to build an independent cyber workforce. As such, the ultimate purpose of the teams was to collect data to inform resource allocation for

---

[1055] Insight from Ryan and Helm, interviews.

[1056] Helm, interview. By 2003, two priorities had begun to emerge among these staffers: first, to work with the Office of the Secretary of Defense on a Navy implementation strategy for the 2003 Department of Defense IO Roadmap, and second, to assist those in N2 and N6 in justifying why the Navy should invest in CNO independently of the NSA.

[1057] Ryan, interview. Then-CAPT Ryan secured the $38 million dollars after a briefing to key decision makers. The first slide of the briefing asked, "Is CNA a Navy mission?" An answer of no would end the briefing, since it was not worth discussing a capability that was not part of the Navy's core mission set. On the other hand, an answer of yes would logically require independent naval funding rather than continued reliance on national resources. The decision-makers answered yes, and by that logic, decided to fund it.

[1058] The point that most of the Navy's cyber-savvy sailors were contained within NIWA came from Michael Brown, who took command of NIWA in 2002.

[1059] See pages 37-39 for more on NETWARCOM.

upcoming budget cycles.[1060] In other words, the final audience of the NCAT initiative was less naval warfighters than those at the Pentagon who controlled the Navy's purse strings.[1061]

Because the NCATs were intended to serve the Navy rather than the national intelligence enterprise, they had to operate against targets that were of maritime significant, but not so important as to merit national attention or resources. Leadership selected three targets that fell within this category: a nation state, a counter-terrorist target, and a geographic region that was of interest to the Navy but not to the national security enterprise. They then built three teams comprised of cryptologic sailors within NETWARCOM to operate against these targets. The sailors were selected for their specific expertise based on the operational need of the team to which they were assigned. Most of the sailors came from NIOC Maryland or NIOC Suitland and worked out of Fort Meade, with a few based at geographically dispersed field sites. While the bulk of team personnel were enlisted cryptologic sailors, most of the high-skill developers were a combination of government civilians and officers with technical degrees who had a specific aptitude and passion for the work.[1062] The work these sailors performed for the NCATs was in addition to the jobs they already held in support of national intelligence missions, and every hour spent on an NCAT target was carefully logged.

The teams faced several challenges over their three year existence. First were the legal battles necessary to gain approval to conduct independent target development.[1063] Every requirement the teams intended to action had to be submitted in a separate approval package through the joint staff to the DIRNSA. Team leadership worked for nine months with joint staff lawyers to get SIGINT operational tasking authority (SOTA) from the NSA.[1064] With SOTA, a military commander can operationally direct

---

[1060] Helm, interview.

[1061] Ryan, Helm, interviews.

[1062] Ibid.

[1063] Ryan, interview.

[1064] SOTA is what gives a cryptologic element the ability to conduct independent operations against its own targets, rather than having to go through the NSA for approval. See Robert M. Gates, Department of Defense Directive 5100.20, "National Security Agency/Central Security Service (NSA/CSS)," January 26, 2010.

and levy SIGINT requirements on designated SIGINT resources.[1065] In other words, SOTA is the key to operational independence for a military commander. However, in gaining this authority to operate, the Navy had to work against a national cryptologic community whose support and partnership they had spent years working to carefully cultivate.[1066] There was a resultant fear among navy leadership that the NCATs' acquisition of SOTA could potentially jeopardize the Navy's standing in the national intelligence community.[1067]

Complicating the Navy's efforts to gain legal authority to operate was the fact that the bulk of NCAT targets were not inside a theater of declared hostilities. This meant that there was a limited combatant commander appetite to support their prosecution. While it is relatively easy to get approval to do things in support of troops on the battlefield in the midst of a shooting war, as post-9/11 cyber activity can attest, it is comparatively difficult to get approval to conduct target development in support of an unrelated contingency plan.[1068] Even attempting to find the right language to describe NCAT activity was difficult for the teams: while NCAT operations looked like computer network exploitation, and as such could have fallen purely under intelligence authorities, in reality they were military target development that was more akin to a pre-positioning of cyber forces in preparation for follow-on action.[1069]

An additional challenge concerned the NCAT cyber toolset: namely, it did not exist. The tools that the NCATs often wanted to use were controlled by the NSA, which meant that they were subject to highly restrictive regulations designed to limit the possibility of compromise. Agency restrictions on tool sharing led the NCATs to conclude that they would need their own tool set that could be used

---

[1065] Headquarters, Department of the Army, *Field Manual 2-0 Intelligence*, (Washington D.C.: Headquarters, Department of the Army, March 2010), section 12-27.

[1066] As one can imagine, the NSA is reluctant to delegate SOTA. The pursuit of SOTA for service component cyber commands proved a contentious issue throughout the 2010s.

[1067] Acquiring SOTA was an incredibly unpopular move within the Navy and the NSA, and took a lot of top cover from cryptologic admirals. Once the O6s who worked the case retired, Navy leadership systematically dismantled SOTA within thirty days (Ryan, interview). There is speculation that one of the reasons for this dismantling was political: the Navy hadn't had a Director of the NSA in decades, and did not want to get on the agency's bad side (Echoed by Ryan, Helm, Roughead, Dorsett). See also p. 5 Dorsett notes, from SECNAV 11/14/2007: "discussed need for Navy to play for senior jobs (NSA, DIA)."

[1068] Helm, interview.

[1069] Ryan, interview.

independently of the national intelligence system. In response, the NCATs began to recruit military and civilian tool developers, many of whom came from the Office of Naval Research and DARPA, to build just such a tool set. The foundation laid by these developers fell under the management of NIOC Suitland, which later became the Naval Cyber Warfare Development Group.[1070]

After a three year operational period, the NCATs were disbanded in 2009. Much of their functionality was absorbed into the newly formed Fleet Cyber Command.[1071] However, while the NCATs themselves were short-lived, their legacy helped to educate the Navy on how to approach cyberspace operations. This educational campaign had a threefold audience. The first was the Navy cryptologic community itself. Outside of a few visionaries who recognized that the cryptologic environment was changing, and who consequently put forth the bulk of the effort in organizing, staffing, and gaining approval for the NCAT construct, there remained a portion of the cryptologic community that was resistant to accept either conceptual or structural changes. Much of this reluctance had to do with the close relationship the Navy had built with the NSA. Cryptologic leaders were loathe to jeopardize, through independent naval action, what they saw as the main reason the Navy had surpassed the other services in its cryptologic reputation.[1072] Many cryptologic leaders also suffered from a conceptual road block based on the community's storied history. Specifically, because the Navy cryptologic heritage exists in the RF tradition at the shipboard level,[1073] some cryptologists were skeptical of a capability whose shore-based operation was seen as insufficiently fleet-focused to be of long-term relevance.[1074] By providing dedicated cyberspace support to targets of maritime interest, the NCAT experiment helped to educate some of these skeptics within the cryptologic community.

[1070] Tighe, interview.

[1071] Singer, interview.

[1072] As stated in footnote 209, there was also concern that too much independent Navy cryptologic action would put the Navy's intended candidate for the next DIRNSA, which had been identified early as Admiral Michael Rogers, at risk. (On the identification of Rogers: Roughead, interview).

[1073] Sean Heritage, telephonic interview with the author, October 23, 2018. Mark Neighbors, telephonic interview with the author, February 8, 2019.

[1074] Ryan, Helm, interviews.

In addition, the NCAT experiment also informed the Navy cryptologic community on personnel management practices. The NCATs were created two years after the establishment of the enlisted Cryptologic Technician-Network (CTN) rating in 2004, yet before the Navy had figured out exactly how to manage, train, or operationally employ these personnel. Thus, the NCAT construct provided quantifiable feedback on how to manage the Navy's CTNs, from the specific proficiencies they would need to develop to what type of jobs they could be expected to fulfill.[1075] The teams also provided feedback on how to employ cryptologic officers in cyberspace.

The second audience consisted of members of the national cryptologic enterprise. There was a sense within the NSA that not only did they own the national cryptologic mission, but that, by nature of this ownership, they also had sole purview over whatever it was that cyberspace was going to become. The NSA controlled the infrastructure, they controlled the expertise, they controlled the accesses, and they controlled the targets. Thus, the Navy had to convince this population that there were cyber targets of military relevance that existed outside of this national sphere, and that as a result would never appear on a nationally prioritized target list. Instead, the only way to action said targets would be to leverage independent military teams. NCAT targets were selected specifically for this reason.[1076]

The third and final audience consisted of the senior leaders in the Navy, who would need to be persuaded through measurable data that, first, the Navy was capable of pursuing independent cyberspace operations; second, that these operations would be of value to naval warfighting; and third, that said operations would be neither cost- nor manpower-prohibitive. While the NCATs were ultimately disbanded in 2009, their functionality and lessons learned were absorbed into the Navy's new service component command for cyberspace, Fleet Cyber Command.[1077]

[1075] Ryan, interview.

[1076] Ibid. In addition to the national cryptologic enterprise, the NCATs also influenced the thinking of joint military leadership. Several NCAT members worked day jobs for JFCC-NW, and JFCC-NW often sent representatives to weekly NCAT meetings to better understand their processes, requirements, and methods.

[1077] Ryan, Helm, interviews.

The NCAT story affirms the singular importance of Navy cryptologists in driving cyberspace operations development in the Navy during the first decade of the 2000s. This importance manifested itself in several ways. First, the development of an independent, offensive cyberspace capability was led entirely by a group of visionaries within the cryptologic community who were inspired by changes taking place in the national cryptologic enterprise. As these officers began to realize that the cryptologic environment was changing, they had to work to convince first the rest of their own community and then the rest of the Navy that these changes were both real and that they were important.

Second, the NCAT experiment highlights the twofold importance of the Navy's late 1990s investment into the national cryptologic enterprise. Alone among the services in the intensity of its commitment to supporting national SIGINT, the Navy's close relationship with the NSA gave it the access and the expertise to quench the DoD's thirst for tangible cyberspace activity upon the initiation of hostilities in Afghanistan and Iraq. These operations, in turn, helped to convince Navy senior leadership that cyberspace operations were a worthwhile investment. However, the senior leaders' reluctance to jeopardize the service's relationship with NSA ultimately limited their appetite for the type of independent cyberspace development that the NCAT experiment recommended.

COMPUTER NETWORK DEFENSE

The NCATs represented the Navy's most significant attempt to organize for computer network attack prior to the creation of Fleet Cyber Command. However, since the NCATs focused exclusively on offense, the Navy had to undertake a separate effort to strengthen its computer network defense. This effort began in earnest in October 1995 with a five-person Navy Computer Incident Response Team in the Information Warfare Defensive Division of the Fleet Information Warfare Center. By 2003, the NAVCIRT had grown to 250 personnel and had become the operations department of FIWC.[1078] On 16 June 2003, the Navy removed NAVCIRT from FIWC and merged it with NCTF-CND to form the

[1078] "Navy Cyber Defense Operations Command Celebrates Past, Present, Future."

NAVCIRT Task Force. This organization became the Navy Cyberspace Defense Operations Command (NCDOC) in January 2006.[1079] Comprised mostly of enlisted information technicians (ITs) and cryptologic technician-networks (CTNs), NCDOC has served as the central authority for naval network defense since its founding.[1080] It was subsumed into Fleet Cyber Command in 2009 as Task Force 1020.

Separately, on 31 January 1999, the Navy launched the Navy Component Task Force for Computer Network Defense in response to a Department of Defense Directive. NCTF-CND served as the service component to the Joint Task Force for Computer Network Defense (JTF-CND), which had been formed in response to the Solar Sunrise intrusion of 1998.[1081] The mission of the NCTF-CND was to serve as the single focal point for the defense of Navy computer networks and systems, which at the time were just beginning their consolidation under the IT-21 and NMCI initiatives. Its responsibility included conducting continuous information assurance vulnerability alerts, monitoring networks for compliance, and detecting, protecting, and responding to network intrusions. Following an incident, NCTF-CND would coordinate defensive actions with appropriate organizations to ensure the restoration of network security and functionality. The NCTF-CND was also responsible for the oversight of disparate computer and network incidents.[1082]

In 2002, the Navy created Naval Network Warfare Command in Norfolk, Virginia, to serve as the single point of focus for Navy networks and to consolidate responsibility for network oversight.[1083] The command served as the central operational authority responsible for coordinating all information technology, information operations, and space requirements within the Navy. In order to execute this

---

[1079] Grainger, interview.

[1080] Ibid.

[1081] U.S. Congress. House. Armed Services Committee. *Information Technology: An Examination of DoD Network Vulnerabilities.* May 17, 2001. Statement by Vice Admiral Richard W. Mayo, Director, Space, Information Warfare, Command and Control, Office of the Chief of Naval Operations..

[1082] Ibid.

[1083] Vice Admiral P.A. Tracy, Memorandum to the Secretary of the Navy, "Establishment of Commander, Naval Network Warfare Command, Norfolk VA," January 7, 2002. See also "Navy Establishes Network Warfare Command," Navy.mil, March 28, 2002, https://www.navy.mil/submit/display.asp?story_id=1156.

wide-ranging responsibility, NETWARCOM merged some 23 different commands under its authority, to include Naval Network and Space Operations Command, Naval Computer and Telecommunications Command, FIWC, and NCTF-CND. The substantial variety of organizations underneath the NETWARCOM umbrella speak to the breadth of the field of naval information operations writ large. It was NETWARCOM's responsibility to improve the Navy's information operations effectiveness, and in so doing to better position the Navy to respond to the information-related demands of the global war on terror.[1084] In conjunction with the creation of NETWARCOM, the commander of NAVSECGRU assumed an additional duty as the NETWARCOM director of information operations.[1085] This arrangement allowed NETWARCOM to call on the Navy's Title 50 authority when needed.[1086]

The creation of a single command to hold responsibility for naval networks was a direct response to the gradual consolidation of those networks that had taken place over the preceding four years.[1087] As such, NETWARCOM was intended to better support the concept of one naval network and to support that network's end-to-end operational management. Given its responsibility to answer the question of how the Navy should communicate, NETWARCOM was comprised largely of communicators from the Navy's IT enlisted rating and IP officer community.[1088] However, while NETWARCOM served as an improvement over the Navy's previously fractured system of network management, its exclusive focus on network maintenance and defense left the fields of offense and exploitation functionally and structurally distinct. This separation impeded the Navy's ability to fully realize its holistic vision for information operations.

[1084] Ted Branch, NAVADMIN 023/16, "Information Dominance Corps Redesignated Information Warfare Community," February 2, 2016.

[1085] "Navy Establishes Network Warfare Command."

[1086] Joseph Gunder, "Naval Security Group Aligns with NETWARCOM," Naval Network Warfare Command Public Affairs Office Press Release 05-010, October 4, 2005.

[1087] Recall the twin consolidation initiatives of IT-21 (1998) and NMCI (2000).

[1088] Brown, interview and Edward H. Deets, telephonic interview with the author, January 8, 2019.

In September of 2005, the Navy radically changed its approach to both offense and defense when it decided to decommission the seventy-year-old Naval Security Group and merge it with NETWARCOM.[1089] The stated purpose of the merger was to bring all components of Navy information operations capabilities — at this point considered to encompass the five core areas of IO as well as Navy networks and signals intelligence — into a coherent operational art under a single command.[1090] The merger sought to eliminate organizational stovepipes and to create a true cadre of Navy professionals through the consolidation of the resources and functions of the Navy's various information-related ratings and communities, from information professionals and cryptologists on the officer side to information and cryptologic technicians on the enlisted side.[1091] In conjunction, all 31 Naval Security Group Activities (NSGAs) and Detachments (NSGDs), as well as the NETWARCOM-subordinate Fleet Information Warfare Command, were renamed as Navy Information Operations Commands (NIOCs) and Navy Information Operations Detachments (NIODs). The functionality of these organizations remained largely the same in spite of their change in name. These new organizations reported to the NETWARCOM Information Operations Directorate.[1092]

The consolidation of two of the Navy's largest information-related organizations — not to mention the functional consolidation of offense and defense — demanded a culture shift among their respective personnel communities.[1093] This shift was not easy to enact.[1094] Importantly, the elimination of NAVSECGRU meant that NETWARCOM assumed the role of the Navy's service cryptologic element. That this was merely one role among many for the three star command led to a fear among some

---

[1089] F.J. Niner, OPNAV Notice 5450, "Disestablish Commander, Naval Security Group Command (COMNAVSECGRU), Fort George G. Meade, MD; Rename and Realign All Subordinate NAVSECGRU Commands and Detachments," December 29, 2005.

[1090] Ron Steiner, "NETWARCOM/NAVSECGRU Alignment Communications Plan," September 21, 2005

[1091] Ibid.

[1092] Ibid.

[1093] Ibid.

[1094] Leigher, interview.

cryptologists that the signals intelligence mission would ultimately become of secondary or tertiary importance.[1095]

This concern, however, was not reflected by all members of the cryptologic community. In fact, much of the NAVSECGRU/NETWARCOM merger was driven by several career cryptologists who saw proficiency in information operations as the future of their discipline.[1096] In the words of then-Captain William Leigher, Special Assistant for Information Operations at NETWARCOM:

> Cryptology is made up of two distinct parts. One is the protection of our communications, the other is the exploitation of our adversaries' communications. As for the relationship with Information Operations, nearly everything we do in IO depends on access to other information streams so we can exploit them to our benefit in a combat setting.[1097]

In an effort to encourage this shift in perspective, the cryptologic community rebranded itself on 23 May 2005.[1098] Four cryptologic officer designators were retitled from "cryptology" to "information warfare" to acknowledge the expanded scope of responsibility the Navy expected from that officer community.[1099] The change was meant to broaden the focus of the information warfare community, and in so doing change fleet expectations of what an information warfare officer could provide.[1100] NETWARCOM Vice Commander Rear Admiral Edward Deets captured the intent behind the name change well when, in 2007, he described Navy information warfare as a

---

[1095] Grainger, Brown, interviews. Given this fear, it is noteworthy that the NETWARCOM/NAVSECGRU merger was driven by two visionary cryptologists, Winsor Whiton and Andy Singer.

[1096] Singer and Whiton were instrumental in driving the merger.

[1097] Gunder, "Naval Security Group Aligns with NETWARCOM."

[1098] From G.L. Hoewing, NAVADMIN 233/05, "Cryptologic Officer Name Change to Information Warfare," September 15, 2005: "In 2002, the CNO established information operations (IO) as a primary warfare area on par with other warfare areas, and the CNO guidance for 2005 directed the development of the IO career force. The information warfare community is a core component of the emerging IO career force. The community has a long and distinguished history of providing actionable signals intelligence to strategic, operational, and tactical commanders. Information warfare officers will continue to build upon the foundation of signals intelligence, target and system knowledge as applied to joint and naval warfare, delivering effects-based operational capability."

[1099] Ibid.

[1100] Singer, interview.

> community of war-fighters who deliver overwhelming information superiority to naval and joint commanders…by applying the core capabilities of Information Operations and Signals Intelligence to shape, influence, and defeat adversaries and other audiences in support of commanders' objectives and to provide warning of adversary intent.[1101]

The Navy cryptologic community was thus nominally disbanded, replaced by a community of information warfare professionals who were expected to be proficient across a broad range of information-related disciplines.

Of course, many were concerned that the cryptologic community might be functionally disbanded as well — that the new emphasis on proficiency in information warfare, which was broadly defined as "a warfare area that influences, disrupts, corrupts, or usurps an adversary's decision-making ability while protecting our own," would come at the expense of what was still considered the community's core proficiency of signals intelligence.[1102] In the final analysis, it was uncertain whether the changes made to information warfare officer training were sufficient to produce the type of expertise that the fleet came to expect.[1103] However, the name change did serve to emphasize the increasingly divergent trajectories between the rival intelligence and cryptologic communities: cryptology endeavored to become more operational and warlike with their pursuit of computer network operations and information warfare, while intelligence struggled to come to grips with the geopolitical realities and consequent intelligence demands of the post-Cold War era.[1104]

No such confusion followed the personnel changes that were made to the enlisted cryptologic community during the same time period, likely because these changes did not entail a wholesale rebranding of the enlisted cryptologic function. In 2004, the Navy created a new rating called Cryptologic

---

[1101] James Murphy, "Give Information Personnel More Training and Credibility," *Proceedings* Issue 134 (September 2008).

[1102] Murphy, "Give Information Personnel."

[1103] Heritage, interview.

[1104] Turner, interview.

Technician-Network (CTN) to meet the growing demand for expertise in computer network operations. The new rating was implemented to monitor, identify, collect and analyze information; provide data for digital network products; and conduct computer network operations worldwide in support of Navy and Department of Defense missions.[1105] While the CTN rating was not formally introduced until February of 2004, discussions among cryptologic community leaders on the need for such a rating began to occur as far back as 1998.[1106]

Because the CTNs were seen as a logical extension of the cryptologic career field rather than an entirely new community, it proved relatively easy to gain support for the new rating from naval leadership writ large.[1107] Once again, the most significant pushback came from within the cryptologic community itself. On the one hand were leadership who saw computer network operations as a passing fad that distracted from the development of core cryptologic proficiency. On the other were enlisted sailors who were reluctant to see their ratings change after full careers spent in a familiar discipline.[1108] In spite of this internal resistance, community leadership recruited its first CTNs through a testing process that focused on the service's population of Cryptologic Technician-Communications (CTO) sailors. As a result of this testing, roughly ninety percent of the CTOs were converted to CTNs.[1109] The remainder merged with the IT rating in 2006 in an effort to streamline the Navy's overall management of network administrators.[1110]

Where did all these changes leave the Navy's cryptologic community in the late 2000s? The Navy cryptology community from 2001 to roughly 2008 was divided on the topic of cyberspace. While a few

---

[1105] "The Cryptologic Technician Rating," U.S. Naval Cryptologic Veterans Association, last updated June 10, 2016, https://usncva.org/history/ct-rating-history.html.

[1106] Brown, interview. Sandy Brooks stated that the movement began in earnest in 2001, when she was the community detailer. By 2003, the Navy had incorporated ad hoc cyber defense and exploitation training into its enlisted cryptologic courses at Pensacola, Florida.

[1107] Ibid..

[1108] Brooks, interview.

[1109] Ibid.

[1110] J.C. Harvey, NAVADMIN 338/05, "Merger of the Information Systems Technician (IT) and Cryptologic Technician (Communications) (CTO) Ratings," December 28, 2005. The CTO-IT merger was announced 28 December 2005 and went into effect between March and October of 2006.

visionaries took the ongoing societal migration towards digital communication technology to mean that the future of cryptology, or at least a portion of it, was in cyberspace, others saw cyberspace operations as a temporary distraction from service's core cryptologic expertise. The push for increased cyber resources that took place in the early 2000s was therefore met with resistance from both inside and outside of the cryptologic community.

Navy cryptologists launched a number of initiatives in order to encourage a community perspective shift on cyberspace operations. First, computer network exploitation and defense were incorporated into the enlisted training program at the Navy's cryptologic training headquarters in Pensacola, Florida between 2002-2003.[1111] This was followed by the creation of the Cryptologic Technician-Network enlisted rating in 2004, and the rebranding of the cryptologic officer community to Information Warfare in 2005.[1112] These investments in training, operations, and personnel culminated with the 2006 creation of Navy Cyber Attack Teams. As a cyber proof-of-concept, NCATs demonstrated that, first, the Navy could engage in independent cyberspace operations that were of value to maritime warfare, and second, that doing so would not prove excessively costly in terms of either money or personnel. However, the service's reluctance to jeopardize its relationship with the national security enterprise prevented it from fully capitalizing on the opportunity that the NCATs presented. Regardless, by the late 2000s, an expanded awareness of the value of cyberspace to naval operations had begun to solidify within the senior-most levels of Navy leadership.

Conceptual Development: The Strategic Studies Group

The cryptologic community was not the only voice calling for reform in how the Navy approached cyberspace operations in the mid-2000s. From October 2006 to July 2008, the Navy's Strategic Studies Group (SSG), an operational research and concept generation center at the Naval War

[1111] Brown, interview.

[1112] Hoewing, NAVADMIN 233-05.

College that worked directly for the Chief of Naval Operations, studied cyberspace in detail at the direction of then-CNO Admiral Michael Mullen.[1113]

In fall 2006, as part of a study on "fighting in cyberspace in 2030," the SSG was tasked to study the potential impacts of cyberspace on naval operations.[1114] The CNO asked the group to generate concepts that addressed the people, processes, and products for a Navy capable of operating at the convergence of sea power and cyber power.[1115] Three broad questions emerged from this exploration: what is cyberspace, why is it relevant to maritime forces, and how can maritime forces use cyberspace?[1116] The results of the effort were briefed to the CNO in July 2007, and were released to the rest of the Navy in March 2008.[1117]

In its report, the SSG established a definition of cyberspace that sought to balance its technological and human dimensions, in contrast to what the group saw as a set of contemporary definitions that were overwhelmingly focused on technology. The report defined cyberspace as

> An unconstrained interaction space for human activity, relationships and cognition; where data, information, and value are created and exchanged; enabled by the convergence of multiple disciplines, technologies, and global networks; that permits near instantaneous communication, simultaneously among any number of nodes, independent of boundaries.[1118]

[1113] The strategic studies group was established in 1981 at the behest of then-CNO Admiral Thomas Hayward. As the 7th Fleet Commander, Admiral Hayward realized that no one in the Navy had ever taught him how to think at the operational or strategic level. He created the SSG to both provide in-depth study of the Navy's key strategic issues and to educate senior naval officers on strategic thinking. Each year, the SSG would work on a task that the CNO wanted. For the first seven to eight years, the SSG was focused on war plans with the Soviets. In 1995, Admiral Borda transformed the SSG into a group whose sole mission is the generation of revolutionary naval warfare concepts. The SSG today, located at the Naval War College in Newport, Rhode Island, follows in line with this tradition, and can be thought of as an "operational research and concept generation center." (Strategic Studies Group XXVI, "The Convergence of Sea Power and Cyber Power," March 2008, xiii). It was unusual that the group would study any topic for two years, rather than the customary one; but Admiral Mullen directed this extended study based upon a keen interest in cyberspace and a sense that the Navy did not properly understand it. (William Glenney, telephonic interview with the author, January 14, 2019).

[1114] SSG XXVI, xvii.

[1115] Ibid., iii.

[1116] Ibid., xvii.

[1117] SSG XXVI, iii.

[1118] Ibid., xvii.

The report described a future Navy that "will have to be capable of operating in the physical world and in the virtual world, at the convergence of sea power and cyber power."[1119] To fulfill this vision, each of the Navy's unique warfighting capabilities — the access derived from forward presence, the options derived from sovereign flexibility, the staying power of platform-based naval endurance, and the potential for decisive effects — were all given virtual analogues.[1120] Concepts of sea control and controlling sea lines of communication were transformed to "sea-based cyber control" and projecting power across "cyber lines-of-communication." In other words, the report described an information age Navy that must be able to protect national interests and project power across both traditional sea lines of communication and cyber lines of communication that are accessible from the sea, to include undersea cables, the maritime electromagnetic spectrum, and low-earth orbiting satellites.[1121] The effect of this transformed strategic environment would require a future Navy able that could provide maritime access and effects across two global commons — the sea and cyberspace.

From this strategic context emerged the twin concepts of Global Reach Forward and Virtually Enabled Operations.[1122] The former is a translation of the Navy's traditional mission of forward presence to the virtual world, such that the Navy can achieve the same level of power projection in virtual space as it can in physical space. As the report states, "the Navy's [future] relevance will depend upon its ability to conduct forward-deployed, cyber-centric maritime operations."[1123] The latter consists of the merging of cyberspace and physical capabilities to allow the Navy to operate in even more geographically dispersed fashion. Both of these concepts can be seen as extensions and expansions of existing Navy operational thought. Virtually enabled operations in particular reflected the concepts of seaborne command, control, and communications that have transfixed naval thinking since the early 1900s.

[1119] SSG XXVI, xviii.

[1120] Ibid., 3-2.

[1121] Ibid., 3-5.

[1122] Ibid., xx.

[1123] Ibid., 3-2.

However, while the report's effort to advance naval strategic thinking into the cyber realm was laudable, far more striking were two of the report's primary recommendations that were ultimately discarded: first, the establishment of cyber warfare as a primary warfare area, and second, the creation of specific cyber units and innovation cells to serve as the incubator of concept and capabilities development. The establishment of cyber warfare as a primary warfare area was the report's top recommendation. It stated, "In order for the Navy to be able to fight and win, [it has to create] a Cyber Warfare Community comprised of warriors equal in every way to those who operate in traditional warfighting domains."[1124] Consequently, the report recommended the creation of a Cyber Warfare Community comprised of both enlisted sailors and unrestricted line officers. The designation of unrestricted line status to cyber warfare officers was seen as particularly important to establishing parity with the other warfighting communities. Accordingly, the report suggested that cyberspace officers should be bred "to be warfighters, not administrators," with cyber warfare as their principal mission rather than as simply one mission of many.[1125] Cyber Warfare Officers should also have both cyber-specific skill and the general warfighting acumen to command at the highest levels of the Navy, on par with their aviator, surface warfare, and submariner peers.[1126] The cyber warfare community would be created by the merger of Information Professionals and select members of the Information Warfare community who possess a demonstrated cyberspace aptitude.

In addition to changes in the officer ranks, the report also recommended the creation of an enlisted cyber warfare rating through the merger of the Cryptologic Technician-Network (CTN) and the Information Systems Technician ratings. By combining network maintainers with network attackers, the merger would effectively end the segregation of offensive and defensive functions that had been institutionalized through separate enlisted ratings. The resulting cyber warfare sailor would be bred to

---

[1124] SSG XXVI, 5-18.

[1125] Ibid.

[1126] Ibid., 5-19.

possess technical aptitude across the full spectrum of network operations, network attack, network defense, and network exploitation.[1127]

In keeping with the recommendation to elevate cyberspace into a warfare area, the report also recommended adding a cyber warfare commander to the Navy's composite warfare commander concept to oversee cyberspace capabilities and to command sea-going cyber forces. This commander would exist in addition to the information warfare commander that the Navy had already established.[1128] The report offered a number of other recommendations on how to further institutionalize cyberspace as a warfare area across the Navy. These recommendations included improving cyber training and education for the total Navy as well as the cyber workforce; evolving the maritime strategy to better reflect cyberspace as a reality of the future operating environment; developing a cyber warfare concept of operations; and developing a new deterrence framework that extended deterrence principles into the virtual world.[1129]

The Strategic Studies Group published a follow on report, called SSG XXVII, in December of 2008 to study how to integrate "physical-world and cyber-world capabilities into a seamless continuum of sea power" through 2020 and beyond.[1130] This report reiterated many of the conclusions from its predecessor, to include the idea of cyberspace as part and parcel of the Navy's mission of global reach. It called cyberspace "a new frontier for forward presence that complements traditional physical forward presence."[1131] In an effort to articulate a more robust cyber conceptual framework, the report also delineated between different types of cyber activities that existed across a spectrum of collaboration and compellance. These activities ranged from "cyber probe" and "cyber obstruct" on the compel end to "cyber assist" and "cyber connect" on the end of collaboration.[1132]

[1127] SSG XXVI, 5-19.

[1128] Ibid., 5-20.

[1129] Ibid., 6-2.

[1130] Strategic Studies Group XXVII, "Collaborate and Compel — Maritime Force Operations in the Interconnected Age," December 2008, xvii.

[1131] Ibid., xx.

[1132] SSG XVII, xxii to xxiii.

The report recommended that the Navy work to establish a "cyber forward presence" beyond the dot-mil "Maginot line" — in other words, to mimic the Navy's physical posture of global dispersion with a virtual posture that would allow persistent access to critical networks worldwide.[1133] In justifying this forward presence, the report argued that

> Cyberspace is an unconstrained, yet largely untapped interaction space. Operations beyond dot-mil transcend political borders and physical limitations, and do so with near instantaneous global reach […] The nation's adversaries will achieve the advantage if U.S. forces are not in cyberspace beyond dot-mil.[1134]

As with its predecessor, this report was noteworthy for its emphasis on the human dimension of cyberspace, this time with respect to the types of sailors that the Navy would have to recruit to operate within it. In accordance with this emphasis, a second recommendation was to establish the parity of cyber operations with other maritime operations, under the premise that "cyber warfare is as real as submarine warfare and surface warfare; it is not just about intelligence gathering or technology."[1135] The report argued that "cyber operations are marginalized relative to the Navy's traditional warfighting areas." To overcome this marginalization and push cyberspace into the institutional mainstream, the Navy would have to establish an unrestricted line cyber warfare community, improve cyber education and training for all Navy personnel, develop cyber operations doctrine, invest in capabilities development, and integrate cyber operations into Naval War College core curricula.[1136]

Many of SSG's conclusions stood in contrast to the arguments that were coming out of the cryptologic community, which was the only other part of the Navy making any significant effort towards an expanded cyberspace investment at the time. While the cryptologic community wanted more money and manpower dedicated to cyberspace operations, it still wanted to retain ultimate operational control of

---

[1133] SSG XXVII, xxviii.

[1134] Ibid., 3-2.

[1135] Ibid., 5-1.

[1136] Ibid., xxviii.

the field under the premise that it was simply an offshoot of the traditional cryptologic mission. The SSG, meanwhile, saw cyberspace as something wholly different from intelligence gathering. To the SSG, cyberspace was its own unique battlespace whose connection to and inseparability from the physical world rendered it of existential concern to all aspects of naval warfare. In order take full advantage of its operational significance, cyberspace would have to be treated like a traditional warfare area; and yet in order to do that, the Navy would have to make a deliberate effort to give cyberspace all the symbolic trappings enjoyed by its surface, subsurface, and air counterparts: an unrestricted community designation, new doctrine and training centers, and equal opportunities for command at sea. The parallel efforts of both the cryptologic community and the SSG to increase naval attention on cyberspace approached the problem from two different perspectives, and, as a result, offered two different and competing sets of solutions.

SUMMARY: THE STRATEGIC STUDIES GROUP

The SSG offered a robust analysis of the cyber dimension that concluded with a set of recommendations that were at once creative, unique, and prescient — and which differed starkly from the recommendations provided by other factions of either the service or the DoD writ large. However, these recommendations were ultimately rejected by Admiral Mullen. Given the prescience of the SSG's analysis, why were its recommendations ultimately rejected? And what enabled the group to arrive at such recommendations in the first place?

First, the composition of the SSG enabled it to overcome the limitations of individual community influence in order to arrive at a theory of cyberspace that was holistic, unique, and forward-thinking, rather than constrained by the experiences or interests of any one community. The SSG deliberately sought fellows who hailed from a variety of operational backgrounds and who had a reputation for thinking differently from their peers. Fellows were comprised of senior officers who were selected based on warfighting expertise and promotion potential; junior officers from all military services; and civilian

academics.[1137] These fellows were augmented by a robust professional network of civilian experts with backgrounds in both the hard and soft sciences. This diverse academic and operational composition, which was deliberately crafted by the SSG director to foster intellectual creativity and to ensure a maximally holistic approach to problem-solving, enabled to group to approach the problem of cyberspace with a different perspective.

Second, the Navy's ultimate rejection of SSG recommendations provides insight into where cyberspace stood in the mid-2000s. At that time, both the military services and the DoD writ large lacked strong consensus on either the importance of cyberspace or how to adequately characterize it. Absent this consensus, it was unclear what would constitute an appropriate organizational response. For Admiral Mullen, the report's recommendations and the consequent structural and cultural changes they required were seen as too much too soon.[1138]

Structurally, because the battle for billets was a zero-sum game, every new billet devoted to cyber warfare would have had to come at the expense of a billet somewhere else in the Navy. With a conservative estimate of 500 cyberspace personnel necessary to get the community off the ground, the zero-sum growth model of the mid-2000s naturally worked against the stand-up of a new community.[1139] Culturally, the creation of an unrestricted line cyber warfare community was seen as a threat to the power of the Navy's three dominant warfighting tribes. Perhaps due to the strong, simultaneous influence of the cryptologic community, there remained a sense among this warfighting class that cyberspace and cryptologic warfare comprised one in the same activity.[1140] The creation of a separate cyberspace

---

[1137] The majority of fellows would hail from unrestricted line backgrounds, with the remainder coming from the restricted line. The junior officer fellows would typically have regular representation from each of the military services, and the senior fellows would have representation from each of the maritime services. Of the 23 contributors to SSG XXVI, 17 were from the Navy, two from the Marine Corps, two Air Force, one Army, and one Coast Guard, with an additional eight civilian contributors (SSG XXVI).

[1138] Glenney, interview.

[1139] Ibid.

[1140] Ibid.

personnel cohort of equal stature to the other three warfighting communities was therefore seen as both culturally unacceptable and materially unnecessary.

The report's reception was also plagued by the problem of ignorance. To most warfighters in the Navy, cyberspace was still considered the nebulous activity that simply kept the networks running, and was not yet seen in the type of grand strategic terms outlined in the SSG reports. While there were a handful of naval officers who were well-versed in the particular challenges of cyberspace by the mid-2000s, few could articulate those challenges in terms that would resonate with the mainstream unrestricted line communities.[1141] It would take new leadership at the top to gain momentum for significant cyberspace change.

The Navy Embraces Information Dominance

PHASE 3: 2009 TO PRESENT

There was an additional reason for Admiral Mullen's reluctance to accept some of the cyber-centric proposals of the Strategic Studies Group: he saw cyberspace as only one component of the much larger problem of how to manage intelligence and information.[1142] At the heart of this problem were the relationships among the Navy's various information-related communities, comprised primarily of intelligence, cryptology, space, electronic warfare, and network operations. The fragmentation of these communities into independent fiefdoms with no common flag officer advocate on the Navy staff meant that there was no single point of focus in the Navy for control over networks and the electromagnetic spectrum.[1143] Structural differences were compounded by cultural differences, such that cooperation across disciplines was more often a product of individual personalities than of habitual relationships.[1144]

[1141] Ironically, the year the SSG published its first study on cyberspace, the Naval War College was shut down for 26 days due to a Chinese network intrusion (Glenney, interview).

[1142] Vice Admiral David J. Dorsett, "Navy Intelligence and Information Dominance Discussions, 2006-2010," personal notes.

[1143] Dorsett, "Discussions," 2.

[1144] Dorsett, Turner, interviews.

The fragmentation of these communities, coupled with the operational challenges presented by a rapidly changing information environment, lent Admiral Mullen the sense that the Navy was failing in its ability to gain knowledge and understand information.[1145]

Beginning around 2005, this question of how to better organize the Navy for success in the information environment held a preeminent position in senior leader discussions.[1146] Much of the conversation centered around what to do with the Navy's intelligence and cryptologic communities, as well as how to handle the Navy's command and control capabilities. Regarding the former, some, to include the then-Vice Chief of Naval Operations, supported the idea of merging the two disciplines into a single community.[1147] Regarding the latter, Roughead cautioned that focusing too narrowly on command and control systems would lead to an overly technical perspective that would miss the bigger picture: in other words, the Navy's approach to command and control would need to remain grounded in an appreciation for the decision-making purposes the information serves rather than distracted by the technical systems the information transits.[1148]

Discussion during the final months of Admiral Mullen's tenure hinted at a number of reforms that would take place over the next two years. Mullen was particularly adamant about the need to bring together ISR, information operations, networks, and space underneath a single resource sponsor on the OPNAV staff. In addition, he emphasized the human component of information by questioning how the Navy should manage its information-related talent pool. Mullen also believed, in reflection of the growing perception that information was a warfighting space, that any new information management construct would have to be run by a warfighter from one of the Navy's big three platform communities. This move

---

[1145] Dorsett, "Discussions," 2.

[1146] Turner, interview.

[1147] In April 2007, the Vice CNO proposed merging intelligence and Network Warfare Command into a single Naval Information and Intelligence Command. Dorsett, "Discussions," 3.

[1148] Ibid., 4.

would help maintain focus on information's operational relevance, and in so doing allow the information realm to gain credibility across the rest of the service.[1149]

When Admiral Roughead took over from Admiral Mullen, he made the Navy's approach to information the centerpiece of his tenure as Chief of Naval Operations. Roughead did not want mere programmatic changes, but a total transformation of outlook and strategy that would enable the Navy to dominate in both the intelligence and information arenas. The first step Roughead took was the elevation of the N2, the Deputy Chief of Naval Operations for Intelligence, from a two to a three star position in early 2008.[1150] Concurrent with its elevation, the N2 assumed responsibility for the Navy's intelligence and cryptologic communities.[1151] Increasing the rank of the N2 was one step toward the Chief's goal of restoring naval intelligence to a position of prominence, and putting it on par with the prestige of the platform communities.[1152] Specifically, naval intelligence had suffered from the loss of a maritime strategic rival with the demise of the Soviet Union, and in this loss had struggled to adapt to the intelligence needs of the post-Cold War world.[1153]

In addition to his broad concerns about information and intelligence, the Chief also harbored specific concerns about cyberspace. Roughead did not see cyberspace as something wholly unique or distinct; rather, he considered it just one component of a holistic information environment. However, while Roughead did not want to emphasize cyberspace at the expense of the other information disciplines, he also acknowledged that cyberspace was something with which the Navy greatly struggled and in which it was beginning to lag behind.[1154] Roughead saw the Navy's approach to cyberspace as

---

[1149] Dorsett, "Discussions," 5.

[1150] Roughead, Dorsett, interviews.

[1151] Dorsett, "Discussions," 6.

[1152] Mark R. Hagerott, telephonic interview with the author, December 11, 2018. With only a two star at the top, the intelligence community had little relative power compared to the other communities.

[1153] Dorsett, interview.

[1154] Ibid. The chief's perception was that the Navy struggled relative to the joint community as well as the service's own needs. This perception that the Navy lagged behind in cyberspace was further exacerbated by the operational and doctrinal development that was ongoing in the Chinese PLA.

lacking appropriate sophistication and urgency, with insufficient focus on how to train and manage personnel. Under Roughead's vision, it was not enough to simply use networks as means of command and control — instead, the Navy would need to develop the ability to conduct command and control of the networks themselves and all offensive, defensive, and exploitative activity within them.[1155]

By the fall of 2008, the OPNAV staff had discussed a number of different courses of action with regard to the Navy's treatment of cyberspace. Alternatives included whether to change NETWARCOM to Navy Cyber Forces Command, whether to create a new numbered fleet for cyber for the Navy, and whether to create a new cyber community.[1156] However, none of these proposals seemed holistic enough to satisfy the Chief's vision.

THE MERGER OF N2N6

In 2009, the CNO launched three sweeping organizational changes. First was the establishment of the Deputy Chief of Naval Operations for Information Dominance, a position on OPNAV staff that was created by merging the N2 and N6 into a single three star office.[1157] The standup of N2N6 was described as "a landmark transition in the evolution of naval warfare, designed to elevate information as a main battery of our warfighting capabilities, and firmly establish the U.S. Navy's prominence in intelligence, cyber warfare, and information management."[1158] It was also zero-sum, in that it could entail no additional growth within any of the involved organizations.[1159] The strategic objectives of N2N6 included the elevation of information to a core Navy warfighting capability; the functional integration of

---

[1155] Dorsett, "Discussions," 6.

[1156] Ibid., 8-9.

[1157] Roughead announced the directive on June 26, 2009. The reorganization began on October 1, 2009 and was completed by December. From Sam J. Locklear, NAVADMIN 286/09, "Department of the Navy Memorandum for Director of Naval Intelligence (N2), Reorganization of the Office of the Chief of Naval Operations (OPNAV) Staff," June 26, 2009.

[1158] Sam J. Locklear, NAVADMIN 316/09, "Establishment of the Deputy Chief of Naval Operations for Information Dominance (N2/N6)," October 29, 2009.

[1159] Gary Roughead, Memorandum for Director of Naval Intelligence (N2), June 26, 2009, "Reorganization of the Office of the Chief of Naval Operations (OPNAV) Staff."

intelligence, information warfare, information and network management, oceanography, and geospatial information; deliverance of assured command and control to operational forces; the introduction of "game-changing" concepts, strategies, and capabilities; coordinated resource investment for capabilities development; and the ability to deliver improved intelligence and understanding of potential adversaries.[1160]

The N2N6 was meant to solve several problems endemic to the Navy's previous approach to information. Foremost among these problems was the lack of a single resource sponsor for the various components of information operations, with information functions split among up to nine different elements of the OPNAV staff.[1161] The lack of unified sponsorship inherently precluded the development of a coherent information strategy, and made it prohibitively difficult for some of the more marginalized components of the information space to secure their own resources. Of particular concern in the chief's mind were electronic warfare and space, which had been effectively estranged from the Navy mainstream by virtue of their lack of a flag officer patron.[1162] Fragmented sponsorship made it difficult to discern who was responsible for what, and as a result interfered with the development of strategy, governance, and investment priorities in those fields which were deemed of lesser importance by the mainstream warfighting communities.[1163] The creation of N2N6 was intended to rectify this problem by unifying the Navy's information capabilities both structurally and strategically with a single boss who would operate under one conceptual framework.

A second problem the N2N6 merger sought to remedy, and one intimately tied to the fractured state of naval information operations, was the primacy of the platform communities. Traditional naval platforms have always held a dominant position within the service. The power of these platforms

---

[1160] NAVADMIN 316/09.

[1161] Dorsett, "Discussions," 9. Matthew J. Kohler, in a telephonic interview with the author, February 7, 2019, reiterated that N2N6 is a resource sponsor role.

[1162] Dorsett, interview.

[1163] Dorsett, "Discussions," 9.

communities meant that anything not of primary importance to surface warfare officers, submariners, or aviators, would likely be neglected.[1164] Since none of these communities had been primed or trained to think beyond the warfighter's traditional kinetic focus, this meant that matters of information would continue to be marginalized without the type of sweeping structural change that could force them to the forefront.[1165] Admiral Roughead's realignment of the OPNAV staff marked an explicit effort to break the power of the platforms by forcing just such a shift in the Navy's focus.[1166] Finally, N2N6 sought to overcome cultural barriers to cooperation by uniting culturally disparate information communities underneath a single staff directorate.

The shift in focus that Admiral Roughead sought to inspire had two parts. First was the notion, reminiscent of network-centric warfare theory, that the Navy's sea, air, and undersea platforms were nodes in how the service would fight. As such, the networks between these platforms — and the things that could be done from those networks — were nearly as important as the capabilities of the platforms themselves.[1167] However, as long as the platforms were culturally dominant, the Navy would never see the true effects of network-centric warfare theory.[1168] One prominent example of the platform communities' failure to properly prioritize its networks was their treatment of unmanned systems. Prior to N2N6, unmanned systems were managed by the platform community to which they belonged: aerial systems were managed by aviators, underwater systems by submariners, and surface systems by surface warfare. This arrangement often meant that unmanned systems would be the first to get cut under budgetary constraints.[1169] Roughead moved all unmanned systems under the N2N6 following the merger because

---

[1164] Roughead, interview.

[1165] Dorsett, "Discussions," 7.

[1166] Ibid., 10.

[1167] Roughead, interview.

[1168] Ibid.

[1169] Dorsett, interview. Unmanned systems weren't getting funded by the other communities, and Admiral Roughead wanted to protect the funding.

the platform communities were not prioritizing them highly enough.[1170] The movement of unmanned systems also had the added benefit of giving N2N6 a financial portfolio that would allow them to realistically compete for resources at the Pentagon.[1171]

Second was the idea that the information itself was more important than where that information may have originated. Instead of compartmentalizing information proficiency by source — from digital networks and cyberspace to satellites and meteorological data — the Navy should strive to integrate information into a single conception of information dominance. Roughead wanted the Navy to dominate the entire information arena, not merely to be proficient in its various components.[1172] In this regard, the N2N6 merger was not simply about program management, but about creating a whole capability based on seamless networks, integrated sensors, and data and analysis delivered to the warfighter.

The merger of N2N6 marked the beginning of a campaign to transform how the Navy viewed and managed information. Fundamentally, this campaign was about the pursuit of information dominance: the ability to seize and control the information domain when, where and however required for decisive competitive advantage across the range of Navy missions.[1173] The CNO's pursuit of information dominance directed that the Navy be the most prominent and dominant service in ISR, cyber warfare, command and control, electronic warfare, and information and knowledge management.[1174]

The Navy concept for information dominance and decision superiority encompassed several interrelated ideas about the purpose of information to warfare. Foremost among these ideas was the notion of information power as a prime operational instrument, on par with traditional naval warfighting platforms.

[1170] Roughead, interview.

[1171] Leigher, interview. Of note, the CNO following Roughead, Admiral Greenert, undid this move by returning the drones to their platform communities. This had a substantial impact to the N2N6 budget: the budget dropped from roughly $17 billion in 2014 to around $9 billion a few years later.

[1172] Dorsett, "Discussions," 10.

[1173] Kendall Card, "Information Dominance and the U.S. Navy's Cyber Warfare Vision," Powerpoint briefing by OPNAV N2/N6, April 16, 2010, slide 4.

[1174] Ibid., slide 4.

> To obtain information age dominance, we will exploit new opportunities in distributed command and control, networking, and use vast stores of collected data — information and intelligence that too often lies at rest, undiscovered, unavailable, and untapped. In short, information will be elevated to a "main battery" of the U.S. Navy's arsenal. We do not seek to replace kinetic combat with information warfare or diminish the need for traditional instruments of military power. Rather, we aim to develop a penetrating understanding of our adversaries and an unmatched knowledge of the operating environment to amplify traditional naval combat capabilities and expand options of your operational commanders.[1175]

To achieve information dominance, the Navy would have to transition from a force that

> relies on individual units managing their own electromagnetic spectrum, to fleets and battle forces collectively achieving command and control over the EMS in an automated fashion. This will require us to re-engineer our Navy — our concepts, our weapons, our battle management systems, and our people.[1176]

Unlike past naval transformations, the series of events that began with Admiral Roughead's merger of N2N6 in 2009 were not centered on the introduction of new platforms. Instead, Roughead's initiatives comprised an effort to break the power of the platforms by reshaping how the Navy thought about the information environment.[1177] As described by Vice Admiral Dorsett:

> The creative transformation the CNO has directed is analogous to the powerful revolutions in naval affairs that occurred when the Navy shifted from sail to stem, and from cruisers to dreadnoughts, or when it introduced naval aviation and nuclear power into the fleet. Comparable to these past revolutions, an older order is being supplanted by new structures and more efficient processes to deliver transformational, game-changing warfighting capabilities.

[1175] David J. Dorsett, "The U.S. Navy's Vision for Information Dominance," May 26, 2010, 1.

[1176] Ibid., 4.

[1177] David J. Dorsett, "Memorandum for the Information Dominance Corps," November 2, 2009.

THE CREATION OF FLEET CYBER COMMAND

On 29 January 2009, Admiral Roughead enacted his second major change with the creation of Fleet Cyber Command (FLTCYBERCOM) and the reactivation of the U.S. Navy's 10th Fleet.[1178] The former OPNAV N6 billet that had disappeared with the N2N6 merger was used to establish a Fleet Cyber Commander.[1179] The Fleet Cyber Command/Tenth Fleet initial strategic plan lists three command goals: to conduct full spectrum cyberspace operations in support of Navy, joint, and national requirements; to shape the Navy's cyber workforce; and to provide Navy cyberspace capabilities.[1180]

Like its Naval Network Warfare Command predecessor, Fleet Cyber took over a diverse mission set to serve as the central operational authority for networks, intelligence, cryptology, information operations, cyberspace, electronic warfare, and space in support of forces both afloat and ashore.[1181] Specifically, "FLTCYBERCOM directs cyberspace operations to deter and defeat aggression, [and] ensure freedom of action and achieve military objectives in and through cyberspace. FLTCYBERCOM organizes and directs Navy cryptologic operations worldwide and integrates Information Operations and Space planning and operations as directed."[1182] Fleet Cyber also assumed responsibility for all components of the cyberspace mission, to include cyberspace attack, defense, and the operation of Navy networks. Critically, because Fleet Cyber Command served as both the service cryptologic element and the service component command to U.S. Cyber Command, it possessed both Title 10 and Title 50

[1178] See "Our History," Naval Network Warfare Command website, accessed January 24, 2019, https://www.public.navy.mil/FLTFOR/nnwc/Pages/Command-History.aspx and "Command Description," U.S. Fleet Cyber Command/Tenth Fleet website, accessed January 24, 2019, https://www.public.navy.mil/fcc-c10f/Pages/home.aspx. The original 10th Fleet was created to address the problem of German U-boats during World War II. 10th Fleet was an integrative command, the only numbered fleet in the Navy with no assigned ships. Instead, it's sole purpose was to think differently about the U-boat problem. Similarly, when the Navy needed a command that could think differently about cyber, it chose to reactivate 10th Fleet due to the clear historic analogue.

[1179] Roughead, "Reorganization."

[1180] B.J. McCullough, "U.S. Fleet Cyber Command/U.S. Tenth Fleet Strategic Plan, Calendar Year 2011," May 17, 2011.

[1181] Gary Roughead, Memorandum for Commander U.S. Fleet Forces Command, Director of Naval Intelligence, "Fleet Cyber Command/Commander Tenth Fleet Implementation Plan," July 23, 2009.

[1182] Bill Leigher, "Fleet Cyber Command COMTENTHFLT NCBC 2-3 Dec 2009," briefing, December 2, 2009.

operating authorities.[1183] Possession of these dual authorities gave the command a flexibility that its sister organizations in the Army and Air Force, which were defined by a clear structural bifurcation between cyberspace and signals intelligence, did not possess.

Fleet Cyber Command was built around a typical Navy task force organization, with Tenth Fleet serving as the task force operational commander. This structure assigned regional responsibilities to subordinate task groups and provided a support framework for specific cryptologic requirements.[1184] The Navy moved nearly all of its network organizations under Fleet Cyber operational control. Naval Network Warfare Command, for example, was moved from an independent three star organization that was responsible for Navy cryptology and cyberspace missions to a subordinate Tenth Fleet task force, Task Force 1010, with the simplified mission to execute network and space operations.[1185] Navy Cyber Defense Operations Command became Task Force 1020 with responsibility for naval network defense. Fleet Cyber also took control of the Navy Information Operation Centers and rebranded each as a subordinate task force. The command was directed to achieve initial operating capacity by 1 October 2009, and full operational capacity by 1 October 2010.[1186]

Because Fleet Cyber was created to solve the problem of how to present cyber forces for operational use,[1187] it demanded an operationally-minded commander who could overcome the ingrained cultural divisions of the command's constituent tribes.[1188] Admiral Roughead selected a career surface warfare officer, Vice Admiral Barry McCullough for the task. In addition to creating a unified, fleet-focused culture, McCullough's initial priority was to establish an operational picture of the Navy's

---

[1183] Roughead, Memorandum, "Implementation Plan."

[1184] U.S. Congress, House, Armed Services Committee, *Digital Domain: Organize the Military Departments for Cyber Operations,* September 23, 2010, (statement of VADM Bernard J. McCullough III, Commander, US Fleet Cyber Command).

[1185] M.S. Rogers, M.A. Brown, W.E. Leigher, S.R. Filipowski, J.E. Tighe, G.W. Clusen, W.L. Metts, J.P. Rapin, M.D. Neighbors, "Cryptologic Community Foundational Principles," document, 7 Sep 2011; Roughead, Memorandum, "Implementation Plan."

[1186] Roughead, Memorandum, "Implementation Plan."

[1187] Parode, interview.

[1188] McCullough, interview.

networks, akin to what an operational commander would expect to see for his physical battlespace. McCullough refocused his initial budget towards standing up an operations center that would achieve this critical task. The focus of the center was to define the network, establish a comprehensive understanding of threats and vulnerabilities, and then figure out how to develop appropriate cyber tools for both network defense and offense.[1189]

McCullough also faced substantial cultural challenges in establishing Fleet Cyber Command. These cultural issues were in many ways far more difficult to address than the operational ones. The most fundamental of these challenges was in getting the command's traditional support communities — many of whom were career cryptologists who had grown accustomed to supporting the national SIGINT enterprise rather than the warfighting Navy — more operationally focused.[1190] McCullough put up pictures of ships, airplanes, and submarines in the Fleet Cyber headquarters to emphasize the command's ultimate customer.[1191] McCullough also got the command involved in a series of Pacific Fleet exercises called Terminal Fury from 2010-2011. Fleet Cyber sailors provided network support to this combatant command-level exercise in the form of a joint cyber operations center — an effort which helped to convince both the Navy's warfighters and the information dominance sailors of how cyberspace could be relevant to the fleet. Finally, McCullough instituted a series of cyber inspections to both examine and enforce cyber hygiene on ships. These inspections served to increase awareness of cyberspace fleet-wide, and also to explore what type of capabilities it would be possible to give to an individual ship commander.[1192]

[1189] McCullough, interview. Admiral McCullough sought inspiration from a number of private companies, to include ISPs and telecoms companies, to see how they achieved a real-time picture of their networks.

[1190] "Operational Culture" was listed as the commander's first guiding principle in the U.S. Fleet Cyber Command/U.S. Tenth Fleet Strategic Plan for calendar year 2011. This was also affirmed in the author's interview with VADM McCullough. Of note, McCullogh also highlighted the more consensus-based cryptologic culture as an obstacle to implementing change, which contrasted with the the hierarchical culture to which McCullough had grown accustomed as a SWO.

[1191] McCullough, interview.

[1192] Ibid.

A second issue concerned the distinction between administrative and operational control. The Navy maintains separate operational and administrative commands for its warfighting personnel: operational commanders own the mission, and the communities own the man/train/equip function for those missions.[1193] In the big three warfighting communities, administrative commands, called Type Commands, are responsible for the training and readiness of the individual platform communities. These commands send trained and ready personnel to operational commanders for deployment. Once deployed, operational control of any particular fighting formation will shift as that formation moves through different geographic theaters. From McCullough's standpoint, the fact that the sailors in Fleet Cyber remained geographically stationary in the course of their duties meant that they would never shift to other operational commands.[1194] To simplify the process of personnel management, McCullough fought to retain full administrative and operational control of his personnel.[1195] Because it ran contrary to the traditional Navy way of doing things, this move proved to be a significant cultural adjustment for the rest of the institutional Navy.[1196]

THE CREATION OF THE INFORMATION DOMINANCE COMMUNITY

If the network was to be a warfighting platform, and if information was to be a core warfighting capability, then it followed that it would need its own community to fight and maneuver within it.[1197] In 2009, Admiral Roughead followed the merger of N2N6 and the establishment of Fleet Cyber Command with the creation of the Information Dominance Corps (IDC). The information dominance corps

[1193] Tighe, interview.

[1194] Initial administrative control went to a new organization called Navy Cyber Forces (CYBERFOR), established 18 January 2010 under Naval Fleet Forces Command with the mission to man, train, and equip the Navy's cyber force (Kevin R. Hooley, interview with the author, February 13, 2019). This organization later became Navy Information Dominance Forces (NAVIDFOR) and later Naval Information Forces (NAVIFOR). ("Naval Information Forces," IWCsync, https://www.iwcsync.org/about/navifor).

[1195] Roughead, Memorandum, "Implementation Plan;" David J. Dorsett, "Memorandum for the Information Dominance Corps," DCNO Update, April 2, 2010.

[1196] McCullough, interview.

[1197] A 2011 pamphlet on the Information Dominance Corps described the purpose of the IDC as: to fight and maneuver in cyberspace and the EMS.

brought 44,000 personnel within the Navy's five information-related communities — intelligence, cryptology, information technicians, space, and meteorology and oceanography — under a single integrating personnel construct.[1198] The intent was to structurally reinforce the CNO's vision of a holistic information ecosystem, and in so doing to remove the stovepipes that had impeded the Navy's approach to information integration in the past.[1199]

The creation of the IDC did not eliminate each of the five communities that comprised it. Rather, each community would retain its separate areas of expertise, but would also have to accumulate a generalized and generalizable knowledge of each of the other four subject areas that would allow the communities to compete with one another for promotion and command. This meant that, in theory, any member of the information dominance community could qualify for any type of information dominance command: a meteorology and oceanography officer could just as easily be selected to serve as information dominance composite warfare commander of a strike group as could an intelligence or cryptologic officer. The intent was to create information dominance officers who were

> specialized experts within their parent community, and subject matter experts in general information dominance warfare. The specialization allows them to excel as technical experts within their community. The general information dominance expertise allows for synergy between the various communities and acts as a force multiplier within the information domain.[1200]

On February 19th, 2010, Admiral Roughead announced the approval of the Information Dominance Corps Warfare program for officers and enlisted.[1201] With this approval came four significant changes. First was the designation of information dominance as a warfare specialty, akin to surface, subsurface, and aviation. With that designation came the second major change, which was the creation of

---

[1198] David J. Dorsett, "NIP Information Dominance Presentation," briefing, October 16, 2009.

[1199] Card, "Information Dominance."

[1200] Kendall L. Card, OPNAV Instruction 1412.15, "Information Dominance Corps Command Qualification Program," December 3, 2012.

[1201] David J. Dorsett, "IDC Officer Community Consolidation 18XX Memo," February 10, 2019.

an information dominance community warfare pin.[1202] Warfare pins were uniform badges worn to distinguish specific warfare expertise. They served as the primary visible distinctions between the service's warfighters — aviators, submariners, surface warfare officers, special operations, and explosive ordinance disposal — and their support. The adoption of a warfare pin put the information dominance community aesthetically on par with their platform-focused peers. The third change was the creation of a standardized qualification process to earn that warfare pin, a move which again sought to mimic the qualification processes found within the Navy's traditional warfighting communities.[1203] The fourth and final change was the consolidation of the five information dominance officer communities into a single 18XX series of designators to further reinforce the community relationship and to establish a common lexicon for cross-detailing assignments.[1204]

Table 8. Navy Information Warfare Community[1205]

Designation	Purpose
1800	Meteorology and Oceanography (METOC)
1810	Cryptologic Warfare
1820	Information Professional
1830	Intelligence
1840	Cyber Warfare Engineer

There were three significant consequences of the creation of the IDC. First was the establishment of new career paths that forced members of the individual IDC communities outside of their core

[1202] Mark Ferguson, NAVADMIN 058/10, "Information Dominance Corps Warfare Insignia," February 19, 2010.

[1203] David J. Dorsett, NAVADMIN 314/10, "Enlisted Information Dominance Warfare Specialist Program," September 20, 2010; David J. Dorsett, NAVADMIN 328/10, "Information Dominance Warfare Officer Program," October 1, 2010; David J. Dorsett, NAVADMIN 062/11, "Enlisted Information Dominance Warfare Specialist Program," February 23, 2011.

[1204] Dorsett, "IDC Officer Community Consolidation." See also Mark Ferguson, NAVADMIN 206/10, "Information Dominance Corps Officer Designator Alignment," June 22, 2010, and NAVADMIN 058/10.

[1205] The Information Dominance Community was renamed the Information Warfare Community in 2016.

specialties. This emphasis on broadening was in line with the Navy's effort to create a more well-rounded cadre of officers and enlisted who could use their generalized knowledge to contribute to a broader range of Navy missions. It also reflected the personnel management practices of the Navy's other major warfare areas, in which unrestricted line officers were expected to be able to command mixed-type maneuver units comprised of a broad variety of capabilities.[1206] The second consequence was that it enforced a new perspective on the role of information-centric naval personnel. This perspective marked a deliberate shift from information as enabler to information as a warfighting specialty, and as such was in line with the OPNAV staff reorganization into N2N6. Finally, the creation of the IDC expanded the Navy's information community from a series of small, narrowly defined specialties to a larger and more diverse corps.[1207]

The creation of the IDC was accompanied by appropriate shifts in training, education, and personnel management. In September 2009, the Navy created a new officer rating called Cyber Warfare Engineer (CWE), to address the increased demand for officers with computer network operations expertise.[1208] Officers were selected for a direct commission based on outstanding technical academic records in the fields of computer science, electrical engineering, computer engineering, and other information technology related programs. Unlike the cyberspace career paths established in the Army and Air Force, however, the cyber warfare engineer was deliberately limited in scope: CWE officers were assessed into the service to serve in high skill technical jobs for five years, after which point they would have to either leave the service or cross over into another rating to continue in their naval careers.[1209]

[1206] Henry Stephenson, "Masters or Jacks?" *Proceedings* Issue 140 (October 2014).

[1207] David J. Dorsettt, "The Information Dominance Corps: What Does it Mean to Me?" Note From the DCNO for Information Dominance, June 14, 2010.

[1208] Roughead, Memorandum for Director of Naval Intelligence (N2). 26 June 2009. "Reorganization of the Office of the Chief of Naval Operations (OPNAV) Staff" and Mark Ferguson, NAVADMIN 205/10, "Establishment of the Cyber Warfare Engineer Designator," June 21, 2010.

[1209] The Navy had two other officer designators that followed this five year, limited career accessions model: 1210 Nuclear Power School Instructor, and 1220 Naval Reactor Engineer. Like the CWEs, 1210 and 1220 officers were recruited to serve for a limited period of time in a limited duty capacity based on a set of highly specialized technical skills. There was no expectation that they would go to sea, or otherwise serve in any capacity outside of their technical designations.

CWEs would thus be prohibited from serving beyond the rank of lieutenant (O3), and precluded from a long-term Navy career as cyberspace specialists. CWEs provided the bulk of the Navy's technical expertise and tended to be concentrated in cyberspace research and development organizations, like NIOC Suitland.[1210]

In April of 2010, the Navy established cyber warfare warrant officers under the 743X designation. This move was also intended to address the increasing demand for officers with specific computer network expertise. Accessions into the cyber warrant warrant officer field were initially limited to enlisted sailors in the rank of E7 who were already qualified as apprentice interactive network operators.[1211] This limitation was lifted as cyber warfare warrant duties and responsibilities evolved, with warrants eventually recruited from the ranks of E5 and E6 who were no longer required to possess interactive network operator qualification.[1212] Finally, beginning in October 2010, the Navy added an introductory course in cyber warfare to its officer and enlisted intelligence training at the Navy Marine Corps Intelligence Training Center in Dam Neck, Virginia.[1213]

Officer accessions programs also began to institute changes in order to better prepare for the Navy's emphasis on information dominance. In June of 2009, the Naval Academy Academic Dean created the Cyber Warfare Ad Hoc Committee to define the scope of cyber understanding needed by future naval officers.[1214] The committee's work led to a number of changes to the Naval Academy curriculum. First, beginning in 2011, the Naval Academy added two courses in cyberspace operations to its mandatory curriculum: an introductory course on the technical fundamentals of cybersecurity for

---

[1210] Tighe, interview.

[1211] Mark Ferguson, NAVADMIN 139/10, "Establishment of the Cyber Warrant Officer Community," April 20, 2010.

[1212] Heritage, interview. See also R. P. Burke, NAVADMIN 177/16, "Change to the Cyber Warrant Officer Commissioning Program," August 10, 2016.

[1213] David J. Dorsett, "Note from the DCNO for Information Dominance," October 21, 2010.

[1214] Tracy Emmersen, Joseph M. Hatfield, Jeff Kosseff, Stephen R. Orr IV, "The U.S. Naval Academy's Interdisciplinary Approach to Cyber Security Operations," *Computer* 52:3 (March 2019): 48-57. In an interview with Chris Inglis, one of the cyber advisory board members as the then-Deputy Director of the NSA, the Naval Academy was responding to a very strong demand signal from Admiral Mullen, who was the Chairman of the Joint Chiefs of Staff when Buckshot Yankee hit the Department of Defense.

freshman followed by a more detailed, technical course for juniors.[1215] The freshman course was intended to give students a principled understanding of the basic physical and virtual architecture of the cyber domain. Upon its completion, midshipmen were able to explain why the cyber domain is important to the Navy, describe the operational components of computer fundamentals, analyze and explain the output of programs, identify and describe the principles of defensible information systems, and perform basic actions related to attack, defense, and forensic analysis of information systems.[1216] The junior offering was a project-based course that introduced students to information warfare, electronic warfare, and offensive and defensive cyberspace operations.

In addition to the two mandatory courses, the Naval Academy introduced a new cyber operations major in 2013, with the first class of midshipmen graduating in 2016. The cyber operations major was an interdisciplinary course of study that included aspects of law, policy, human factors, ethics, and risk management in addition to its technical course offerings.[1217] This interdisciplinary nature granted cyber operations graduates a deep understanding of the intersection between technical and non-technical aspects of cyberspace operations. At the time of its creation, the cyber operations major was the third most programming-heavy major at the Naval Academy behind computer science and information technology. Of note, the cyber operations major was housed in its own Cyber Science Department that was separate from the related departments of Computer Science and Electrical Engineering. The Naval Academy also established a Center for Cyber Security Studies, an outward-oriented think tank designed to foster links with other cyber-focused organizations.[1218]

[1215] The Naval Academy had a previous mandatory course in computer programming that was dropped from the curriculum in the early 2000s. (John C. Inglis, telephonic interview with the author, January 30, 2019).

[1216] Emmerson, et al. "Interdisciplinary Approach."

[1217] Technical course offerings still comprise 80% of the major..

[1218] Emmerson, et al. "Interdisciplinary Approach."

The cyber operations major has proven popular. Numbers of midshipmen have expanded from 22 in the first graduating class to 110 — or 9.3 percent of the student body — in the class of 2021.[1219] Since the Navy lacks a cyberspace operations community, most graduates of the program go on to become cryptologic warfare officers. However, a number of grads also become pilots, surface warfare officers, information professionals, and others.[1220] Since its inception, variants of the cyber operations major have been replicated at naval ROTC programs around the country.[1221]

Given that the Navy does not have a cyberspace operations career field — and that the Navy only recently allowed USNA graduates to commission directly into cryptology, rather than transferring into the field later in their careers — what explains the Naval Academy's decision to create a separate cyber operations major rather than keep its cyber expertise within the existing department of Computer Science?[1222] The program's architects decided early on that cyber operations were not a proper subset of computer science. Whereas computer science was seen as a purely technical discipline, cyberspace, as an operational field, was seen as a blend of technical, procedural, and human factors. The distinction between the operational mindset of cyberspace and the more technical approach of computer science created friction between the two camps during the initial effort to carve out space for cyber inside the computer science department.[1223] It was for this reason that Academy officials took care to describe the

---

[1219] Joseph Hatfield, "U.S. Naval Academy Cyber Education: Turning Midshipmen into Cyber Warriors," Powerpoint brief, July 2018. Interestingly, while the Computer Science Department originally viewed Cyber Science as a threat, the growth of the cyber operations major has occurred in tandem with the growth of the computer science major. Before the introduction of the cyber operations major, approximately 50-60 midshipmen in any given year majored in computer science. Now, there are roughly 175-180 midshipmen between the two majors of computer science and cyber science. Also of note, surveys have indicated that the two most popular second choice majors among midshipmen in cyber operations were aerospace engineering followed by political science. This suggests that the major attracts a mix of thinkers who are both operationally and technically-minded.

[1220] Ibid. Exact breakdown follows: Class of 2016, 7/27 IW; Class of 2017: 10/46 IW; Class of 2018, 11/24 IW.

[1221] Inglis, interview. Emmersen, et al. "Interdisciplinary Approach."

[1222] Cryptologic Warfare used to be restricted either to ROTC graduates or to USNA grads who were not physically qualified to serve in unrestricted line communities. The Academy was recently given authority to commission up to fifteen people directly into the cryptologic warfare community. According to one individual who was intimately tied to that decision, it was influenced by the fact that West Point graduates were able to commission directly into the cyber branch. As he stated, "The Army-Navy rivalry helps sometimes."

[1223] Inglis, interview.

cyber operations major as a major in operations dependent upon cyber, not as a major in cyberspace operations.[1224]

One can also speculate that the services' respective professional education structures might account for the different approaches to service academy training. Since the Army relies upon a robust professional education system to train its officers in appropriate doctrine, operations, and tactics at each level of promotion, it can afford to have its new lieutenants more well-versed in technology than in operations. West Point's decision to rely upon the existing majors of Computer Science, Information Technology, and Electrical Engineering — as well as Physics and Math — to produce its cadre of cyberspace operations officers could therefore be predicated upon the expectation that these individuals would receive adequate operational training after graduation. However, since the Navy lacks a commensurate post-commissioning professional education program, with most new ensigns learning their respective trades through on-the-job training after short introductory community courses, it would make sense to require a more comprehensive, operationally focused cyberspace major.

In 2016, a new Chief of Naval Operations, Admiral Richardson, renamed the information dominance community. Convinced that the notion of "dominance" was hubristic and insufficiently urgent for an anticipated future of great power conflict, he replaced the word "dominance" with "warfare" to create the Navy's Information Warfare community.[1225] Concurrent to this change, the cryptologic community, which had adopted the Information Warfare moniker in 2005, returned to their cryptologic heritage by assuming the new name of Cryptologic Warfare.[1226] This renaming was accompanied by the distillation of the community's role into three competencies: signals intelligence, electronic warfare, and cyberspace operations. In an effort to continue to structure the information space in a way that would be familiar to the unrestricted line communities, the Navy created the Naval Information Forces type

---

[1224] Inglis, interview.

[1225] Ted Branch, NAVADMIN 023/16, "Information Dominance Corps Redesignated Information Warfare Community," February 2, 2016.

[1226] Heritage, interview.

command in 2014, and the Navy Information Warfare Development Center in 2017.[1227] The Information Warfare Community now had a type command to generate readiness, and a development center to refine the role of information warfare at sea.[1228] These changes completed the transformation of the Navy's information warfare infrastructure to match that of the service's big three warfighting communities.

COMMUNITY REACTIONS

The totality of the reforms undertaken by the Navy from 2009 to 2017 had culminated in an information warfare community that looked like the other naval warfare areas: it had a resource sponsor to buy things, a system command to acquire and maintain those things, and a type command to man, train, and equip the operational force. It had a warfare pin and warfare qualification standards, a composite warfare billet at sea, and a community infrastructure designed to create broad-minded leaders capable of commanding across different information modalities. Each of these reforms was designed to move information from the periphery to the core of naval operations, with cyberspace as one component of that shift. However, since the consolidation of N2N6 and the creation of the information dominance corps were driven largely by the need to overcome the entrenchment of individual service cultures, these efforts prompted an understandably strong reaction from the communities who were affected by them.[1229]

The big three warfighting communities experienced a twofold discomfort with Roughead's reforms. The first concern was that they were losing assets — and, more importantly, the money tied to those assets — in the reallocation of unmanned systems away from their communities and into N2N6. Second was the concern that information was being unjustly placed on par with their own traditional

---

[1227] Mark Pomerleau, "Navy Creates Information Warfare Development Center," *Navy Times*, February 24, 2017; Eckstein Fuentes, "Navy Information Warfare Effort Set to Expand, Evolve," *Navy Times*, February 7, 2018.

[1228] Tighe, interview.

[1229] According to Vice Admiral Dorsett, "Overcoming service cultures was the reason we made dramatic changes to the Navy in 08/09 with N2N6." Bill Leigher also testified that the creation of the IDC was meant to knock down some of the cultural walls that existed by forcing members of different communities to compete for promotion.

warfighting expertise.[1230] The saving grace in keeping these communities at bay was Admiral Roughead himself, a career surface warfare officer who had the vision to push forward and the reputation to quell the discord from below.

The concerns of the Navy's warfighting communities are not surprising given that they were, in many ways, the primary audience of Roughead's reforms. The structure of naval information capability had been unrecognizable to the main communities that information was supposed to serve prior to Roughead's reforms. In a way, this structure predetermined that information would be treated as merely another form of supporting fires rather than given the place of prominence that the Navy's emerging information dominance theory required. Each of Roughead's incremental changes — promoting the N2 to a three star, commensurate with senior leadership of the other platform communities; merging N2N6 and expanding their budget by assigning them tangible unmanned platforms; creating the information dominance community and granting that community a warfare pin; and creating a numbered cyber fleet — were designed to leverage the symbolism of Navy warfighting in order to depict information in a language that the dominant Navy service cultures could understand.[1231] The selection of a respected surface warfare officer, Admiral Barry McCullough, as the first commander of Fleet Cyber Command, only reinforced this intent. McCullough's experience helped him to operationalize the Navy's nascent cyberspace concepts, while his reputation as a warfighter sent a message about the importance of Fleet Cyber to the rest of the Navy.

Within the cryptologic community, most negative reactions centered around a fear that the IDC's emphasis on broadening assignments would come at the expense of the cryptologic community's core signals intelligence skill set.[1232] As the only remaining dedicated cryptologic community among the military services, cryptologists were wary of any further generalizing trends that would seek to turn their

---

[1230] Brooks, interview.

[1231] Deets, interview.

[1232] Brown, Dorsett, interviews.

community into broad-functioning intelligence officers.[1233] While many cryptologists saw cyberspace operations as a natural evolution and thus a logical extension of cryptology, they did not want that evolution to come at the expense of the community's classical SIGINT expertise.[1234]

The intelligence community, as a second naval community with a proud heritage and a storied history, was also concerned that the merger would potentially blur the distinction between the intelligence and cryptologic functions. In particular, the community was loathe to accept any change that would relegate the proud tradition of naval intelligence to a conceptual subcategory of an untested information theory.[1235] In understanding this reluctance, it is important to reflect once again upon the historic rivalry between the intelligence and cryptologic communities.[1236]

Intelligence and cryptology were operationally united by a common enemy during the Cold War. However, the demise of the Soviet Union led the respective communities to move in two different directions in response to a new strategic environment: cryptology endeavored to become more operational and warlike with their pursuit of computer network operations and information warfare, while intelligence struggled to find its role in a world that had less demand for maritime great power analysis and a far greater need for joint intelligence that supported land forces and special operations.[1237] The intelligence community was similarly reluctant to recognize the potential of cyberspace and related changes in the information domain.[1238]

[1233] Brown, interview.

[1234] Michael Rogers, interview with the author, January 2, 2019.

[1235] The Office of Naval Intelligence, established in 1882, is the oldest purely intelligence organization in the U.S. Government.

[1236] Nearly all former cryptologists and intelligence officers that I interviewed affirmed the existence of this rivalry.

[1237] Turner, interview.

[1238] Wolf Melbourne, "The Intelligence Community's Lost Decade," *Proceedings*, December 2018. The author states: "Far too much effort has been devoted to administratively adapting naval intelligence to the bureaucratic structure of the IWC, and too little has been invested in recruiting, training, and cultivating the types of analysts needed. Just as the nature of the information domain has changed, so too must the composite skill set of the naval intelligence professional. Naval intelligence needs more critical thinkers who can separate signal from noise and transform information into knowledge. Analysts need to be more than information warriors—they need to be knowledge warriors."

Already hesitant to accept the intelligence transformation that 21st century geopolitical realities demanded, intelligence personnel saw the changes wrought by cyberspace as yet another threat to their core identity and expertise.[1239] This hesitation to embrace the Navy's concept of information dominance is largely to blame for the fact that Vice Admiral Dorsett was the only intelligence officer to fill the N2N6 billet between 2011 and 2018.[1240] One could also speculate that it is the reason why Fleet Cyber Command has never been commanded by an intelligence officer.[1241] Furthermore, the intelligence community was reluctant to embrace the "warfighter" designation that implicitly followed the Navy's embrace of information as a warfare area.[1242] In contrast to the cryptologists, for whom the attack and defense of signals had always been an operational endeavor, intelligence officers had traditionally seen themselves as professional staff officers. The warfare emphasis of the information dominance construct threatened this sense of professional identity.

The reaction from the communications community, comprised of officer information professionals and enlisted information technicians, was similarly mixed. On the one hand, as a small community with no real historical lineage and little collective identity, many communications specialists recognized the advantages of being subsumed by a larger personnel superstructure. Being a part of the 44,000 person information dominance community would thus offer benefits in training, promotion, and budgetary considerations that the information professionals would not be able to achieve on their own.[1243] However, these perks came with the simultaneous fear that the communications population risked being substantially overshadowed, if not completely subsumed, by the much older, much larger communities of intelligence and cryptology.[1244]

[1239] Brown, Rogers, interviews.

[1240] Vice Admiral Matthew Kohler, who assumed the role of N2N6 in June 2018, was the first intelligence officer to hold the position since Jack Dorsett. Rogers, Brown, interviews.

[1241] At the time of this writing, Fleet Cyber has had two line officers and three cryptologic warfare officers as its commanders.

[1242] Neighbors, interview.

[1243] Brooks, interview.

[1244] Deets, Dorsett, interviews.

What explains the Navy's decision to include meteorology and oceanography within its information dominance construct, particularly at the exclusion of other, perhaps more informationally-relevant communities like public affairs or the Navy's foreign affairs officers? The decision to include METOC further reinforces the sense of inclusivity that defined Admiral Roughead's vision for the information domain. The ultimate purpose of the information dominance community was "to ensure the commander gets the right information to the right place at the right time so they can effectively perceive, understand, reason, decide, and as the culture of the Navy, command."[1245] Commensurate with this purpose, Roughead believed that the source of information was irrelevant to how it was used. The oceanographer community, focused as they were on weather and sea patterns, produced perhaps the most immediately relevant information for a seafaring service.[1246] As such, METOC was seen as far more relevant to the achievement of decision superiority than something like public affairs.[1247]

In addition to the theoretical justification, there were significant monetary considerations that drove METOC under the umbrella of information dominance as well. The METOC community had suffered large cuts in personnel and budget during the early 2000s based upon a growing belief that the Navy could save money by outsourcing its predictive weather analysis.[1248] Information dominance leadership saw the inclusion of METOC as a way to protect the community and its critical functionality from further cuts.[1249]

[1245] Roughead. "Information Dominance: The Navy's Initiative."

[1246] In the words of Admiral Roughead during an interview with the author, "If I wanted to know whether pirates would be in the Somali basin, I didn't talk to intel, I talked to my weather guesser."

[1247] Two overriding concerns ultimately led to the exclusion of public affairs from information dominance. First, that they were terrible at keeping secrets by design, and second, that their inclusion would cause them to be involved in deception, which was illegal. Parode, interview.

[1248] Turner, interview.

[1249] Ibid.

WHAT ABOUT CYBER?

Given Admiral Roughead's recognition that the Navy was most deficient in cyberspace of all the information-related functions, why did the he choose not to include the creation of a new cyberspace-focused career path in his series of organizational reforms? Why does the Navy still remain alone among the services in its insistence that cyberspace is neither separate nor distinct from the rest of the information domain?

The fact that the Navy chose not to create a separate cyber career field does not mean that the idea was never discussed. On the contrary, similar such ideas were floated around the cryptologic community and within the OPNAV staff before being formally proposed — and formally rejected — to the Chief of Naval Operations by the Strategic Studies Group in 2007. However, two factors prevented these ideas from ever receiving serious consideration or material investment: the Navy's strong history in cryptology, and its decision to anchor its theoretical innovation on the idea of information dominance rather than on the idea of cyberspace.

Regarding the former, both the strength of the Navy's cryptologic community and the service's implicit deference to its cryptologic heritage gave the community free license to define cyberspace as it saw fit. When combined with the lack of community competitors, akin to the signal branch in the Army or the communicators in the Air Force, Navy leadership never really questioned the idea that cyberspace could belong anywhere else.[1250] The Navy's unique cryptologic partnership with the National Security Agency also had a significant influence on the early perception that cyberspace was simply another technological evolution in the field of signals intelligence.[1251] Even as this perception began to shift in the early 2000s to the idea that cyberspace might afford a potential for offensive action that exceeded the legal authorities

[1250] Dorsett, Tighe, Rogers, interviews.

[1251] Tighe, interview.

available to intelligence collectors, the lack of any competitor communities meant that, whatever cyberspace ultimately became, it would still implicitly belong to the cryptologists.[1252]

Regarding the latter, all of Admiral Roughead's 2009 reforms — the creation of the information dominance community, N2N6, and a Fleet Cyber Command with an expansive portfolio of responsibilities — were predicated upon the assumption that the information space was a single unified continuum in which all components were of equal importance.[1253] Adding yet another tribe to the mix in the form of a separate cyberspace community was seen as counterproductive to both the vision of the IDC and the structural reforms that were created to enact it.[1254] Roughead was intent upon enacting a structural reorganization that would overcome community tribalism through a holistic framework for information that preserved the independence of individual communities while still forcing collaboration across them.[1255] These factors made it difficult for the Navy to justify the creation of a separate cyberspace community or an independent cyberspace operations construct.

Conclusion

The Navy first began to experiment with cyberspace operations and organizations in the late 1990s through a substantial investment of signals intelligence personnel into select elements of the National Security Agency. This NSA partnership allowed the Navy to gain a level of operational proficiency in cyberspace in the early 2000s that was unmatched by the other military services. However, the very same strength of the cryptologic community ultimately proved to be a weakness: recommendations to create a separate cyberspace career field, organization, and warfare area in the mid-2000s were unable to gain institutional traction due to the implicit assumption that cyberspace,

[1252] Dorsett, Tighe, Rogers, interviews.

[1253] Brooks, interview.

[1254] Ibid.

[1255] Deets, interview.

regardless of how little or much of it comprised actual intelligence collection, ultimately belonged with the cryptologists. Furthermore, the very strength of the Navy's relationship with the national intelligence enterprise served to dissuade any innovation that offered too much service independence.

As theories of cyberspace operations began to work their way up to senior Navy leadership, the need for an independent cyberspace operational concept quickly grew subordinate to the need to tame the larger informational environment of which cyberspace was a part. Thus, in its integration with the dominant Navy service cultures, cyberspace was ultimately subsumed into a theory of information dominance whose origins can be traced back to the information saturation problems of the second World War — and, in turn, to the inherent communication challenges of a distributed maritime fighting force. The model that the Navy eventually adopted for its cyberspace operations was not, therefore, driven by cyberspace operations, nor was it focused on optimizing activity in the cyberspace domain.[1256] In this sense, the information dominance theory that the Navy embraced to capture its approach to cyberspace is little more than a contemporary answer to a decades-old problem: how to overcome the challenge of information saturation on a sensor-dependent, three-dimensional battlefield.

[1256] Kohler, interview.

CHAPTER 6 | **Conclusion**

The inspiration for this dissertation arose from observation of a simple puzzle: if cyberspace technology is the same everywhere, what explains variation in how different military organizations have chosen to use it? The resultant theoretical framework rests upon two complimentary hypotheses. First, that the initial process of innovation under conditions of uncertainty will be driven by the cognitive and behavioral predispositions of the service subcultures which are given responsibility for it. Second, that as uncertainty about the nature of the innovation diminishes, the role of these subcultures will likewise diminish, and will be replaced by the strategic vision of the military service writ large. Competition among different ideas will be resolved in a way that aligns with the broader service mission and the dominant service culture. The history of cyberspace innovation in the U.S. military offers an affirmation of both hypotheses.

SUMMARY OF FINDINGS

Cyberspace operations began under similar conditions in all three military services, spurred on by the command and control warfare theories that found success in Desert Storm. The resultant theoretical framework was based upon the premise that future wars would be won by the side which could most rapidly gain and exploit information. Implicit in this thinking was the need to defend one's own information systems, to attack those of the adversary, and to deny the adversary the same capability, all of which served the purpose of affecting the enemy's ability to make sound decisions. The notion of cyberspace operations as something that could achieve discrete battlefield effects was first articulated in these information warfare theories. Simultaneous developments in the signals intelligence community led to a migration of collection methods into the digital realm. These developments confronted the services with two simultaneous problems: how to defend and attack information systems, and how to exploit the new digital environment for maximum intelligence value.

However, the lack of a unified national strategy for information warfare, combined with joint ambivalence on both doctrinal terminology and the concepts behind it, afforded the services a wide degree of latitude in how they approached the domain from the mid-1990s into the 2000s. The influence of subcultures came to the fore during this period to create substantial variation in how each service approached cyberspace doctrinally, and in how each service solved problems of training, personnel, and organizational development.

The creation of Cyber Command in 2009 marked an inflection point in the cyber innovation story. Its impact was twofold. First, Cyber Command forced service senior leadership to take a more concerted interest in cyberspace and in the various subcultural initiatives that had taken place in the services to that point. Second, it had the effect of decreasing the uncertainty surrounding cyberspace by imposing certain structural and doctrinal frameworks upon its pursuit. The creation of Cyber Command thus set the conditions necessary for this dissertation's second hypothesis to take effect: reduced uncertainty and increased senior leader involvement caused the dominant service culture to overtake the service subcultures as the primary determinant of the innovation outcome.

Importantly, however, personnel management within the services was not standardized following the creation of Cyber Command. This allowed for the continued manifestation of service cultural imprints on the process of creating cyber personnel cohorts. Various service-specific initiatives also arose during this time period that reflected each service's culture and priorities.

Army

In the Army, cyberspace operations developed through the interaction of five different subcommunities: information operations, signals intelligence, signal, space, and electronic warfare. From roughly 1995 to 2010, cyberspace operations were comprised of a collection of individual efforts that were dominated by the intelligence, signal, and information operations subcommunities. With no clear guidance from Army senior leadership, each community defaulted to an understanding of cyberspace that

was shaped by their existing cultural and operational predispositions. Each community's respective effort to expand cyberspace operations during the mid-2000s was thwarted by a technologically averse institutional culture, combined with senior leader preoccupation with the ground wars in Iraq and Afghanistan.

The creation of Army Cyber Command in 2010 marked the beginning of a period of transition to a more unified service approach, albeit one hindered by continued disagreement between the intelligence and signal communities over who should play the dominant role in the new warfighting domain. The information operations community also contributed to this discussion, though their influence was attenuated by changes in doctrine and inconsistent performance in Iraq and Afghanistan. The Army Chief of Staff's discontent over the subcommunities' inability to resolve their disagreements contributed to his decision to direct the creation of a new, independent cyber infrastructure. Critically, the Army chose not to designate this new career field as a component of combat arms on par with the service's chief warfighting communities. This decision came in spite of the extent to which the Army had begun to value the integration of cyber effects with ground force maneuver.

The establishment of a cyber career field and attendant training structures in 2014, along with the Chief of Staff directive to drop operations to the tactical level in order to make it relevant to maneuver, finally granted cyberspace the institutional momentum it needed to break free from the constraints of its previous subcultural influences and to move from a peripheral to a core Army function. This effort resulted in the creation of tactically-focused cyberspace units that were trained and equipped to provide cyberspace effects for maneuver commanders. Subcultures which were formerly abandoned, such as electronic warfare, took on new significance once embraced by the Army cyber enterprise, and were allowed to flourish in ways that they never could when fighting for dominance on their own.

The creation of the Army cyberspace operator position in 2017 further distinguished the Army's path from that of the other services: no longer reliant on the national cryptologic enterprise to train and certify its remote operators, the Army was free to pursue independent Title 10 cyberspace operations in

support of ground force maneuver. This action stood in noteworthy contrast to the Navy, which was reluctant to take action that would jeopardize its historically close relationship to the national cryptologic enterprise. The manner in which the Army accelerated its efforts to institutionalize and operationalize cyberspace from 2014 to 2019 caused the formerly skeptical service to emerge as a leader in joint cyberspace operations.

Air Force

The Air Force began to experiment with cyberspace operations, doctrine, and organizations at least a decade prior to any other military service, with its first operational cyber unit coming online in 1995. This experimentation was the culmination of decades of theorizing on how information and information technology might affect the outcome of future war. To Air Force thinkers, the strategic perspective and global experience gained from operating in the aerospace continuum made the service uniquely qualified to embrace cyberspace as a new warfighting domain. Cyberspace operations were thus seen as the natural fulfillment of the historic intent of airpower: to use technology to overcome the limitations of distance, terrain, and time in order to achieve strategic effects directly against otherwise unimpeachable enemy centers of gravity.

Cyberspace operations originated and initially matured within the Air Force signals intelligence and electronic warfare communities: the former was concerned with intelligence collection, and the latter with disrupting enemy air defense systems that were increasingly digital in nature. However, uncertainty as to how to properly manage both the cyberspace mission and the intelligence community that housed it led to a number of counterproductive reorganizations between 1995 and 2006. These reorganizations were rendered moot in 2005, when the bold declaration of a new Air Force mission statement set the precedent that cyberspace was a separate domain of warfare, and as such would need to be populated and managed by warfighters. The distinction of cyberspace as a warfighting domain foreshadowed a split between the cyberspace and intelligence communities. This split was hastened by the selection of 8AF as the first

patron of Air Force cyber command in 2006, and was solidified by the decision to transfer Air Force cyber capabilities to Space Command in 2008.

From 2008 to 2010, the Air Force deliberated over how to manage cyberspace personnel development. While the electronic warfare and intelligence communities provided initial input to the process, both eventually withdrew due to dissatisfaction with their relative standing in the final proposal. The communications community, eager to reverse years of downsizing, took advantage of the opportunity that resulted and offered to serve as the seedbed for the Air Force cyberspace population. In 2010, the Air Force established the first service cyber career field by renaming its communicators as cyberspace officers and adjusting training accordingly.

The period between 2006-2010 marked the first Air Force efforts to assimilate cyberspace into its dominant service culture. However, cultural dissimilarities between space and cyber, combined with cultural dissimilarities between communications and cyber, led to inefficient cyberspace development over the next decade. Many of the advances made by the provisional Air Force cyber command under 8AF were forgotten or undone as subsequent commanders fought for mission prioritization under a headquarters that culturally and operationally undervalued them. New training methods struggled to strike the right balance between the technical needs of cyberspace operations and the managerial needs of the routine network administration which most cyber officers would ultimately perform. The absorption of cyberspace into the dominant service culture beginning in 2006 brought an increase in resources and expectations, yet resulted in a noticeable friction as the domain's practitioners struggled to earn the operational reputation to which their career field designation entitled them. In the years since the creation of the 609 IWS, the Air Force has struggled to successfully operationalize the theoretical innovation that inspired its early embrace of the cyberspace domain.

Navy

In contrast to the Army and Air Force, cyberspace innovation in the Navy was not initially shaped by the interaction of peripheral subcultures, due largely to the fact that these peripheral subcultures did not exist in the same form as they did in the other services. For example, in spite of the historic importance of communications to naval operations, the Navy did not have a distinct officer communications community before the creation of the IP career designation in 2001. Similarly, it did not have a strong tradition of information operations prior to the semantic rebranding of the cryptologic community in 2005. Instead, Navy cyberspace innovation was driven by the interaction of a single subcommunity, cryptologists, with the dominant warfighting subcultures of service senior leadership. The singular influence of cryptologists within the Navy, combined with the service's uniquely close relationship with the national cryptologic enterprise, would come to play a defining role in the final shape of Navy cyberspace capability. In this sense, the Navy's decision to maintain a separate cryptologic career field had a substantial impact on the trajectory of its later cyberspace development.

The Navy first began to experiment with cyberspace operations and organizations in the late 1990s through an investment of signals intelligence personnel into select elements of the National Security Agency. This NSA partnership allowed the Navy to gain a level of operational proficiency in cyberspace in the early 2000s that was unmatched by the other military services. However, recommendations to create a separate cyberspace career field, organization, and warfare area in the mid-2000s were unable to gain institutional traction due to the implicit assumption that cyberspace ultimately belonged within the Navy tradition of cryptology, regardless of how little or how much of it comprised actual intelligence collection. Furthermore, fears of jeopardizing the Navy's relationship with the national intelligence enterprise limited the viability of any cyberspace innovation that afforded too much service independence.

As theories of cyberspace operations began to work their way up to senior Navy leadership, the idea of an independent cyberspace operational concept quickly grew subordinate to the need to tame the larger informational environment of which cyberspace was a part. Over the course of its integration with

the dominant service cultures, cyberspace was ultimately subsumed into a theory of information dominance that sought to address the communication challenges inherent to fleet-centric, maritime warfare. The model that the Navy eventually adopted for its cyberspace operations was not, therefore, driven by cyberspace itself, nor was it focused on optimizing activity in the cyberspace domain.[1257] In this sense, the information dominance theory that the Navy came to embrace for cyberspace can be seen as a contemporary answer to the long-time problem of information management in maritime warfare.

TRENDS AND IMPLICATIONS

Three trends are evident in the history so described. First, this dissertation demonstrates the doctrinal linkage between cyberspace operations and early theories of information warfare. More importantly, it helps to explain why cyberspace eventually overtook the information warfare concepts from which it emerged.[1258] While information warfare captured the services' imagination in the immediate aftermath of the Gulf War, the lack of a dedicated subcommunity in any of the services meant that the theory had to be implemented by personnel from mixed operational backgrounds. These personnel then filtered their interpretations of information warfare through the lens of their own operational experience — much of which was derived from the technically-oriented intelligence and communications communities. Under the influence of these communities, information operations became focused on technical network issues and on physical rather than cognitive effects. The idea of information as bits and bytes that could be attacked and degraded overtook the notion of information as intelligible content that could be manipulated to affect the end user.

[1257] Kohler, interview.

[1258] Interestingly, information warfare is now beginning to overtake cyberspace, at least in name and general inquiry. See Kimberly Underwood, "Army Cyber to Become and Information Warfare Command," Signal Magazine, March 14, 2019, https://www.afcea.org/content/army-cyber-become-information-warfare-command; Mark Pomerleau, "Is the U.S. Behind in Cyber-Enabled Info Operations?" Fifth Domain, November 27, 2017, https://www.fifthdomain.com/dod/2017/11/27/is-the-us-behind-in-cyber-enabled-info-operations/; and Mark Pomerleau, "Where Do Information Operations Fit in the DoD Cyber Enterprise? Fifth Domain, July 26, 2018, https://www.fifthdomain.com/c2-comms/2018/07/26/where-do-information-operations-fit-in-the-dod-cyber-enterprise/.

Later efforts to expand information operations into the realm of inform and influence ran aground when faced with service cultures that were more concerned with the visible and the quantifiably measurable. Recall from chapter 3, for example, that the information operations community in the Army became institutionally irrelevant when their doctrine shifted to "inform and influence" in the late 2000s. Even if members of that community had developed a theory of cyberspace that focused on its cognitive potential, the community's effective marginalization would have prevented any such theories from germinating. The initial cognitive motivations of information warfare were thus gradually supplanted by a preoccupation with the domain's potential to replace or augment kinetic weapon systems. The result was a cyber doctrine which focused on creating technical effects on discrete systems, and which neglected the epistemological possibilities of the broader information environment in which it was embedded. In short, the absence of a strong military subculture that could advocate for cyberspace's cognitive potential allowed the more technical interpretations to take over the process of innovation. Cyberspace then came to be seen as another weapon to add to the military arsenal rather than as something which could potentially change how interstate conflict was pursued.

This phenomenon offers an affirmation of the second point, which is the primary theoretical argument of this dissertation: that organizational culture matters to the study of innovation, and so too do the individual subcultures which comprise it. Subcultures will develop interpretations of a new idea based upon their operational experiences and predispositions. The different interpretations of competing subcultures will then interact to enact a defining influence on the process of military innovation. While similarity between subcultures can extend across service or organizational lines, the outcomes of the interactions among these service subcultures can have significant variation. One can see this mechanism at work in various inflection points that distinguished the trajectory of cyberspace operations in the Army, Navy, and Air Force. I will highlight three such points here.

First, while each of the services had cyberspace-focused units within their intelligence organizations in the early 2000s, the presence of a dedicated cryptologic career field in the Navy made a

decisive difference in the quality and quantity of cyberspace expertise that they were able to initially develop. Through its unique partnership with the National Security Agency, the Navy was able to establish itself as the undisputed service leader in national-level cyberspace operations until the mid-2000s. However, as cyberspace evolved into a more militaristic capability that required an expanded operational imagination, the other services, unconstrained by the presence of a strong cryptologic alternative, created a cyberspace infrastructure that was deliberately independent of their intelligence organizations. While the Navy's close ties to the national cryptologic enterprise initially vaulted them ahead of the other services when cyberspace was seen as an extension of signals intelligence collection, it later caused the service to lag behind as cyberspace evolved new military applications that demanded a new way of thinking.

A second cultural inflection point exists in the manner in which the Air Force created its cyberspace career field. Rather than carve out a home for cyberspace operations within its cryptologic community, as in the Navy, or create a new cyberspace community wholesale, as in the Army, the Air Force chose to nominally convert its 3,000 communications officers into cyberspace officers in 2010. However, the support predispositions ingrained within the communications culture persisted through its name and mission change. The resultant career field, comprised as it was of personnel who were accustomed to providing a support function that required comparatively little technical training, struggled to adapt to the operational realities of its new mission space. The counterintuitive result was that the service most historically welcoming of technological innovation has struggled to develop a cyberspace talent pool that befits its technological heritage.

Finally, the Army's approach to enlisted cyberspace personnel development offers a third example of the cultural logic described above, this time at the level of subcultural integration with the dominant service culture. The Army has been notably reluctant to overturn its traditional officer and enlisted paradigm — in which officers lead based on a generalist expertise while enlisted execute based on a technical specificity — in its approach to cyberspace. Specifically, the Army has maintained an insistence

that it can build out a sufficient body of enlisted technical experts to fill billets that the Air Force and Navy have proven more willing to fill with more highly educated officers. In this example, organizational interaction produced an outcome in which the norms of the dominant culture overrode the functionalist needs of the integrated subculture, to an effect which has yet to be determined. Army personnel management thus demonstrates the type of innovation outcome that our theoretical framework predicts: that competition among different ideas will be resolved in a way that aligns with the broader service mission and the dominant service culture.

However, while the outcome of subcultural interaction in each service varied depending on the type and scope of subcultural influence, the process resolved itself in a similar way when service senior leadership chose to intervene. The service case studies thus also affirm the second half of our hypothesis: that resolution of subcultural interaction will be determined by the dominant service culture. This involvement begins when clarity — or perceived clarity — about the nature of the innovation inspires increased senior leader attention to its process, which in turn has a centralizing effect on service innovation patterns.

At a broader level, the above history suggests a third trend: that military services will tend to create cyberspace capabilities that are relevant to their combat arms rather than those that explicitly answer to joint requirements. While this is an intuitive conclusion from the standpoint of organizational self-interest, it is noteworthy in two ways. Theoretically, it demonstrates that the inherent characteristics of a technology — its nature, as it were — is not enough to drive a uniform application of that technology cross-organizationally. Organizations will instead derive their own methods of employment that are shaped by their operational backgrounds, constrained by their cultures, and that tend to serve their interests. They are unlikely to deviate from this pattern in pursuit of a theoretical ideal.

The practical implications of this point are considerable given current discussions over the future of U.S. Cyber Command.[1259] It suggests, for one, that there are concrete operational consequences to the continued tethering of Cyber Command to the National Security Agency, and that these consequences will persist regardless of how explicitly the dual-hatted command tries to emphasize one mission or the other. Furthermore, it raises the question of whether relying upon the individual military services to pursue their own cyberspace capabilities will produce the most efficient wartime outcomes. In other words, is there some aspect of cyberspace's potential that the current arrangement has failed to exploit? The extent to which Cyber Command has struggled to come to terms with the relationship between information operations and cyberspace suggests that the answer to this question is yes.[1260] In this sense, it is not just the lack of a strong information operations subcommunity that should be reconsidered: it is the underlying theory of information that led to the conclusion such a community was not needed.

This potential for cyberspace to enable information operations, and the related difficulty with which the U.S. military establishment has embraced that potential, raises an additional important question: whether wartime outcomes are the most important measure of effectiveness for cyberspace innovation. The fact that cyberspace enables effects which are ephemeral and nonviolent has made it a compelling alternative to the overt use of force in matters of geopolitical tension. That it can be so readily used outside of a state of armed conflict has in turn contributed to the state of continuous low-level engagement which defines international cyber affairs.

In addition, cyberspace's diffusion of user-edited content has enabled a type of epistemological conflict in which reality is reshaped and accepted truths are subverted in pursuit of geopolitical goals. Attacks on military targets can thus become less alluring than attacks on the underlying legitimacy of

---

[1259] Conrad Crane, "The United States Needs an Information Warfare Command: A Historical Perspective," War on the Rocks, June 14, 2019, https://warontherocks.com/2019/06/the-united-states-needs-an-information-warfare-command-a-historical-examination/?fbclid=IwAR32ysjtg3NmO4UkHgmblHvFr3fOvOYsoPL0INR57HdzRQ6_IGs7rFYOEP0; Andrew Schoka, "Cyber Command, the NSA, and Operating in Cyberspace: Time to End the Dual Hat," War on the Rocks, April 3, 2019, https://warontherocks.com/2019/04/cyber-command-the-nsa-and-operating-in-cyberspace-time-to-end-the-dual-hat/; Michael Sulmeyer, "Much Ado About Nothing? Cyber Command and the NSA," War on the Rocks, July 19, 2017, https://warontherocks.com/2017/07/much-ado-about-nothing-cyber-command-and-the-nsa/.

[1260] Pomerleau, "Is the U.S. Behind?" and "Where do Information Operations Fit?"

political and societal institutions.[1261] In both contexts, one notices an ongoing shift of the battle ground from the realm of uniformed militaries engaging in armed conflict to the realm of ordinary civilians and the civic and political institutions they comprise. Taken together, this means that the most noteworthy attribute of cyberspace is also the one with which the U.S. military has most historically struggled: its potential for actuating a type of informational conflict that exists beyond ordinary land, air, and sea warfare. If the military will tend to create cyberspace capabilities that are most relevant to their combat arms, then these applications of cyberspace which lie outside the bounds of military conflict will risk going insufficiently explored.[1262]

ADDITIONAL CONSIDERATIONS

While the conclusions of this chapter rest upon a substantial body of historical evidence, there were a number of research limitations that deserved to be addressed. Most obviously, the research for this dissertation was limited to unclassified sources of data. Surprisingly, a substantial amount of the organizational and doctrinal history of cyberspace is, in fact, unclassified. I was therefore able to piece together the historical narrative of how the services created their cyber infrastructure with relative ease. That said, the majority of the work that this infrastructure performed — the actual cyberspace operations themselves — remains classified. As a result, I was not able to compare the effectiveness of different service reforms in a standardized or mathematically satisfying fashion. Any conclusions made in the preceding chapters about the effectiveness of different decisions rested instead upon the testimony of those I interviewed as well as the content and tone of public discourse.

[1261] This effort to erode the legitimacy of public institutions was the crux of the Russian cyber campaign that occurred in conjunction with their invasion of Georgia in 2008, as well as their ongoing efforts to target democratic elections in the U.S. and Europe.

[1262] It is important to note here that conceptual exploration can happen independently of practical application. In other words, identifying insufficient conceptual development as a weakness does not mean that the remedy is for the U.S. to engage in a type of subversive information warfare that might contradict foundational elements of American political culture. Instead, this dissertation argues that the conceptual limitations imposed by the U.S. cyber establishment's organizational trajectory could potentially limit its ability to understand — and thus counter — the alternative methods of cyberspace operation that are employed by nation-state adversaries.

A second, equally obvious limitation is the fact that the cyberspace story remains unfinished. In a sense, no innovation story is ever finished, since military organizations must continuously adjust their doctrine to new internal and external realities. That much is clear in the various doctrinal assessment mechanisms that the services have institutionalized. However, enough service reorganization took place over the course of writing this dissertation to suggest that the defense establishment continues to wrestle with the same questions that have plagued the development of cyberspace for the past thirty years: how might this change war, and how can we best position ourselves to take advantage of those changes.[1263] Interview responses echoed this same sentiment in overwhelming fashion.

While this unfinished state lends a tone of irresolution to any study of cyberspace innovation, the benefit is that it allows for the continued application of the theoretical framework to the services' new organizational decisions. How, for example, will the Air Force's recent decision to consolidate its 24th and 25th Air Forces into a single numbered air force underneath Air Combat Command affect its approach to cyberspace? How will the influence of maneuver culture affect the development of the Army's tactical cyber officers? Will the continued growth of Cyber Command create a transcendent cyber culture across the services that comprise it? The answers to these questions remain to be seen, yet they could provide additional insight into the relationship between operational backgrounds and innovation outcomes.

Importantly, this dissertation does not attempt to argue that culture is the only explanation for innovation outcomes, nor does it attempt to argue that culture acts singly or deterministically on the innovation process. On the contrary, the empirical history contained a number of factors beyond culture that helped drive cyberspace innovation. Observations of the external security environment, for example — with specific attention given to the activities of Russia in the Ukraine — contributed to the Army's push to emphasize cyberspace operations at the tactical level and to reinvigorate its electronic warfare

[1263] Since beginning this dissertation, 24 and 25 AF were moved underneath Air Combat Command and the Air Force announced that it would potentially merge these two organizations into a single numbered air force for information operations; the Army announced a tentative name change of Army Cyber Command into Army Information Warfare Command, implemented the first direct hire cyberspace officers, activated the I2CEWS, and announced the impending activation of the first Cyber Warfare Support Battalion; and the Navy changed the name of SPAWAR to NAVWAR (Navy Information Warfare Systems Command).

capabilities. Failure in the form of network intrusions also helped generate the sense of urgency necessary to enact sweeping organizational change at the joint level. The creation of JTF-CND in 1998 was largely a response to Solar Sunrise, while Buckshot Yankee had a similarly galvanizing effect on the creation of U.S. Cyber Command a decade later. Moreover, Russian digital disinformation campaigns have contributed to the current push to determine where information operations fit in the defense cyber enterprise.

However, these instances of failure and observation can tell an organization that it must adapt, but not how or to what end. Similarly, uncertainty about either the nature of an innovation or the strategic environment in which it sits can generate a sense of urgency to abandon old ways of doing things, but it cannot determine what should replace them. It is here that culture intervenes to shape the process. In helping organizations give meaning to the world around them, culture guides an organization's decisions when confronted with ambiguous threats or a changing security environment. Moreover, it affects this process more strongly at certain times than at others. Culture influences what possibility is pursued when there is more than one way of doing things, and it makes certain ways of doing things persist even when they appear to become less functionally or rationally efficient. While culture and subculture are not the sole forces of change, they can play a decisive role in the organizational learning process.

Both the cultural framework described above and the empirical history that tested it leave ample room for future research. Domestically, the history contained in this dissertation was not exhaustive: the U.S. Marine Corps and Coast Guard were excluded, as were the National Security Agency and the numerous joint cyber organizations that dotted the organizational landscape from 1998 to the present. These joint organizations offer a particularly compelling opportunity to study how subcultures interact across service lines, and of how service cultures interact in a joint framework. The theory of subcultural innovation would be additionally well-served by a cross-national study, in which the cyberspace infrastructure of different nation-states are evaluated by their organizational histories and the cultural

proclivities of their personnel. How, for example, did the theory of electronic struggle, and the organizations that embodied it, shape the nature of Russian cyberspace doctrine today? How has the unique culture of the Israeli intelligence establishment imprinted on the country's approach to cyberspace? What can we learn about the Chinese approach to cyberspace from the nature of the various organizations that have contributed to it? While cross-national comparisons will have data availability problems of their own, my suspicion is that, as with the U.S. case, the data will be there for those who desire to look for it.

Conclusion

While the existence of service cyber commands might tempt one to conclude that the innovation endstate across the services was the same, the empirical history demonstrates substantial variation in how the Army, Navy, and Air Force approached the problems of training, personnel, and organizational development, as well as the shape of the final cyberspace doctrine that each adopted. In spite of this variation in outcome, the process that led up to it was largely the same: the subcultural dynamics that drove innovation in the uncertain early years were eventually replaced by the influence of the dominant service culture. This influence, in turn, emerged when clarity about the nature of the innovation precipitated increased senior leader involvement. The development of cyberspace operations in the U.S. military services thus offers an affirmation of the hypotheses of this dissertation. In so doing, it argues that organizational culture matters, both in how we understand the process of innovation and in how we approach problems of innovation in the future. Innovation decisions are not always made based on the cost-maximizing matching of means with ends, but are often the product of ingrained and unconscious cultural influences.

This dissertation makes both a theoretical and an empirical contribution to the study of cyberspace and cyber conflict. Empirically, it provides a historical account of the development of cyberspace operations in the U.S. military services. In the process, it shows the relationship between

contemporary cyberspace operations and earlier notions of information warfare and command and control warfare. It also helps to explain why cyberspace doctrine ultimately diverged from, and then supplanted, its more cognitively-oriented predecessors.

Theoretically, the framework described above brings familiar arguments of organizational culture to the level of organizational subcultures to demonstrate the substantial and often constraining effect that these influences can have on the process of innovation. In so doing, it reminds policymakers and military leadership that it matters who has responsibility for the development of a new idea. It reminds academics to consider the composition of organizations as a variable in understanding why certain decisions are made and, equally, why certain opportunities are overlooked. And it reminds us that the nature of a new technology — the potential it possesses by virtue of what it is — is often not enough to drive its optimal employment in either war or peace.

Table 9. Timeline of Significant Events

Date	Joint	Army	Air Force	Navy
1990	First joint guidance on command and control warfare (C2W), JCS Memo of Policy No 30.			
1991	Gulf War I, "first information war."		Electronic Security Command becomes Air Force Intelligence Command (AFIC).	
1992	First guidance on information warfare, DoDD TS 3600.1.		AFDD-1 *Basic Doctrine*, describes importance of attacking C2 nodes.	Space and Electronic Warfare Commander billet created.
1993	JCS Memo of Policy No 30, "Command and Control Warfare" revised.		Air Force Electronic Warfare Center becomes Air Force Information Warfare Center (AFIWC); AFIC becomes Air Intelligence Agency.	
1994				Fleet Information Warfare Center (FIWC) and Naval Information Warfare Activity (NIWA) created.
1995		Army activates Land Information Warfare Activity (LIWA).	*Cornerstones of Information Warfare* released; 609 Information Warfare Squadron activated.	
1996	First doctrine on command and control warfare, JP 3-13.1. DoDD S-3600.1 replaces information warfare with information operations. Joint Vision 2010 describes future info environment.	FM 100-6 *Information Operations* released. FSTs deploy to Bosnia.		
1997	Eligible Receiver demonstrates network vulnerabilities.		AFDD-1 updated to include information warfare.	IT-21 initiative to update Navy networks.
1998	Solar Sunrise, Moonlight Maze intrusions. JTF Computer Network Defense created, assigned to USSPACECOM. JP 3-13.1 *Information Operations* introduces computer network attack.	B/742nd MI BN, 704th MI BDE tasked with computer network operations.	AFDD 2-5 *Information Operations* defines information warfare.	Cebrowski introduces the concept of Network-Centric Warfare. Winsor Whiton begins cryptologist investment in the NSA.
1999		Army creates IO functional area.	609 IWS disbanded, capabilities moved to 67th Intelligence Group. Intel units become IO units.	Navy creates IT rating, Navy Component Task Force for Computer Network Defense (NCTF-CND).

Table 9. Timeline of Significant Events (Continued)

Date	Joint	Army	Air Force	Navy
2000	JTF-CND becomes JTF-Computer Network Operations, responsible for computer network attack.	B/742nd becomes Detachment Meade.	Air Force activates 67th Information Operations Wing and 70th Intelligence Wing to focus on IO.	NMCI initiative overhauls Navy networks.
2001	Space and Information Operations Element (SIOE) created to provide IO support to Global War on Terror.		AIA moves to Air Combat Command due to growth of IO mission.	Information Professional Community and Naval Network Warfare Command (NETWARCOM) created.
2002	SPACECOM merges with STRATCOM, takes responsibility for cyberspace ops.	LIWA becomes 1st Information Operations Command.		Information Operations established as a primary warfighting area.
2003	Information Operations Roadmap released. SIOE becomes Information Operations Task Force (IOTF).	FM 3-13 *Information Operations* introduces computer network operations to Army doctrine.	AFDD 1 updated to include IO as one of 17 functions of air power, information superiority as one of six core competencies. Describes network warfare as a component of IO.	Enlisted EW techs merge with cryptologic CTT rating. FIWC merges with Naval Component Task Force Computer Network Defense (NCTF-CND). CTN rating established.
2004	JTF -CNO becomes JTF-Global Network Operations. Joint Functional Component Command Network Warfare (JFCC-NW) created under STRATCOM for offense.			
2005		IED Task Force concludes that the Army needs electronic warfare (EW) capability.	Air Force adds cyberspace to mission statement, updates AFDD 2-5 to affirm IO as integral to all Air Force operations	NETWARCOM merges with NAVSECGRU; NSGAs renamed NIOCs; cryptology renamed IW. IT and CTO ratings merge.
2006	JP 3-13 describes computer network operations as a core component of IO.		Chief orders plan for career field. 67th IO becomes 67th Network Warfare Wing. AFWIC becomes AFIOC. ARCYBER (P) created under 8AF. Absorbs 67th NWW and AFIOC.	Navy creates Navy Cyber Attack Teams, Navy Cyberspace Defense Operations Command (NCDOC).
2007	Cyber attacks on Estonia. Operation Orchard enables Israeli attack on Syrian nuclear site.	Det Meade becomes Army Network Warfare Detachment. Army Chief directs embrace of EW.	AIA becomes AFISRA. Undergraduate Network Warfare Training created. Nuclear incident.	SSG XXVI recommends creation of cyberspace career field, warfare area.
2008	Buckshot Yankee network intrusion. JFCC-NW takes operational control of JTF-GNO. Russia invades Georgia, engages in cyber attacks.	FM 3-0 update includes cyberspace. ANWD becomes CNO-TF, Army Network Warfare Battalion. SMDC/ARSTRAT interim HQ for cyber.	*Air Force Roadmap for the Development of Cyberspace Professionals* outlines strategy for cyberspace personnel. Schlesinger Report causes significant reorganization.	

Table 9. Timeline of Significant Events (Continued)

Date	Joint	Army	Air Force	Navy
2009	US Cyber Command created.	FM 3-36 *Electronic Warfare* released. ANWB becomes 744th MI BN. ARFORCYBER created to C2 cyberspace operations. Electronic Warfare branch approved.	AFCYBER (P) becomes 24th Air Force under Air Force Space Command. AFIOC becomes 688th IO Wing. Communications becomes cyber career field.	NCATs disbanded. N2 and N6 merge to create N2N6
2010	Joint Cyber Analysis Attack Course (JCAC) created.	ARCYBER established. Signal Corps creates 255S. C/EW CBA released.	AFDD 3-12 *Cyberspace Operations* released. AFDD 1 updated to add cyberspace superiority as one of 12 core functions.	Navy establishes Fleet Cyber Command, Information Dominance Community, Cyber Warfare Engineer.
2011		744th MI BN becomes 780th MI BDE (Cyber).		NIOC Suitland becomes Naval Cyber Warfare Development Group.
2012		Budget cuts elimate EW billets. 35Q MOS created. Army Cyber Center established at West Point, later renamed Army Cyber Institute.		
2013		FM 3-13 *Inform and Influence Activities* replaces IO. Cyber CBA completed.	688th IO Wing becomes 688th Cyberspace Wing.	Naval Academy creates Cyber Science major.
2014	USCYBERCOM activates Cyber National Mission Force.	Army creates Cyber Branch, Cyber Center of Excellence, 25D MOS. Cyber Support to Corps and Below begins.	AFISRA becomes 25th Air Force.	
2015		EW absorbed by cyber branch. Tool Developer Qualification Course begins.		
2016	Joint Task Force Ares created to counter ISIS cyber activity.			Information Dominance Community renamed Information Warfare Community. Information Warfare officers renamed Cryptologic Warfare.
2017		Army creates Basic Cyber Operator and FM 3-12, *Cyberspace Operations.*		
2018	USCYBERCOM elevated to combatant command.		24 and 25 AF move under Air Combat Command.	
2019		First I2CEWS activated, creation of 915 Cyber Warfare Support Battalion approved. Potential change of ARCYBER to Army Information Warfare Command announced.	24 and 25 AF to merge into single numbered air force.	

Bibliography

"17C Cyber Operations Specialist." Powerpoint briefing. June 2, 2015.

"18-03 Integration of CEMA to Deliver Effects." Powerpoint briefing. No date.

"18-03 Integration of Cyber and OSINT to Deliver Effects." Powerpoint briefing. No date.

"1st IO Command (Land) History — Information Paper." Information paper. May 7, 2014

"Aeronautical Division, U.S. Army Signal Corps." NGA.mil. Accessed August 9, 2018. https://www.nga.mil/About/History/NGAinHistory/Pages/AeronauticalDivision,USArmySignalCorps.aspx.

"AFCYBER Activities and Initiatives." September 2007. Provided via email by Robert J. Elder, August 2018.

"AFSC 17X Cyberspace Operations Officer Career Field Education and Training Plan." Headquarters, U.S. Air Force. June 1, 2015. https://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/cfetp17x/cfetp17x.pdf

"Air Combat Command History." ACC.af.mil. Last updated February 10, 2017. https://www.acc.af.mil/About-Us/ACC-History/.

"Air Command Announces 24 and 25 AF Merger." ACC.af.mil. April 4, 2019. https://www.acc.af.mil/News/Article-Display/Article/1805297/air-combat-command-announces-24-and-25-af-merger/.

"Air Force Communications Command." Air Force Historical Research Agency. January 10, 2009. https://www.afhra.af.mil/About-Us/Fact-Sheets/Display/Article/433902/air-force-communications-command/.

"Air Force Global Command Fact Sheet." AF.mil. November 20, 2015. https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104462/air-force-global-strike-command/.

Air Force Personnel Center. "Air Force Officer Classification Directory (AFOCD): The Official Guide to Air Force Officer Classification Codes." Air Force Personnel Center. April 30, 2018.

"Air Force Space Command History." AFSPC.af.mil. Accessed June 29, 2018. https://www.afspc.af.mil/About-Us/AFSPC-History/.

"Air Force Strategic Plan 2006-2008." AU.af.mil. October 5, 2006. http://www.au.af.mil/au/awc/awcgate/af/af_strat_plan_06-08.prf

"Air Force Transfers Cyber Responsibility to ACC." AF.mil. June 7, 2018. https://www.af.mil/News/Article-Display/Article/1544072/air-force-transfers-cyber-responsibility-to-acc/.

"Air Intelligence Agency to Become Air Force ISR Agency." AF.mil. May 15, 2007. https://www.af.mil/News/Article-Display/Article/126859/air-intelligence-agency-to-become-air-force-isr-agency/.

Alexander, Keith R. Interview by Sarah White. In person. Fulton, Maryland. September 24, 2018.

Allison, Graham and Philip Zelikow. *Essence of Decision: Explaining the Cuban Missile Crisis (2nd Edition)*. New York: Longman, 1999.

"An/MLQ-40 Prophet." Globalsecurity.org. Accessed March 12, 2018. https://www.globalsecurity.org/intell/systems/prophet.htm.

Anderson, Scott. "The History of the U.S. Army Cyber School and Branch." U.S. Army Cyber School and Branch Historian. Powerpoint presentation. No date.

Anderson, Scott. Army Cyber Chronology. No date.

Anderson, Steven J. "Airpower Lessons for an Air Force Cyber-Power Targeting Theory." Maxwell Air Force Base, AL: Air University Press, 2016.

Annex 3-04 Countersea Operations. "The Navy Composite Warfare Commander." Curtis E. LeMay Center for Doctrine Development and Education. November 7, 2014.

Annex 3-13: Information Operations. Maxwell Air Force Base, AL: Curtis E. LeMay Center for Doctrine Development and Education. April 28, 2013.

Annex 3-51 Electronic Warfare. Maxwell Air Force Base: Curtis E. LeMay Center for Doctrine Development and Education. October 10, 2014.

Arguero, Bob. Editor. "Air Intelligence Agency and Air Combat Command to Merge." GovCon. Accessed June 28, 2018. https://www.govcon.com/doc/air-intelligence-agency-and-air-combat-comman-0001.
.

Armstrong, James R. Email message to the author. March 13, 2018.

"Army Creates Electronic Warfare Career Field." Defense-Aerospace.com. February 6, 2009. http://www.defense-aerospace.com/articles-view/release/3/102144/us-army-re_establishes-electronic-warfare-career-field.html.

"Army Cryptologic Operations." INSCOM.army.mil. Last updated May 2, 2019. https://www.inscom.army.mil/MSC/ACO.aspx.

"Army Cyber Career Field Implementation IPR to CAC CG." Powerpoint briefing. Fort Leavenworth, Kansas. Sep 12, 2014.

"Army Cyber Command DOTMLPF-P Assessment of CEMA Support to Corps and Below (CSCB) and Techniques to Integrate Cyberspace Electromagnetic Activities (CEMA) into Division and Brigade Combat Team Operations." Draft manual. Shared with the author via email by Lieutenant Colonel Wayne Sanders January 31, 2018.

Army Cyber Command/2nd Army Leavenworth Support Element. "Army Cyberspace Operations Capabilities Based Assessment (Cyber CBA) Executive Summary." Fort Leavenworth, KS. July 1, 2013.

Arnold, Todd, Rob Harrison, and Gregory Conti. "Professionalizing the Army's Cyber Officer Force." *Army Cyber Center* Vol 1337 No II (November 23, 2013).

____. "Towards a Career Path in Cyberspace Operations for Army Officers." Small Wars Journal. August 18, 2014.

Association of the United States Army. "AUSA Cyber Hot Topic 2018, Panel 3: Cyber Support to Corps and Below." Filmed August 2, 2018. YouTube video, 1:15.23. Posted August 6, 2018. https://www.youtube.com/watch?v=ccjt7gCjnV0.

Avant, Deborah D. "From Mercenary to Citizen Armies: Explaining Change in the Practice of War." *International Organization* 54, 1 (Winter 2000): 41-72.

____. *Political Institutions and Military Change: Lessons From Peripheral Wars.* Ithaca: Cornell University Press, 1994.

Barnes, Julian E. and Peter Spiegel. "Air Force Ads' Intent Questioned." *Los Angeles Times*, March 30, 2008. https://www.latimes.com/archives/la-xpm-2008-mar-30-na-airforce30-story.html.

Barrett, Danielle. "Developing a Community of C4IW Professionals." *Proceedings* Issue 126 (June 2000). https://www.usni.org/magazines/proceedings/2000-06/developing-community-c4iw-professionals.

Beach, Matthew G. "Managing Cyber Operator Training Curriculum." Thesis, Air University, 2010.

Bebber, Robert. "Cryptology at a Crossroads." *Proceedings* Issue 141 (March 2015). https://www.usni.org/magazines/proceedings/2015-03/cryptology-crossroads.

Bednar, Jenna and Scott E. Page. "Culture, Institutional Performance, and Path Dependence." *UC Berkeley: Institute of Governmental Studies.* February 2, 2006. https://escholarship.org/uc/item 1bq6d126#author.

Bennett, Lisa C. Interview by Sarah White. Phone call. Fort Montgomery, New York. October 23, 2018.

Biermann, R.J. "24th Air Force Joins Air Combat Command, Welcomes New Commander." AF.mil, July 18, 2018. https://www.af.mil/News/Article-Display/Article/1577754/ 24th-air-force-joins-air-combat-command-welcomes-new-commander/.

Bigelow, Michael E. "A Short History of Army Intelligence." https://fas.org/irp/agency/army/short.pdf.

Blackwell, Paul E., Trent N. Thomas, Paul E. Menoher, and Otto J. Guenther. Memorandum of Understanding Among Deputy Chief of Staff for Operations and Plans and Deputy Chief of Staff for Intelligence and Director of Information Systems for Command, Control, Communications, and Computers and Commander U.S. Army Intelligence and Securities Command. "The U.S. Army Intelligence and Security Command's Land Information Warfare Activity." March 24, 1995.

Boland, Rita. “Military Branch Undertakes Massive Troop Conversion.” Signal Magazine, February 2, 2010. https://www.afcea.org/content/?q=node/2196.

Bolger, Daniel P. Memorandum for Commander, U.S. Army Intelligence and Security Command. “Concept Plan to Establish United States Army Intelligence and Security Command (USAINSCOM) Cyber Brigade." December 9, 2010.

Bond, Alex. Interview by Sarah White. Phone call. Fort Montgomery, New York. August 19, 2018.

Boslaugh, David L. *First-Hand: No Damned Computer is Going to Tell Me What to Do — the Story of the Navy Tactical Data System.* Engineering and Technology History Wiki. Updated August 2017. https://ethw.org/First-Hand-No_Damned_Computer_is_Going-to_Tell-Me-What_to_DO_-_The_Story_of_the_Naval_Tactical_Data_System_NTDS.

____. *When Computers Went to Sea: The Digitization of the United States Navy.* Los Alamitos: IEEE Computer Society, 1999.

Boudreau, Todd M. “Army Training Infrastructure for Career Field 17 Training.” Information paper. Fort Gordon, GA, December 21, 2015.

____. “Career Field/Branch 17 Development Update.” Information paper. Fort Gordon, GA. June 12, 2014.

____. “Cyber Branch/Career Field Implementation.” Information paper. Fort Gordon, GA. October 3, 2014.

____. “Cyber CoE and Intel CoE Home on Home (HoH) Task Update: CF29 Infusion into Cyber Branch.” Information paper. Fort Gordon, GA. January 12, 2016.

____. “Cyber CoE and Intel CoE Home on Home (HoH) Task Update.” Information paper. Fort Gordon, GA. January 7, 2016.

____. “Cyber Instructor Strategy.” Information paper. Fort Gordon, GA. January 8, 2015.

____. “U.S. Army Cyber School Functional Courses.” Information paper. Fort Gordon, GA. January 10, 2017.

____. “U.S. Army Cyber School Training Courses Construct.” Information paper. Fort Gordon, GA. January 10, 2017.

____. Cyber-Electromagnetic (CEM) Career Field/Branch Development Update. Information paper. Fort Gordon, GA. April 30, 2014.

____. U.S. Army Cyber School Cyber Center of Excellence. Powerpoint briefing. Fort Gordon, GA. January 15, 2017.

Bova, Shawn D. Interview by Sarah White. Phone call. Fort Montgomery, New York. December 7, 2018.

Bowman, Wendell W. “Electronics in Air War.” *Air University Quarterly* Vol 3 No 1 (Summer 1949): 48-57.

Branch, Austin. Interview by Sarah White. Phone call. Fort Montgomery, New York. November 9, 2018.

Branch, John D. Interview by Sarah White. Phone call. Fort Montgomery, New York. October 19, 2018.

Branch, Ted. NAVADMIN 023/16. "Information Dominance Corps Redesignated Information Warfare Community." February 2, 2016.

Brauner, Marygail K., Hugh G. Massey, S. Craig Moore, and Darren D. Medlin. "Improving Development and Utilization of U.S. Air Force Intelligence Officers." Santa Monica, CA: RAND Corporation, 2009.

Brooks, Sandra. Interview by Sarah White. Phone call. Fort Montgomery, New York. January 16, 2019.

Brown, Michael D. Interview by Sarah White. Phone call. Fort Montgomery, New York. January 3, 2019.

Brunninge, Olof. "Imprinting and Organizational Path Dependence: Studying Similarities, Differences and Connections Between Two Concepts Along the Case of a Large Swedish Bank." 2011. https://www.wiwiss.fu-berlin.de/forschung/pfadkolleg/Archiv/_NEU_Veranstaltungen/konferenzen/download_center_2011/papers/Brunninge_Olof.pdf.

Bryant, Susan and Heidi A. Urben. "Reconnecting Athens and Sparta: A Review of OPMS XXI at 20 Years." *The Land Warfare Papers* No. 114 (October 2017).

Buckhout, Laurie M. "Short History of U.S. Army Electronic Warfare." *SITREP Review of DoD Technology Advancements* (Q1 2016). http://www.leonardodrs.com/sitrup/q1-2016-the-invisible-fight/short-history-of-us-army-electronic-warfare/.

Buckner, Jennifer G. Interview by Sarah White. Phone call. Fort Montgomery, New York. December 7, 2018.

Builder, Carl. *The Masks of War: American Military Styles in Strategy and Analysis.* Baltimore: Johns Hopkins University Press, 1989.

Burke, R.P. NAVADMIN 177/16. "Change to the Cyber Warrant Officer Commissioning Program." August 10, 2016.

Camacho, Michelle. Text correspondence with the author. February 2018.

Card, Kendall L. OPNAV Instruction 1412.15. "Information Dominance Corps Command Qualification Program." December 3, 2012.

____. "Information Dominance and the U.S. Navy's Cyber Warfare Vision." Powerpoint briefing. April 16, 2010.

Cate, James L. "Development of Air Force Doctrine 1917-1941." *Air University Quarterly Review.* Vol 1 No 3 (Winter 1947).

Cebrowski, Arthur K. and John H. Garstka. "Network-Centric Warfare: Its Origin and Future." *Proceedings* Issue 124 (January 1998).

Chairman of the Joint Chiefs of Staff. Chairman of the Joint Chiefs of Staff Instruction 3210.03. "Joint Command and Control Warfare Policy." March 31, 1996.

____. Chairman of the Joint Chiefs of Staff Memorandum of Policy 30. "Command and Control Warfare." Issued 17 July 1990, 1st Revision 8 March 1993.

Chapman, Robert M. "Technology, Airpower, and the Modern Theater Battlefield." *Air Power Journal* Vol 2 No 2 (Fall 1988): 42-52.

Chavez, Abel. Interview by Sarah White. Phone call. Fort Montgomery, New York. September 13, 2018.

Chezem, John. "Air Force Cyber Mission Success Depends on Cultural Change." Signal Magazine, October 1, 2015. https://www.afcea.org/content/?q=Article-air-force-cyber-mission-success-depends-cultural-change.

Cicalese, Carmine. Interview by Sarah White. Phone call. Fort Montgomery, New York. October 18, 2018.

Clark, Colin. "Air Force Mulls Merging Cyber, ISR Troops." *Breaking Defense*, September 20, 2017. https://breakingdefense.com/2017/09/air-force-mulls-merging-cyber-isr-troops/.

Clark, Joseph Roger. "Innovation Under Fire: Politics, Learning, and U.S. Army Doctrine." PhD Dissertation, George Washington University, 2011.

Clemins, Archie. "It's More Than E-mail." *Proceedings* Issue 126 (February 2000).

Clothier, Dean C. "Cyberspace Weapon System Briefing." Script for the AFSCP CC Conference. 27 April 2011. Received via email from Lieutenant Colonel (R) Dean C. Clothier, September 12, 2018.

____. "Cyber Weapon Systems." Slides 2 and 7. Powerpoint briefing, April 20, 2011. Received via email from Lieutenant Colonel (R) Dean C. Clothier, September 12, 2018.

____. Interview by Sarah White. Phone call. Fort Montgomery, New York. April 11, 2018.

____. Interview by Sarah White. Phone call. Fort Montgomery, New York. September 11, 2018.

Cohen, William. "Report of the Quadrennial Defense Review." *Joint Forces Quarterly* (Summer 1997): 8-14.

Combined Arms Center, Capability Development Integration Directorate. "Army Cyber/Electromagnetic Contest Capabilities Based Assessment (C/EM CBA) Final Report." Fort Leavenworth, KS. March 30, 2011.

"Comments and Discussion." *Proceedings* Issue 122 (November 1996).

"Concept of Cyber Warfare." Eighth Air Force Operational Concept. June 1, 2007. Received from Lieutenant General (R) Bob Elder via email, August 9, 2018.

Connell, Michael and Sarah Vogler. "Russia's Approach to Cyber Warfare." *CNA Occasional Paper Series* (2017). https://www.cna.org/CNA_files/PDF/DOP-2016-U-014231-1Rev.pdf.

Conti, Gregory and David Raymond. *On Cyber: Towards an Operational Art for Cyber Conflict.* Kopidion Press, 2017.

Conti, Gregory and Jen Easterly. "Recruiting, Development, and Retention of Cyber Warriors Despite an Inhospitable Culture." *Small Wars Journal*, 2010. https://smallwarsjournal.com/jrnl/art/recruiting-development-and-retention-of-cyber-warriors-despite-an-inhospitable-culture.

Conti, Gregory J. and John R. Surdu. "Army, Navy, Air Force, and Cyber — Is it Time for a Cyberwarfare Branch of the Military?" *IA Newsletter.* Vol 12 No 1. (Spring 2009): 14-18.

Conti, Gregory J. Interview by Sarah White. Phone call. Fort Montgomery, New York. October 19, 2018.

Conti, Gregory J., John Nelson, Jacob Cox, and Jon Brickey. "The Case for Cyber." *Small Wars Journal*, 2012. https://smallwarsjournal.com/jrnl/art/the-case-for-cyber.

Convertino, Mike, Lou Anne DeMattei, and Tammy Knierim. "Flying and Fighting in Cyberspace." Thesis, Air University, February 23, 2007.

"Cornerstones of Information Warfare." Air Force White Paper. 1995.

Corrin, Amber and Mark Pomerleau. "Army Merging Electronic Warfare into New Cyber Directorate." C4ISRnet, July 12, 2016. https://www.c4isrnet.com/c2-comms/2016/07/12/army-merging-electronic-warfare-into-new-cyber-directorate/.

Crane, Conrad. "The United States Needs an Information Warfare Command: A Historical Perspective." War on the Rocks, June 14, 2019. http://warontherocks.com/2019/06/the-united-states-needs-an-information-warfare-command-a-historical-examination/?fbclid=IwAR32ysjtg3NmO4UkHgmblHvFr3fOvOysoPL0INR57HdzRQ6_IGs7rFYOEP0.

"Cryptologic Technician-Technical." Navy Personnel Command. Accessed January 18, 2019. https://www.public.navy.mil/bupers-npc/enlisted/community/crypto_it/Pages/CTT.aspx.

"Cyber Center of Excellence (Provisional): Offsite #2." Powerpoint briefing. March 24, 2014.

"Cyber School Course Overview." Powerpoint briefing. Fort Gordon, GA. No date.

Cyber Technical College. "Cyber School Course Descriptions." Fort Gordon, GA. September 15, 2016.

"Cyberspace Career Field CSA Briefing, Draft, Pre-Decisional." Powerpoint briefing. August 12, 2008. Received via email from William J. Thompkins, October 5, 2018.

Daly, John C.K. "U.S. Air Force Prepares for Cyber War." Space Daily, October 9, 2006.

Daugherty, Lindsay, Laura Werber, Kristy N. Kamarck, Lisa M. Harrington, and James Gazis. "Officer Accession Planning: A Manual for Estimating Air Force Officer Degree Requirements." Santa Monica, CA: RAND Corporation, 2016.

Davidson, Janine. *Lifting the Fog of Peace: How Americans Learned to Fight Modern* War. Ann Arbor: The University of Michigan Press, 2010.

Davis, John A. Interview by Sarah White. Phone call. Yorktown, New York. November 29, 2018.

Debban, Alan W. "Disabling Systems: War-fighting Option for the Future." *Air Power Journal* Vol 7 No 1 (Spring 1993): 44-52.

Deets, Edward H. Interview by Sarah White. Phone call. Fort Montgomery, New York. January 8, 2019.

Demspey, Martin E. Memorandum for General Peter W. Chiarelli. "Posturing the Army for Cyber, EW, and IO as Dimensions of Full Spectrum Operations." October 16, 2009.

Department of the Air Force. "The Air Force Roadmap for the Development of Cyberspace Professionals 2008-2018." Washington, DC: HQ USAF/A30-CF. April 15, 2008.

Department of Defense Directive S-3600.1. "Information Operations." December 9, 1996. http://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Other/14-F0492_doc_02_Directive_S-3600-1.pdf.

Department of Defense Directive TS-3600.1. "Information Warfare." December 21, 1992.

Department of Defense. *Joint Publication 1-02 Department of Defense Dictionary of Military and Associated Terms*. Washington D.C.: Department of Defense. February 15, 2016.

____. *Joint Publication 3-12 (R) Cyberspace Operations.* Washington, D.C.: Department of Defense. February 5, 2013.

____. *Joint Publication 3-13.1 Electronic Warfare.* Washington D.C.: Department of Defense. January 25, 2007.

____. *Joint Publication 3-13.1: Electronic Warfare*. Washington, D.C.: Department of Defense, 2007.

Department of the Army Memorandum. "Addendum 1 to Army Structure (ARSTRUC) Memorandum 2020-2024, Dated 08 December 2017." April 3, 2018.

Dickstein, Corey. "Army Launches Direct Commissioning Program for Civilian Cybersecurity Experts." *Stars and Stripes,* December 5, 2017.

Dima Adamsky. *The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel.* California: Stanford University Press, 2010.

"DoD/Army Cyber: Authorities, Roles, and Responsibilities." Powerpoint briefing by the JAG Corps to the CSA Cyber Summit. July 14, 2012.

Dominique, Michael. Interview by Sarah White. Phone call. Fort Montgomery, New York. November 13, 2018.

Donnithorne, Jeffrey. *Culture Wars: Air Force Culture and Civil-Military Relations.* Maxwell Air Force Base, AL: Air University Press, 2013.

Dorsett, David J. "IDC Officer Community Consolidation 18XX Memo." February 10, 2019.

____. "Memorandum for the Information Dominance Corps." DCNO Update. April 2, 2010.

____. "Memorandum for the Information Dominance Corps." DCNO Update. November 2, 2009.

____. "Navy Intelligence and Information Dominance Discussions, 2006-2010." Personal notes. Sent to the author via email, January 12, 2019.

____. "NIP Information Dominance Presentation." Briefing. October 16, 2009.

____. "Note from the DCNO for Information Dominance." October 21, 2010.

____. "The U.S. Navy's Vision for Information Dominance." May 26, 2010.

____. Interview by Sarah White. Phone call. Fort Montgomery, New York. January 12, 2019.

____. NAVADMIN 062/11. "Enlisted Information Dominance Warfare Specialist Program." February 23, 2011.

____. NAVADMIN 314/10. "Enlisted Information Dominance Warfare Specialist Program." September 20, 2010.

____. NAVADMIN 328/10. "Information Dominance Warfare Officer Program." October 1, 2010.

____. "The Information Dominance Corps: What Does it Mean to Me?" Note From the DCNO for Information Dominance. June 14, 2010.

Dougherty, William A. "Storm from Space." *Proceedings* Issue 118 (August 1992).

Doughty, Robert. *The Evolution of U.S. Army Tactical Doctrine, 1946-1976.* Leavenworth, KS: Combat Studies Institute, 1979.

Douhet, Giulio. *The Command of the Air.* New York: Coward-McCann, 1942.

Downey, Gabriel R. Interview by Sarah White. Phone call. Fort Montgomery, New York. November 9, 2018.

Drezner, S.M. *The Computer Resources Management Study.* Santa Monica: Rand, 1976.

Dunlop, Matthew. Interview by Sarah White. Phone call. Fort Montgomery, New York. August 15, 2018.

Durante, Massimo. "Violence, Just Cyber War, and Information." *Philosophy and Technology* 28 (2015): 369-385.

Dyson, George. *Turing's Cathedral: The Origins of the Digital Universe.* New York: Vintage Books, 2012.

Easterly, Jen. Interview by Sarah White. Phone call. Fort Montgomery, New York. November 6, 2018.

"Eighth Air Force Fact Sheet." Air Force Historical Research Agency. February 19, 2019. https://www.afhra.af.mil/About-Us/Fact-Sheets/Display/Article/432272/eighth-ari-force-air-forces-strategic-acc/.

Elder, Robert J. "Cyberspace Paper for COMACC." No Date. Received via email from Lieutenant General (R) Robert J. Elder, August 9, 2018.

____. Interview by Sarah White. Phone call. Fort Montgomery, New York. August 9, 2018.

____. Memorandum to Commander, Air Combat Command, 28 December 2007. "Operational Cyberspace Command "Go Do" Letter, One-year Report."

Emmersen, Tracy, Joseph M. Hatfield, Jeff Kosseff, Stephen R. Orr IV. "The U.S. Naval Academy's Interdisciplinary Approach to Cyber Security Operations." *Computer* 52:3 (March 2019): 48-57.

"Enlisted Rating Insignia." Navy.mil. Updated June 28, 2009. https://www.navy.mil/navydata/nav_legacy.asp?id=262.

Fanning, Eric K. General Order No. 2016-11. "Designation of United States Army Cyber Command as an Army Service Component Command." Headquarters, Department of the Army. July 11, 2016.

Fastabend, David, Jeff Becker, and Greg Gardner. "Mad Scientist: The 2050 Cyber Army." Conference final report. November 7, 2016.

Fehrenbach, T.R. *This Kind of War: The Classic Korean War History,* 50th anniversary edition. Dulles, VA: Potomac Books, 2001.

Ferguson, Mark. NAVADMIN 058/10. "Information Dominance Corps Warfare Insignia." February 19, 2010.

____. NAVADMIN 139/10. "Establishment of the Cyber Warrant Officer Community." April 20, 2010.

____. NAVADMIN 205/10. "Establishment of the Cyber Warfare Engineer Designator." June 21, 2010.

____. NAVADMIN 206/10. "Information Dominance Corps Officer Designator Alignment." June 22, 2010.

Fischerkeller, Michael P. and Richard Harknett. "Deterrence is Not a Credible Strategy for Cyberspace." *Orbis* Vol 61(3) (2017): 381-393.

Fitzgerald, James R. Raymond J. Christian, Robert C. Manke. "Network-Centric Antisubmarine Warfare." *Proceedings* Issue 124 (September 1998).

Fogarty, Stephen G. "Cyber Career Field Implementation Plan (CMF 17 SME Panel & Way Ahead)." Powerpoint briefing. Fort Gordon, GA. September 25, 2014.

____. "Cyber Center of Excellence (Cyber CoE)." Powerpoint briefing. AFCEA TechNet, September 10, 2014. https://www.afcea.org/events/augusta/14/documents/FogertyAFCEAv10.pdf.

Fort Gordon Public Affairs Office. "Army Cyber Branch Offers Soldiers New Challenges, Opportunities." Army.mil. November 24, 2014. https://www.army.mil/article/138883/army_cyber_branch_offers_soldiers_new_challenges_opportunities.

Fox, Mike. "Growing the Army's Cyber Warriors." Powerpoint briefing. SMDC/ARSTRAT Training Conference. September 14, 2010.

Franz, George J. III. Email correspondence with the author. August 12, 2018.

____. "Information — the Fifth Element of Combat Power." Thesis, School of Advanced Military Studies, U.S. Army Command and General Staff College, Fort Leavenworth, KS. May 23, 1996.

Franz, Timothy P., Matthew F. Durkin, Paul D. Williams, Richard A. Raines, and Robert F. Mills. "Defining Information Operations Forces: What Do We Need?" Air and Space Power Journal, Vol 21 No 2 (Summer 2007): 53-67.

Fredericks, Brian. "Information Warfare: The Organizational Dimension." Thesis, U.S. Army War College, Carlisle Barracks, PA. February 7, 1996.

Freedberg Jr., Sydney J. "Cyber Course Fights Training Shortfalls: NSA, IONs, and RIOT." Breaking Defense, September 27, 2018. https://breakingdefense.com/2018/09/cyber-force-fights-training shortfalls-na-ions-riotfbclid=IwAR29KvAgtVtQlk5ob1pL2sauYFr21gVHcn3QU_55mFT1Gy5vXTB_V5VYS5k.

____. "Electronic Warfare Trumps Cyber for Deterring Russia." Breaking Defense, February 1, 2018. https://breakingdefense.com/2018/02/electronic-warfare-trumps-cyber-for-deterring-russia/.

Friedman, Norman. *Network-Centric Warfare: How Navies Learned to Fight Smarter Through Three World Wars.* Annapolis: Naval Institute Press, 2009.

Fuentes, Eckstein. "Navy Information Warfare Effort Set to Expand, Evolve." *Navy Times*, February 7, 2018.

G3 Network Warfare Directorate. "G3 Network Warfare Directorate Brief." Powerpoint briefing. February 13, 2013.

Galway, Lionel A.. Richard J. Buddin, Michael R. Thirtle, Peter S.H. Ellis, and Judith D. Mele. *Understrength Air Force Officer Career Fields: A Force Management Approach.* Santa Monica: Rand, 2005.

Gartzke, Erik. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth." *International Security Studies* 38 No 2 (2013): 41-73.

Gates, Robert M. Department of Defense Directive 5100.20. "National Security Agency/Central Security Service (NSA/CSS)." January 26, 2010. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/510020p.pdf.

Geisler, Robert J. Interview by Sarah White. Phone call. Fort Montgomery, New York. September 24, 2018.

Gigerenzer. Gerd and Wolfgang Gaissmaier. "Heuristic Decision Making." *Annual Review of Psychology.* Vol 62 (2011): 451-482.

Giles, Keir. "Information Troops — A Russian Cyber Command?" *3rd International Conference on Cyber Conflict*, C. Czosseck, E. Tvugu, T. Winfield (Eds.). Tallinn: CCD COE Publications, 2011).

____. "Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power." *Chatham House: The Royal Institute for International Affairs,* March 2016. https://www.chathamhouse.org/publication/russias-new-tools-confronting-west.

____. "The Military Doctrine of the Russian Federation 2010." *NATO Research Review.* February 2010. http://www.conflictstudies.org.uk/files/MilitaryDoctrine_RF_2010.pdf.

Ginsburgh, Robert N. and Edd D. Wheeler. "The Evolution of Air Warfare." *Air University Review*, Vol 23 No 3 (March-April 1972).

Giovanni, Matthew D. Interview by Sarah White. Phone call. Fort Montgomery, New York. December 14, 2018.

Glenney, Willliam. Interview by Sarah White. Phone call. Fort Montgomery, New York. January 14, 2019.

____. Interview by Sarah White. Phone call. Fort Montgomery, New York. March 11, 2019.

Golembiewski, Joseph R. "From Signals to Cyber: The Rise, Fall, and Resurrection of the Air Force Communications Officer." Thesis, Air University, June 2010.

Gould, Gordon T. "Computers and Communication in the Information Age." *Air University Review* Vol 21 No 4 (May-June 1970): 5-18.

Gourley, Robert D. "The Devil is in the Details." *Proceedings* Issue 123 (September 1997).

____. Interview by Sarah White. Phone call. Fort Montgomery, New York, July 26, 2018.

Graham, Janice. "Does the Navy Need the 1700 Community?" *Proceedings* Issue 125 (Feb 1999).

Grainger, Jim. Interview by Sarah White. Phone call. Fort Montgomery, New York. September 12, 2018.

Gray, Frank E. Interview by Sarah White. Phone call. Fort Montgomery, New York. October 19, 2018.

Gregory, Andrew. "Lethality Upgrade: Why a New Stryker Variant is Needed on the Modern Battlefield." *War on the Rocks.* April 12, 2017. https://mwi.usma.edu/lethality-upgrade-new-stryker-variant-needed-modern-battlefield/.

Gunder, Joseph. "Naval Security Group Aligns with NETWARCOM." Naval Network Warfare Command Public Affairs Office Press Release 05-010. October 4, 2005.

Hagerott, Mark R. Interview by Sarah White. Phone call. Fort Montgomery, New York. December 11, 2018.

Haggard, Stephan and Jon Lindsay. "North Korea and the Sony Hack: Exporting Instability through Cyberspace." *Asia-Pacific Issues,* No. 117 (2015): 3-8.

Halperin, Morton H. *Bureaucratic Politics and Foreign Policy.* Brookings Institution Press, 2002.

Hames, Jacqueline M. "Electronic Warfare - A New Way of Fighting." Army.mil, August 21, 2009. https://www.army.mil/article/26408/electronic_warfare_a_new_way_of_fighting.

Hanna, Mark. "Task Force XXI: The Army's Digital Experiment." *Strategic Forum* No. 119 (July 1997).

Harasimowicz, Michael. Interview by Sarah White. Phone call. Fort Montgomery, New York. June 20, 2018.

Harknett, Richard and Emily Goldman. "The Search for Cyber Fundamentals." *Journal of Information Warfare* Vol 15(2) (2016): 81-88.

Harley, Jeffrey S. Interview by Sarah White. Phone call. Fort Montgomery, New York. October 26, 2018.

____. "Space and Information Operations." *Army Space Journal* (Summer 2002): 10-11, 38.

Harrington, Lisa M., Lindsay Daugherty, S. Craig Moore, and Tara L. Terry. "Air Force-Wide Needs for Science, Technology, Engineering, and Mathematics (STEM) Academic Degrees." Santa Monica, CA: RAND Corporation, 2014.

Hartman, William J. Memorandum for Commanders and Staff Operationally Controlled by U.S. Army Cyber Command. "Authority to Operate for Army Cyberspace Operators." Fort Belvoir, VA: U.S. Army Cyber Command. July 7, 2017.

Harvey, J.C. NAVADMIN 338/05. "Merger of the Information Systems Technician (IT) and Cryptologic Technician (Communications) (CTO) Ratings." December 28, 2005.

Hastings, Scott. "Is There a Doctrine in the House?" *Proceedings* Issue 120 (April 1994).

Hatfield, Joseph. "U.S. Naval Academy Cyber Education: Turning Midshipmen into Cyber Warriors." Powerpoint brief. United States Naval Academy, Annapolis, MD. July 2018.

Hayden, Dale L. "Air-Mindedness." *Air & Space Power Journal* Vol 22 No 4 (Winter 2008): 44-46.

Hayden, Michael V. Memorandum to Lieutenant General Donald G. Cook, Vice Commander of Air Combat Command, from Lieutenant General Michael V. Hayden, Director of the National Security Agency, October 16, 2001. Received October 16, 2018, from 25AF FOIA manager via FOIA request 2018-04089-F.

Heacock, Phillip K. "The Viability of Centralized Command and Control." *Air University Review* Vol 30 No 2 (Jan-Feb 1979): 34-38.

Headquarters, Department of the Air Force. *Air Force Doctrine Document 1: Air Force Basic Doctrine, Organization, and Command*. Washington, D.C.: Headquarters, Department of the Air Force. October 14, 2011.

____. *Air Force Doctrine Document 1: Basic Aerospace Doctrine of the United States Air Force.* Washington, D.C.: Headquarters, Department of the Air Force. March 1, 1992.

____. *Air Force Doctrine Document 1: Basic Doctrine*. Washington, D.C.: Headquarters, Department of the Air Force. September 1997.

____. *Air Force Doctrine Document 1: Basic Doctrine*. Washington, D.C.: Headquarters, Department of the Air Force. November 17, 2003.

____. *Air Force Doctrine Document 1: Basic Doctrine*. Washington, D.C.: Headquarters, Department of the Air Force. February 27, 2015.

____. *Air Force Doctrine Document 2-5: Information Operations*. Washington, D.C.: Headquarters, Department of the Air Force. January 11, 2005.

____. *Air Force Doctrine Document 2-5.1: Electronic Warfare (Draft)*. Washington, D.C.: Headquarters, Department of the Air Force. July 30, 1999.

____. *Air Force Doctrine Document 3-1: Air Warfare*. Washington, D.C.: Headquarters, Department of the Air Force. Jan 22, 2000, incorporating change 1, July 28, 2011.

____. *Air Force Doctrine Document 3-12: Cyberspace Operations*. Washington, D.C.: Headquarters, Department of the Air Force. July 15, 2010.

Headquarters, Department of the Army. *Army Doctrine Publication 1: The Army.* Washington D.C.: Headquarters, Department of the Army. September 2012.

____. *Army Doctrine Reference Publication 1: The Army Profession.* Washington D.C.: Headquarters, Department of the Army. June 2015.

____. Execution Order 057-14. "HQDA EXORD 057-14 Cyber Center of Excellence (COE) Establishment." January 24, 2014.

____. *Field Manual 100-5 Operations*. Washington, D.C.: Headquarters, Department of the Army. June 1993.

____. *Field Manual 100-6: Information Operations.* Washington D.C.: Headquarters, Department of the Army, 1996.

____. *Field Manual 2-0 Intelligence.* Washington D.C.: Headquarters, Department of the Army, March 2010.

____. *Field Manual 3-0: Operations.* Washington, D.C.: Headquarters, Department of the Army, February 27, 2008.

____. *Field Manual 3-12: Cyberspace and Electronic Warfare Operations.* Washington, D.C.: Headquarters, Department of the Army. April 2017.

____. *Field Manual 3-13 Inform and Influence Activities.* Washington, D.C.: Headquarters, Department of the Army. January 2013.

____. *Field Manual 3-13 Information Operations.* Washington, D.C.: Headquarters, Department of the Army. December 2016.

____. *Field Manual 3-36 Electronic Warfare in Operations*. Washington D.C.: Headquarters, Department of the Army. February 2009.

____. *Field Manual 3-36 Electronic Warfare.* Washington D.C.: Headquarters, Department of the Army, November 2012.

____. *Field Manual 3-38 Cyber Electromagnetic Activities.* Washington, D.C.: Headquarters, Department of the Army. February 2014.

____. *Field Manual 34-37: Strategic, Departmental, and Operational IEW Operations.* Preliminary Draft. https://fas.org/irp/doddir/army/fm34-37_97/3-chap.htm.

____. *Army Doctrine Publication 6-0: Mission Command.* Washington, D.C.: Headquarters, Department of the Army 2012.

____. "U.S. Army Electronic Warfare Strategy for Unified Land Operations 2025." Headquarters, Department of the Army: DAMO-CY (Cyber Directorate). August 23, 2018.

Headquarters, Department of the Navy. *Naval Doctrine Publication 1: Naval Warfare.* Washington, D.C.: U.S. Navy, March 2010.

____. "Naval Operations Concept 2010: Implementing the Maritime Strategy." Washington, D.C.: Department of the Navy, 2010.

Headquarters, United States Air Force. "Air Force Cyberspace Command Path to FOC." Powerpoint briefing. September 12, 2007.

Headquarters, U.S. Space Command. "USCINCSPACE Implementation Plan for Computer Network Warfare." Peterson Air Force Base, CO: Headquarters, U.S. Space Command. May 13, 2001.

Healey, Jason, editor. *A Fierce Domain: Conflict in Cyberspace, 1986-2012.* The Atlantic Council: Cyber Conflict Studies Association, 2013.

Healey, Jason. "Claiming the Lost Cyber Heritage." Air Force Cyber College. June 1, 2017.

____. "From Cybernetics to Cyberspace." *Air Force Magazine* (January 2019).

Heath, James E. and Woodcock, Alexander E.R. "The Challenge of New and Emerging Information Operations." Unclassified paper released by INSCOM, LIWA. Fort Belvoir, VA, June 1999. http://www.dtic.mil/dtic/tr/fulltext/u2/a468421.pdf.

Heath, Tammy A. Interview by Sarah White. Phone call. Fort Montgomery, New York. November 6, 2018.

Helm, Stephanie. Interview by Sarah White. Phone call. Raleigh, North Carolina. December 28, 2018.

Helphenstine, Justin. Email correspondence with the author. February 20, 2018.

Heritage, Sean. Interview by Sarah White. Phone call. Fort Montgomery, New York. October 23, 2018.

"History of the Twenty-Fourth Air Force and 624th Operations Center." 24th Air Force Heritage Pamphlet. 24 AF Office of History. January 17, 2014.

"History, 780th Military Intelligence Brigade." INSCOM.mil. Accessed September 9, 2018. https://www.inscom.army.mil/MSC/780MIB/history.html.

"History. U.S. Strategic Command." STRATCOM.mil. Accessed October 14, 2018. http://www.stratcom.mil/About/History/.

Hoewing, G.L. NAVADMIN 233/05. "Cryptologic Officer Name Change to Information Warfare." September 15, 2005.

Hooley, Kevin R. Interview by Sarah White. Phone call. Fort Montgomery, New York. February 13, 2019.

Horton, Alex. "Army Looks to Deactivate Long-Range Surveillance Companies." *Stars and Stripes*, July 16, 2016.

"Human Resources Command Briefing to General Odierno." Powerpoint briefing. July 10, 2014.

Hunter, Matthew R. Interview by Sarah White. Phone call. Fort Montgomery, New York. November 28, 2018.

Hunzeker, Michael Allen. "Perfecting War: The Organizational Sources of Doctrinal Optimization." PhD Dissertation, Princeton University, 2013.

Hyland, Matthew T. "Operationalizing the 17D Workforce." *Cyber Compendium: Professional Continuing Education Course Papers* Vol 2 Issue 1 (Spring 2015): 2-8.

Implications of Advancing Technology for Naval Operations in the Twenty-First Century Volume 1: An Overview (Navy-21). Washington DC: National Academy Press, 1988.

"Information Systems Technician." Navy.mil. Updated February 2, 2019. https://www.public.navy.mil/bupers-npc/enlisted/community/crypto_it/Pages/IT.aspx.

Inglis, John C. Interview by Sarah White. Phone call. Fort Montgomery, New York. January 30, 2019.

INSCOM Command History Office. "The INSCOM Story." INSCOM.mil. Updated May 2, 2019. https://www.inscom.army.mil/organization/History.aspx.

"INSCOM Response to HAC Cyber Questions." Powerpoint briefing. August 14, 2012.

"Interactive On-Net Operator." INSCOM 780th Military Intelligence (Cyber) Brigade Career Opportunities. INSCOM.army.mil. Accessed June 10, 2019. https://www.inscom.army.mil/MSC/780MIB/cyberskills/netop.html.

"IT Career Path." Navy.mil. Updated August 2018. https://www.public.navy.mil/bupers-npc/enlisted/community/crypto_it/Documents/IT%20career%20path.pdf.

Jacobs, Michael J. Interview by Sarah White. Phone call. Fort Montgomery, New York. January 11, 2019.

Jamison, Lewis M. "The Information Explosion: Can the Air Staff Handle It?" *Air University Review* Vol 20 No 3 (March-April 1969): 83-89.

Jensen, Benjamin M. *Forging the Sword: Doctrinal Change in the U.S. Army.* Stanford: Stanford University Press, 2016.

Johnson, Harold R. "Organizational Integration — Key to the Military Application of Computer Technology." *Air University Review* Vol 17 No 1 (Nov-Dec 1965): 37-43.

Joint Chiefs of Staff. *Joint Vision 2010.* 1996

Junio, Timothy J. "How Probably is Cyber War? Bringing IR Theory Back Into the Cyber Conflict Debate." *Journal of Strategic Studies* 36:1 (2013): 125-133.

Kaczor, Joy M. "The Cyberspace Domain: Recommendations to Change Mindsets and Air Force Culture." *Cyber Compendium: Professional Continuing Education Course Papers* Vol 1 No 2 (Winter 2013): 98-104.

Kaplan, Fred. *Dark Territory: The Secret History of Cyber War.* New York: Simon and Schuster, 2016.

Karpf, Brandon. "Train Navy Officers for Cyber Lethality." *Proceedings* Issue 146 (February 2019): 24-28.

Khong, Yuen Foong. *Analogies at War: Korea, Munich, Dien Bien Phu, and the Vietnam Decisions of 1965.* Princeton University Press, 1992.

Kier, Elizabeth. "Culture and Military Doctrine: France Between the Wars." *International Security* 19/4 (Spring 1995): 69.

____. *Imagining War: French and British Military Doctrine Between the Wars.* Princeton University Press, 1999.

Kim, David T. Interview by Sarah White. Phone call. Fort Montgomery, New York. October 25, 2018.

King, James. "Never Bring a Stryker to a Tank Fight." Modern War Institute. May 2, 2017. https://mwi.usma.edu/never-bring-stryker-tank-fight/.

Klimburg, Alexander. "Mobilizing Cyber Power." *Survival* 53:1 (2011): 41-60.

Kohler, Matthew J. Interview by Sarah White. Phone call. Fort Montgomery, New York. February 7, 2019.

Korns, Stephen W. and Joshua E. Kastenberg. "Georgia's Cyber Left Hook." *Parameters* (Winter 2008-2009).

Kraus Jr., George F. "Information Warfare in 2015." *Proceedings* Issue 121 (August 1995).

Krepinevich Jr., Andrew F. *The Army and Vietnam*. Baltimore: Johns Hopkins University Press, 1986.

Lanham, Michael. Interview with Sarah P. White. West Point, New York. October 30, 2018.

Lamothe, Dan. "How the Pentagon's Cyber Offensive Against ISIS Could Shape the Future for Elite U.S. Forces." *The Washington Post*, December 16, 2017. https://www.washingtonpost.com/news/checkpoint/wp/2017/12/16/how-the-pentagons-cyber-offensive-against-isis-could-shape-the-future for-elite-u-s-forces/?utm_term=.a82c30417f65.

Lapowsky, Issie. "The Pentagon is Building a Dream Team of Tech-Savvy Soldiers." *Wired,* July 2, 2018.

Lawlor, Maryann. "Command Takes Network Control." Signal Magazine, October 2006. https://www.afcea.org/content/?q=node/1206.

Lawson, Sean. "Beyond Cyber Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber Threats." *Journal of Information Technology and Politics*, 10:1 (2013): 86-103.

Layton, Edwin T., Roger Pineau, and John Costello. *And I Was There: Pearl Harbor and Midway Breaking the Secrets*. New York: William Morrow and Company, 1985.

Lee, Robert M. "Disruptive by Design: Saving the Air Force Cyber Community." Signal Magazine, February 1, 2015. https://www.afcea.org/content/disruptive-design-saving-air-force-cyber community.

____. "The Failing of Air Force Cyber." Signal Magazine, November 1, 2013. https://www.afcea.org/content/?q=failing-air-force-cyber.

Leigher, Bill. "Fleet Cyber Command COMTENTHFLT NCBC 2-3 Dec 2009." Briefing. December 2, 2009.

____. Interview by Sarah White. Phone call. Fort Montgomery, New York. November 13, 2018.

Leonard-Barton, D.A. *Wellsprings of Knowledge: Building and Sustaining the Sources of Innovation.* Boston: Harvard Business School Press, 1995.

Levy, Dina G., Harry J. Thie, Albert A. Robbert, Scott Naftel, Charles Cannon, Rudolph H. Ehrenberg, and Matthew Gershwin. *Characterizing the Future Defense Workforce.* Santa Monica: Rand, 2001.

Lindsay, Jon R. "Stuxnet and the Limits of Cyber Warfare." *Security Studies* Vol 22 No 3 (2013): 365-404.

Locklear, Sam J. NAVADMIN 286/09. "Department of the Navy Memorandum for Director of Naval Intelligence (N2), Reorganization of the Office of the Chief of Naval Operations (OPNAV) Staff." June 26, 2009.

____. NAVADMIN 316/09. "Establishment of the Deputy Chief of Naval Operations for Information Dominance (N2/N6)." October 29, 2009.

Loescher, Michael S. "Copernicus Offers a New Center of the Universe." *Proceedings* Issue 117 (January 1991).

____. "Space and Electronic Warfare: A Navy Policy Paper on a New Warfare Area." Washington DC: Director, Space and Electronic Warfare, June 1, 1992.

Long, Austin. *The Soul of Armies: Counterinsurgency Doctrine and Military Culture in the U.S. and U.K.* Ithaca: Cornell University Press, 2016.

Lopez, C. Todd. "Ground Forces 'Must Never, Ever Fail,' New Army Chief Says." DoD News, August 14, 2015. https://dod.defense.gov/News/Article/Article/613672/.

Lord, William T. "USAF Cyberspace Command: To Fly and Fight in Cyberspace." *Strategic Studies Quarterly* (Fall 2008).

Lospinoso, Josh. "Fish Out of Water: How the Military Is An Impossible Place for Hackers, and What to Do About It." War On the Rocks, July 12, 2018. https://warontherocks.com/2018/07/fish-out-of-water-how-the-military-is-an-impossible-place-for-hackers-and-what-to-do-about-it/.

Luti, William J. "Battle of the Airwaves." *Proceedings* Issue 118 (January 1992). https://www.usni.org/magazines/proceedings/1992-01/battle-airwaves.

Lynch, Joe. "The Logistics of Logistics." October 12, 2014. https://www.thelogisticsoflogistics.com/my-logisticians-are-a-humorless-lot/.

Lynn III, William J. "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs* (Sept-Oct 2010).

MacDonald, Peter E. and William T. Torpey. "Intelligence Architecture, Echelons Corps and Below (ECB): Some Near Term Alternatives." U.S. Army War College Military Studies Program Paper. U.S. Army War College, April 5, 1991.

Maclin, Beth. "Schlesinger Report Calls Attention to Nuclear Mission and Deterrence." *Belfer Center Newsletter* (Spring 2009).

Macmillan, David T. "Technology: the Catalyst for Doctrinal Change." *Air University Review* Vol 29 No 1 (Nov-Dec 1977): 16-23.

Mahnken, Thomas G. and James R. Fitzsimonds. "Tread-heads or Technophiles? Army Officer Attitudes Toward Transformation." *Parameters* (Summer 2004): 57-72.

Mahnken, Thomas G. *Uncovering Ways of War: U.S. Intelligence and Foreign Military Innovation, 1918-1941*. New York: Cornell University Press, 2002.

Mahoney, John. Interview by Sarah White. Phone call. Fort Montgomery, New York. October 12, 2018.

Mann, Edward. "Desert Storm: The First Information War?" *Air Power* Vol 8 No 4 (1994): 4-14.

March, James G. and Simon, Herbert A. *Organizations,* 2nd edition. Cambridge: Blackwell, 1993.

Martelle, Michael. "Joint Task Force ARES and Operation GLOWING SYMPHONY: Cyber Command's Internet War Against ISIL." National Security Archive. August 13, 2018. https://nsarchive.gwu.edu/briefing-book/cyber-vault/2018-08-13/joint-task-force-ares-operation-glowing symphony-cyber-commands-internet-war-against-isil.

Massaro, James. "67th Intelligence Wing Acquires New Mission." *IA Newsletter* Vol 4 No 1 (January 12, 2000).

Mauchly, John W. "Mauchly on the trials of building ENIAC." *IEEE Spectrum* Vol. 12, No. 4 (April 1975): 70-76.

Mazarr, Michael J. *Mastering the Gray Zone: Understanding a Changing Era of Conflict*. Carlisle, PA: U.S. Army War College Press, 2015.

McCarthy, James E. "Training for Cyber Operations." Air Force Research Laboratory Report. April 2018.

McCartney, Scott. *ENIAC - The Triumphs and Tragedies of the World's First Computer.* New York: Walker and Company, 1999.

McComas, Lesa A. *The Naval Officer's Guide*, *12th Ed.* Annapolis, M.D.: Naval Institute Press, 2011.

McConnell, J.M and Edward J. Giorgio. "Building Information Security Layer by Layer." *Proceedings* Issue 124 (December 1998).

McCullough, Bernard J. "U.S. Fleet Cyber Command/U.S. Tenth Fleet Strategic Plan, Calendar Year 2011." May 17, 2011.

____. Interview by Sarah White. Phone call. Fort Montgomery, New York. January 21, 2019.

McHugh, John M. General Order 2014-63. "Establishment of the United States Army Cyber Branch." August 21, 2014.

____. General Order No. 2010-26. "Establishment of the United States Army Cyber Command." Headquarters, Department of the Army. October 1, 2010.

____. General Order No. 2014-02. "Affirmation of Secretary of the Army Commitment to Unity of Effort; Designation of U.S. Army Cyber Command as an Army Force Component Headquarters; Reactivation of Second Army and Designation as a Direct Reporting Unit; Disestablishment of the U.S. Army Network Enterprise Technology Command/9th Signal Command (Army) as a Direct Reporting Unit and Reassignment to Second Army; Designation of General Court-Martial Convening Authorities." Headquarters, Department of the Army. March 6, 2014.

____. Memorandum. "Establishment of the Army Cyber Center at West Point." October 19, 2012.

____. Secretary of the Army Memorandum. "Army Directive 2011-03 (Change of Operational Control for 1st Information Operations Command (Land) and Direction for U.S. Army Cyber Command to Conduct the Information Operations Missions for the Army)." February 2, 2011.

McLaughlin, James K. Interview by Sarah White. Phone call. Fort Montgomery, New York. September 4, 2018.

McMahon, Sheila. Interview by Sarah White. Phone call. Fort Montgomery, New York. October 25, 2018.

McNeill, William. Interview by Sarah White. In person. Fort Meade, Maryland. September 24, 2018.

Memorandum from DA Washington DC to All Army Commanders. "Information Operations Support from LIWA." January 8, 1999.

Memorandum from DA Washington DC to ARSTAF. "Activation of US Army Land Information Warfare Activity." May 8, 1995.

Memorandum from the War Department. "Establishment of the Army Security Agency." Washington D.C. September 6, 1945.

Mesic, Richard, Myron Hura, Martin C. Libicki, Anthony M. Packard, and Lynn M. Scott. "Air Force Cyber Command (Provisional) Decision Support." Santa Monica, CA: RAND Corporation, 2010.

Metropolis, N., J. Howlett, and Gian-Carlo Rota, editors. *A History of Computing in the Twentieth Century.* Orlando: Academic Press, 1980.

"Military Demographics. Air Force Personnel Center." AFPC.af.mil. Updated March 31, 2019. https://www.afpc.af.mil/Portals/70/documents/03_ABOUT/Military%20Demographics%20Ma%2019.pdf?ver=2019-04-18-104044-823.

"Military Doctrine of the Russian Federation." Carnegieendowment.org. Updated February 5, 2010. http://carnegieendowment.org/files/2010russia_military_doctrine.pdf.

Miller, Matthew, Jon Brickey, and Gregory Conti. "Why Your Intuition About Cyber Warfare is Probably Wrong." Small Wars Journal, November 29, 2012. https://smallwarsjournal.com/jrnl/art/why your-intuition-about-cyber-warfare-is-probably-wrong.

Minihan, Kenneth A. Interview by Sarah White. Phone call. Fort Montgomery, New York. January 15, 2019.

Minnick, Homer. Interview by Sarah White. Phone call. Fort Montgomery, New York. July 28, 2018.

Minor, Caleb. "New Space, Cyber Battalion Activates at JBLM." Army.mil, January 16, 2019. https://www.army.mil/article/216236/new_space_cyber_battalion_activates_at_jblm.

Mitchell, William. *Our Air Force: The Keystone of National Defense.* New York: E.P. Dutton and Company, 1921. https://archive.org/details/ourairforcekeys00mitcgoog/page/n7.

Monteiro, Alfred. Interview by Sarah White. Phone call. Fort Montgomery, New York. December 7, 2018.

Moore, Frederick L. "Radio Counter-Measures." *Air University Quarterly* Vol 2 No 2 (Fall 1948): 57-66.

Moore, Richard D. Interview by Sarah White. Phone call. Fort Montgomery, New York. October 18, 2018.

____. Interview by Sarah White. Phone call. Raleigh, North Carolina. December 20, 2018.

Morton, John F. "Space and Electronic Warfare Comes of Age." *Proceedings* Issue 117 (January 1991).

Moseley, T. Michael and Michael W. Wynne. Memorandum. "Establishment of an Operational Command for Cyberspace." September 6, 2006.

Moseley, T. Michael. Memorandum to Lieutenant General Robert J. Elder. "Operational Cyberspace Command 'Go Do' Letter." November 1, 2006.

Munns, Charles L. "A Global Navy Needs a Global Network." *Proceedings* Issue 129 (January 2003).

Murphy, James. "Give Information Personnel More Training and Credibility." *Proceedings* Issue 134 (September 2008).

Murray, William N. "Reimagine Intelligence Officer Training." *Proceedings* Issue 145 (January 2019).

Murray, Williamson. "Armored Warfare: The British, French, and German Experiences." In *Military Innovation in the Interwar Period*, edited by Williamson Murray and Allan R. Millett, 34-45. New York: Cambridge University Press, 1996.

Muztafago, Michael. Interview by Sarah White. Phone call. Fort Montgomery, New York. October 30, 2018.

Myers, Harold P. , John P. Williamson, and Gabriel G. Marshall, eds. "A Continuing Legacy: From USAFSS to 25th Air Force 1948-2015." San Antonio: 25th Air Force History Office.

Nagl, John A. *Learning to Eat Soup with a Knife: Counterinsurgency Lessons from Malaya and Vietnam.* Chicago: The University of Chicago Press, 2002.

Nagy, Paul. "Network-Centric Warfare Isn't New." *Proceedings* Issue 127 (September 2001).

Nakashima, Ellen and Missy Ryan. "U.S. Military Has Launched a New Digital War Against the Islamic State." *The Washington Post*, July 15, 2016. https://www.washingtonpost.com/world/national/security/us-militarys-digital-war-against-the-islamic-state-is-off-to-a-slow-start2016/07/15/76a3fe82-3da3-11e6-a66f-aa6c1883b6b1_story.html?utm_term=.15df6fd49410.

Naples, Anthony J. "Concept Plan: Establish Headquarters, Army Forces Cyber Command (ARFORCYBER) & Army Cyber Operations and Integration Center (ACOIC)." U.S. Army Space and Missile Defense Command/Army Forces Strategic Command. June 4, 2010.

"Naval Information Forces." IWCsync.org. https://www.iwcsync.org/about/navifor.

"Naval Information Warfare Activity Was Established in July 1994." Station Hypo. Accessed January 22, 2019. https://stationhypo.com/2017/07/22/navy-information-warfare-activity-was-established-in-july-1994/.

"Navy Cyber Defense Operations Command Celebrates Past, Present, Future." Navy.mil. February 11, 2016. https://www.navy.mil/submit/display.asp?story_id=93055.

"Navy Establishes Network Warfare Command." Navy.mil. March 28, 2002. https://www.navy.mil/submit/display.asp?story_id=1156.

"Navy Information Professional: Connecting the Global Force." United States Naval Academy Informational Brochure. https://www.usna.edu/CyberCenter/_files/documents/idc/NavyIPCCommunityBrochure.pdf.

Neighbors, Mark D. Interview by Sarah White. Phone call. Fort Montgomery, New York. February 8, 2019.

Nicholson, Clifton L. "Command and Control and the Decision-Making Process." *Air University Review* Vol 15 No 1 (Nov-Dec 1963): 77-81.

Niner, F.J. OPNAV Notice 5450. "Disestablish Commander, Naval Security Group Command (COMNAVSECGRU), Fort George G. Meade, MD; Rename and Realign All Subordinate NAVSECGRU Commands and Detachments." December 29, 2005.

"NIOC Norfolk's History." Navy.mil Accessed January 16, 2019. https://www.public.navy.mil/fltfor/iwtgnorfolk/Pages/NIOCNorfolkHistory.aspx.

Nutwell, Robert M. "IT-21 Intranet Provides Big 'Reachbacks.'" *Proceedings* Issue 124 (January 1998).

O'Connor, Maureen. Interview by Sarah White. In person. Columbia, Maryland. September 28, 2018.

Orr, Stephen. Interview by Sarah White. Phone call. Fort Montgomery, New York. December 3, 2018.

Otto, Robert P. Interview by Sarah White. Phone call. Fort Montgomery, New York. August 16, 2018.

Pancake, Frank R. "The Strategic Striking Force." *Air University Quarterly* Vol 2 No 2 (Fall 1948).

"Panel Urges Air Force to Unify Nuclear Command." *The New York Times.* September 12, 2008. https://www.nytimes.com/2008/09/13/washington/13military.html.

Parode, Steve. Interview by Sarah White. In person. Washington, D.C. September 25, 2018.

Petersen, John L. "Info War: The Next Generation." *Proceedings* Issue 123 (January 1997).

Peterson, John. "Info Wars." *Proceedings* Issue 119 (May 1993).

Petraeus, David H. Memorandum from Headquarters: Multi-National Force-Iraq to the Vice Chief of Staff, United States Army. "Computer Network Operations." July 26, 2008.

Phillips, Jeffrey A. "Engendering Cyber-Mindedness in the United States Air Force Cyber Officer Corps." Thesis, Air University, 2011.

Picklesmeier, John W. Interview by Sarah White. Phone call. Fort Montgomery, New York. August 1, 2018.

Pierce, Terry C. *Warfighting and Disruptive Technologies: Disguising Innovation.* New York: Frank Cass, 2004.

Pomerleau, Mark. "How A Merger Will Expand the Air Force's Cyber Edge." Fifth Domain, April 4, 2019. https://www.fifthdomain.com/dod/air-force/2019/04/04/how-a-merger-will-expand-the-air-forces-cyber-edge/?fbclid=IwAR3eW1AWbSfRddkTp9qoVYNIwHz3ki_0r-gntJet-hslavDsELq0zlhktk8.

____. "Is the U.S. Behind in Cyber-Enabled Info Operations?" Fifth Domain, November 27, 2017. https://www.fifthdomain.com/dod/2017/11/27/is-the-us-behind-in-cyber-enabled-info-operations/

____. "Navy Creates Information Warfare Development Center." *Navy Times*, February 24, 2017.

____. "The Army is Willing to Spend Big to Support the Cyber Mission." Fifth Domain, April 3, 2019. https://www.fifthdomain.com/dod/army/2019/04/03/the-army-is-willing-to-spend-big-to-support-the-cyber-mission/?fbclid=IwAR2vA-ptNrJEK0W8H7VeO47OkOI8i50wNflWg-gjlZZWXvkb_6PxEHX1RYg.

____. "Where Do Information Operations Fit in the DoD Cyber Enterprise? Fifth Domain, July 26, 2018. https://www.fifthdomain.com/c2-comms/2018/07/26/where-do-information-operations-fit-in-the-dod-cyber-enterprise/.

Portare, Anthony F. Interview by Sarah White. Phone call. Fort Montgomery, New York. October 18, 2018.

Posen, Barry R. *The Sources of Military Innovation: France, Britain, and Germany Between the World Wars.* Ithaca: Cornell University Press, 1985.

Pournelle, Phil. Interview by Sarah White. In person. Washington, D.C., September 27, 2018.

Price, Alfred. *The History of U.S. Electronic Warfare Vol III: Rolling Thunder Through Allied Force, 1964-2000.* Association of Old Crows, 2000.

Quattrin, Alan J. Interview by Sarah White. Phone call. Fort Montgomery, New York. October 16, 2018.

Quinn, Ruth. "522nd MI (CEWI) Battalion Passes Tactical Intelligence Test, April 7 1977." *Army.mil.* https://www.army.mil/article123363/522nd_mi_cewi_battalion_passes_tactical_intelligence_test_april_7_1977.

Raaberg, Douglas L. "Commander Directed Report of Investigation, Prepared by MG Douglas L. Raaberg, Investigating Officer, Concerning An Unauthorized Transfer of Nuclear Warheads Between Minot AFB, North Dakota, and Barksdale AFB, Louisiana." August 30, 2007.

Rader, Troy A. Interview by Sarah White. Phone call. Fort Montgomery, New York. December 10, 2018.

"RAND Project Air Force: Annual Report." Santa Monica, CA: RAND Corporation, 2010.

"Ready-for-Sea Modular Course and Handbook." San Diego: Naval Reserve Intelligence Program, April 9, 1999. https://fas.org/man/dod-101/navy/docs/rfs4/ready.pdf.

"Records of the Naval Electronic Systems Command." National Archives. Accessed January 28, 2019. https://www.archives.gov/research/guide-fed-records/groups/345.html.

Reilly, James T. Interview by Sarah White. In person. The Pentagon, Washington, D.C. December 18, 2018.

____. Interview by Sarah White. Phone call. Fort Montgomery, New York. October 17, 2018. 2018.

"Resources for Students and Educators: NSA Partners with Schools." NSA. Accessed October 29, 2018. https://www.nsa.gov/resources/students-educators/.

Rid, Thomas. "Cyber War Will Not Take Place." *Journal of Strategic Studies.* 35:1 (2012): 5-32.

____. "More Attacks, Less Violence." *Journal of Strategic Studies.* 36:1 (2013): 139-142.

Rid, Thomas and Robert M. Lee. "OMG Cyber!" *The RUSI Journal* 159:5 (2014) 4-12.

Rodriguez, Julianna. "Cyber Common Technical Core (CCTC) Methodology and Content." Information paper. Fort Gordon, GA. August 10, 2016.

____. "Cyber Common Technical Core Methodology and Content." Information paper. Fort Gordon, GA. August 10, 2016.

Rogers, M.S., M.A. Brown, W.E. Leigher, S.R. Filipowski, J.E. Tighe, G.W. Clusen, W.L. Metts, J.P. Rapin, and M.D. Neighbors. "Cryptologic Community Foundational Principles." Document. September 7, 2011.

Rogers, Michael S. Interview by Sarah White. In person. Annapolis, Maryland. January 2, 2019.

Rohde, William E. "What is Info Warfare?" *Proceedings* Issue 122 (February 1996).

Romano, Anthony. "Joint Vision 2010: Developing the System of Systems." Thesis, Air University, 1998.

Rona, Thomas. "Weapon Systems and Information War." Washington D.C.: Office of the Secretary of Defense. July 1, 1976.

Rosen, Stephen P. *War and Human Nature.* Princeton: Princeton University Press, 2007.

____. *Winning the Next War: Innovation and the Modern Military.* Ithaca: Cornell University Press, 1991.

Rosenberg, Barry. "Why is SPAWAR Now NAVWAR? Networks and Cyber Warfare." Breaking Defense, June 5, 2019. https://breakingdefense.com/2019/06/why-is-spawar-now-navwar-networks-cyber warfare/.

Roughead, Gary. "Information Dominance: The Navy's Initiative to Maintain the Competitive Advantage in the Information Age." Remarks delivered at the Center for Strategic and International Studies. October 1, 2009.

____. Interview by Sarah White. Phone call. Fort Montgomery, New York. January 16, 2019.

____. Memorandum for Commander U.S. Fleet Forces Command, Director of Naval Intelligence. "Fleet Cyber Command/Commander Tenth Fleet Implementation Plan." July 23, 2009.

____. Memorandum for Director of Naval Intelligence (N2). "Reorganization of the Office of the Chief of Naval Operations (OPNAV) Staff." June 26, 2009.

Rueter, Bradley A. "Cyberspace Integration within the Air Operations Center." Thesis, Air University, May 2013.

Rumsfeld, Donald. "Information Operations Roadmap." Washington, D.C.: Department of Defense. October 30, 2003.

Russell, Alison Lawlor. "The Georgia-Russia War." *Cyber Blockades*. Washington, D.C.: Georgetown University Press, 2014.

Ryan, Amber. Interview by Sarah White. Phone call. Fort Montgomery, New York. January 7, 2019.

Sanders, Wayne. "Expectations Management of Cyberspace Effects at the Tactical Level." White paper. Emailed to Author January 31, 2018.

Sanger, David E. *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power.* New York: Crown Publishers, 2013.

Scales, Robert. "Are You a Strategic Genius? Not Likely, Given the Army's System for Selecting, Educating Leaders." *Association of the United States Army,* October 13, 2016.

Schaeffer, Richard C. Interview by Sarah White. Phone call. Fort Montgomery, New York. February 12, 2019.

Schein, Edward H. *Organizational Culture and Leadership*, 3rd ed. San Francisco: Jossey-Bass, 2004.

Schell, Roger R. "Computer Security: The Achilles Heel of the Electronic Air Force?" *Air University Review* Vol 30 No 2 (Jan-Feb 1979): 16-34.

Schell, Walter. Email correspondence with the author. January 25, 2018.

Schlesinger, James R. "Secretary of Defense Task Force on DoD Nuclear Weapons Management." September 12, 2008.

Schmidt, Lara, Caolionn O'Connell, Hirokazu Miyake, Akhil R. Shah, Joshua William Baron, Geof Nieboer, Rose Jourdon, David Senty, Zev Winkleman, Louise Taggart, Susanne Sondergaard, Neil Robinson. "Cyber Practices: What Can the U.S. Air Force Learn from the Commercial Sector?" Santa Monica, CA: RAND Corporation, 2015.

Schoka, Andrew. "Cyber Command, the NSA, and Operating in Cyberspace: Time to End the Dual Hat." War on the Rocks, April 3, 2019. https://warontherocks.com/2019/04/cyber-command-the nsa-and-operating-in-cyberspace-time-to-end-the-dual-hat/.

Schreyo¨gg, Georg and Kliesch-Eberl, Martina. "How dynamic can capabilities be?" *Strategic Management Journal* 28 (2007): 913– 933.

Scott, Lynn M., Raymond E. Conley, Richard Mesic, Edward O'Connell, Darren D. Medlin. "Human Capital Management for the U.S. Air Force." Santa Monica, CA: RAND Corporation, 2010.

Scribner, Patrick J. Interview by Sarah White. Phone call. Fort Montgomery, New York. November 8, 2018.

Shanahan, John N.T. Interview by Sarah White. Phone call. Fort Montgomery, New York. August 2, 2018.

Sharpe Jr., James D. and Creviston, Thomas E. "Understanding Mission Command." Army.mil, July 10, 2013. https://www.army.mil/article/106872/Understanding_mission_command/.

Sheiffer, Matthew J. "U.S. Army Information Operations and Cyber-Electromagnetic Activities: Lessons from Atlantic Resolve." Military Review online exclusive. March 2018. https://www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2018-OLE/Mar/Army-Info-Ops/.

Shwedo, Bradford J. Interview by Sarah White. Phone call. Fort Montgomery, New York. August 29, 2018.

"Signals Intelligence Analyst." AirForce.com. Accessed June 30, 2018. https://www.airforce.com/careers/detail/signals-intelligence-analyst.

Simon, Herbert A. "The Scientist as Problem Solver." In *Complex Information Processing: The Impact of Herbert A. Simon,* edited by D. Klahr, K. Kotovsky, 373-398. Hillsdale, NJ: Erlbaum, 1989.

Singer, Andrew. Interview by Sarah White. Phone call. Fort Montgomery, New York. December 12, 2018.

Singer, Peter and Emerson T. Brooking. *LikeWar: The Weaponization of Social Media*. New York: Eamon Dolan/Houghton Mifflin Harcourt, 2018.

Sizer, Richard A. "Land Information Warfare Activity." *The Military Intelligence Professional Bulletin.* https://fas.org/irp/agency/army/mipb/1997-1/sizer.htm.

Smeets, Max. "When Routine Isn't Enough: Why Military Cyber Command Needs Human Creativity." War on the Rocks, December 5, 2017. https://warontherocks.com/2017/12/routine-isnt-enough-military-cyber-commands-need-human-creativity/.

"Space and Naval Warfare Systems Command History: 1966 to 2007." Received via email from Steven A. Davis, Space and Naval Warfare Systems Command Public Affairs and Corporate Communications, January 23, 2019.

Speller, Ian. *Understanding Naval Warfare.* New York: Routledge, 2014.

Steiner, Ron. "NETWARCOM/NAVSECGRU Alignment Communications Plan." September 21, 2005. Received via email from Lieutenant Commander William B. Tisdale, U.S. Fleet Cyber Command U.S. Tenth Fleet Public Affairs Officer, November 7, 2018.

Stephenson, Henry. "Masters or Jacks?" *Proceedings* Issue 140 (October 2014).

Stern, Matthew. Interview by Sarah White. Phone call. Fort Montgomery, New York. November 26, 2018.

Stoll, Cliff. *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage.* New York: Pocket Books, 1989.

Stone, John. "Cyber War Will Take Place!" *Journal of Strategic Studies* 36:1 (2013): 101-108.

Strategic Studies Group XXVI. "The Convergence of Sea Power and Cyber Power." March 2008.

Strategic Studies Group XXVII. "Collaborate and Compel — Maritime Force Operations in the Interconnected Age." December 2008.

Stroup Jr., Theodore G. "Leadership and Organizational Culture: Actions Speak Louder than Words." *Military Review* LXXVI, No. 1. January/February 1996.

Sulmeyer, Michael. "Much Ado About Nothing? Cyber Command and the NSA." War on the Rocks, July 19, 2017. https://warontherocks.com/2017/07/much-ado-about-nothing-cyber-command-and-the-nsa/.

Surdu John R. and Gregory J. Conti, "Join the Cyber Corps: A Proposal for a Different Military Service." Accessed at gregconti.com.

Surdu, John R. Interview by Sarah White. Phone call. Fort Montgomery, New York. November 28, 2018.

Swanson, Rowena W. "Information Sciences: Some Research Directions." *Air University Review* Vol 17 No 3 (March-April 1966): 56-68.

Swartz Peter M. and Michael C. Markowitz. "Organizing OPNAV (1970-2009)." Report prepared for the Department of the Navy Naval History and Heritage Command by CNA Analysis and Solutions. https://www.cna.org/cna_files/pdf/D0020997.A5.pdf.

System Technology Associates, Inc. "609 IWS: A Brief History Oct 1995-Jun 1999." Shaw Air Force Base, South Carolina: 20th Fighter Wing, 2006.

"Tactical Cyber Counterfire ISO BCT Operations." Information paper. No date.

"Tactical Offensive Cyberspace Operations in 2020." Powerpoint briefing. April 10, 2013.

Tate, Ryan, Natasha Orslene, Julianna Rodriguez. "Training for Effect: The Army Cyber School Training Strategy." Information paper. Fort Gordon, GA. 2017.

Tate, Ryan. "U.S. Army Cyber School Training Efforts." Information paper. Fort Gordon, GA. October 2014.

Terry, Katrina A. "Overcoming the Support Focus of the 17D Cyberspace Operations Career Field." Thesis, Air Force Institute of Technology, 2011.

"The Army Space Cadre: Space Professionals (FA40) and Space Enablers." Army.mil. September 27, 2010. https://www.army.mil/article/45767/the_army_space_cadre_space_professionals_fa40_and_space_enablers.

"The Cryptologic Technician Rating." U.S. Naval Cryptologic Veterans Association. Updated June 10, 2016. https://usncva.org/history/ct-rating-history.html.

Thibodeaux, Maxell S. "Organizing the Army for Information Warfare." Thesis, U.S. Army War College, March 2013.

Thomas, Timothy. "Russia's 21st Century Information War: Working to Undermine and Destabilize Populations." *Defense Strategic Communications: The Official Journal of the NATO Strategic Communications Center of Excellence* 1:1 (2015): 10-25.

Thomkins, William J. Interview by Sarah White. In person. Fort Belvoir, Virginia. September 27-28, 2018.

Tighe, Jan. Interview by Sarah White. Phone call. Fort Montgomery, New York. October 30, 2018.

Tilley, Ken. "U.S. Army Cyber School and Branch Annual Command History, 4 August 2014 to 31 December 2016." U.S. Army Cyber School, Fort Gordon, GA. December 2016.

Toffler, Alvin and Heidi. *War and Anti-War: Survival at the Dawn of the 21st Century*. New York: Little, Brown and Company, 1993.

"Tool Developer Qualification Course (TDQC) Standard Operating Procedures (Draft)." 780th Military Intelligence Brigade. May 19, 2017.

"Transcript: Lessons from our Cyber Past — The First Military Cyber Units." Transcript from "Lessons from our Cyber Past: The First Military Cyber Units." Event by the Atlantic Council's Cyber Statecraft Initiative. March 5, 2012. https://www.smartdatacollective.com/lessons-our-cyber-past-history-cyber-intelligence/.

Trauschweizer, Ingo. *The Cold War U.S. Army: Building deterrence for Limited War.* Lawrence: University Press of Kansas, 2008.

Trotter, Dietra L. Interview by Sarah White. Phone call. Fort Montgomery, New York. November 19, 2018.

Trump, Donald J. "National Cyber Strategy of the United States of America." September 2018.

Turner, Alfred. Interview by Sarah White. Phone call. Fort Montgomery, New York. January 16, 2019.

USAF Occupational Measurement Center, Air Training Command. "Occupational Survey Report: Communications-Electronics Utilization Field, AFSC 30XX." Randolph Air Force Base, TX: Air Training Command, 1984.

"U.S. Army Cyber Command, Brief History." Powerpoint briefing. No date.

U.S. Army Cyber Command/2nd Army Cyber Proponent. "U.S. Army LandCyber White Paper 2018-2030." Fort Meade, MD, U.S. Army Cyber Command/2nd Army Cyber Proponent. September 9, 2013.

U.S. Army Training and Doctrine Command. *TRADOC 525-7-8 Cyberspace Operations Concept Capability Plan*. U.S. Army Training and Doctrine Command. February 22, 2010.

____. *TRADOC Pam 525-3-0 The Army Capstone Concept. Operational Adaptability: Operating Under Conditions of Uncertainty and Complexity in an Era of Persistent Conflict, 2016-2028.* U.S. Army Training and Doctrine Command. December 21, 2009.

____. *TRADOC Pam 525-3-1 The United States Army Operating Concept, 2016-2028.* U.S. Army Training and Doctrine Command. August 19, 2010.

____. *TRADOC Pam 525-5-600 The United States Army's Concept of Operations LandWarNet 2015.* U.S. Army Training and Doctrine Command. February 11, 2008.

____. *TRADOC Pam 525-7-6: United States Army Concept Capability Plan for Army Electronic Warfare Operations for the Future Modular Force, 2015-2024.* U.S. Army Training and Doctrine Command. August 16, 2007.

____. *TRADOC Pam 525-8-6: The U.S. Army Concept for Cyberspace and Electronic Warfare Operations 2025-2040*. U.S. Army Training and Doctrine Command. January 2018.

U.S. Congress. House. Armed Services Committee. *Information Technology: An Examination of DoD Network Vulnerabilities.* May 17, 2001. Statement by Vice Admiral Richard W. Mayo, Director, Space, Information Warfare, Command and Control, Office of the Chief of Naval Operations.

____. *Network-Centric Warfare and Information Security.* February 23, 1999. Statement by Vice Admiral Arthur K. Cebrowski, President, Naval War College.

____. *Air Force Strategic Initiatives.* 110th Congress, 1st session, October 24, 2007.

U.S. Congress. House. Subcommittee on Military Procurement and Research and Development. *Information Superiority for the 21st Century Battlefield.* March 20, 1997. Statement by Lieutenant General William L. Donahue, Deputy Chief of Staff, Communications and Information, Headquarters, Department of the Air Force.

U.S. Congress. Senate. Committee on the Armed Services. *Hearing to Receive Testimony on 30 Years of Goldwater-Nichols Reform*. November 10, 2015, Washington DC.

"U.S. Cyber Command History." CyberCom.mil. Accessed Oct 14, 2018. https://www.cybercom.mil/About/History/.

U.S. Government Accountability Office. *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks.* GAO/AIMD 96-84. Washington D.C., May 22, 1996.

____. *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks.* GAO/AIMD-96-84. Washington, D.C., 1996.

Underwood, Kimberly. "Army Cyber to Become and Information Warfare Command." Signal Magazine, March 14, 2019. https://www.afcea.org/content/army-cyber-become-information-warfare-command.

"United States Army Intelligence and Security Command Cyberspace Operations." Powerpoint briefing. October 13, 2010.

U.S. Government Printing Office. "Electronic Warfare: Dominate the Electromagnetic Spectrum." Informational Brochure. http://usacac.army.mil/cac2/cew/repository/ElectronicWarfare_Brochure.pdf.

"USCYBERCOM TASKORD 16-0063 to Establish Joint Task Force (JTF)-Ares to Counter the Islamic State of Iraq and the Levant (ISIL) in Cyberspace." May 5, 2016. https://nsarchive2.gwu.edu/dc.html?doc=3678213-Document-07-USCYBERCOM-to-CDRUSACYBER-Subj#document/p23.

Vergun, David. "Army Opens New Intelligence MOS." Army.mil, November 29, 2012. https://www.army.mil/article/92099/Army_opens_new_intelligence_MOS/.

____. "Cyber Network Defender MOS Now Open to NCOs." Army.mil, April 14, 2014. https://www.army.mil/article/123328/Cyber_Network_Defender_MOS_now_open_to_NCOs/.

Vernez, Georges, Craig Moore, Steven Martino, and Jeffrey Yuen. "Improving the Development and Utilization of Air Force Space and Missile Officers." Santa Monica, CA: RAND Corporation, 2006.

Vick, Alan J. "Force Presentation in U.S. Air Force History and Airpower Narratives." Santa Monica, CA: RAND Corporation, 2018.

Wada, Debra S. Memorandum from Department of the Army: Assistant Secretary of the Army for Manpower and Reserve Affairs to CG, ARCYBER. "Civilian Cyberspace Effects Career Program." January 18, 2017.

Warner, Michael. "Notes on the Evolution of Computer Security Policy in the U.S. Government, 1965-2003." *IEEE Annals of the History of Computing*. IEEE Computer Society, 2015.

____. "Notes on Military Doctrine for Cyberspace Operations in the United States: 1992-2014." *The Cyber Defense Review.* August 27, 2015.

____. "Cybersecurity: A Prehistory." *Intelligence and National Security* 27:5 (2012): 781-799.

"Warrant Officer Transition to CF170." Powerpoint briefing. No date.

Waxman, Matthew C. "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)." *The Yale Journal of International Law* Vol 36 (2011): 421-459.

Weatherford, Mark. Interview by Sarah White. Phone call. Fort Montgomery, New York. July 31, 2018.

Wells, Mark D. "Tribal Warfare: The Society of Modern Airmen." *Air and Space Power Journal* Vol 29 No 3 (May-June 2015):82-87.

Welsh III., Mark A. Memorandum for HQ AFSPC/CC. "Weapon System Designation Request for Cyberspace Operations Systems." March 24, 2013.

Wetzel, Thomas. Interview by Sarah White. In person. Fort Meade, Maryland. September 24, 2018.

White, Randall L. "Command and Control Structures for Space and Information Operations in a Joint Command." Masters Thesis, Air Command and Staff College, 2002.

Whiton, Winsor. Interview by Sarah White. Phone call. Fort Montgomery, New York. January 8, 2019.

Williams, Brad. "Meet the Scholar Challenging the Cyber Deterrence Paradigm." Fifth Domain, July 29, 2017. https://www.fifthdomain.com/home/2017/07/19/meet-the-scholar-challenging-the-cyber-deterrence-paradigm/.

Williams, Lauren C. "Air Force to Roll Out New Cyber Job Categories." FCW, April 3, 2019. https://fcw.com/articles/2019/04/03/usaf-cyber-job-categories.aspx?fbclid=IwAR2fEh2Cce71RfDPItFIr54YFvZcNsOE1VCFIHKLx3Hi6YBLE_FIObRq1A.

Williams, Paul D. "USAF Cyber Capability Development: A Vision for Future Cyber Warfare & A Concept for Education of Cyberspace Leaders." Thesis, Air University, 2009.

Wilson, Burke E. Interview by Sarah White. In person. Washington, D.C. September 28, 2018.

Wingo, Joseph, Stacie Rembold, Cully Patch, Scott Anderson, Preston Iverson, Jeremy Solmonson, Elbert Peak, Thomas Asojo. "Revamping the Cyberspace Professional Training Model — The Weapon System Construct." *Cyber Compendium: Professional Continuing Education Course Papers* Vol 2 Issue 1 (Spring 2015): 26-33.

Winnefield, James A. "Why Sailors Are Different." *Proceedings* Issue 121 (May 1995).

Winton, Harold R. "On Military Change," in *The Challenge of Military Change.* Edited by David R. Mets and Harold R. Winton.

Wolters, Timothy S. *Information at Sea: Shipboard Command and Control in the U.S. Navy, from Mobile Bay to Okinawa.* Baltimore: Johns Hopkins University Press, 2013.

Wylie, Joseph Caldwell. *Military Strategy: A General Theory of Power Control.* Naval Institute Press, 1989.

Wynne, Michael W. and T. Michael Moseley. Air Force Document (AFD) 111003-050. "Letter to the Airmen of the United States Air Force." December 7, 2005.

Wynne, Michael W. Interview by Sarah White. Phone call. Fort Montgomery, New York. August 28, 2018.

Yannakogeorgos, Panayotis A. and John P. Geis II. *The Human Side of Cyber Conflict: Organizing, Training, and Equipping the Air Force Cyber Workforce.* Maxwell Air Force Base, AL: Air University Press, 2016.

____. Interview by Sarah White. Phone call. Washington, D.C. September 26, 2018.

"You Can Lead, But Can You Fight? Leadership as a Conduit to the Real Mission." The Company Leader. February 21, 2019. https://companyleader.themilitaryleader.com/2019/02/21/you-can-lead-but-can-you-fight/?fbclid=IwAR2RJykTMmOZ7CYo1pqjW5XZXs4YUYgti6vAYte9q7IWO-YF9PDbaRjtr2s.

Young, Zach. "Cyber Report — Full Unified Draft with Footnotes." August 21, 2013.

Zetter, Kim. "The Return of the Worm that Ate the Pentagon." *Wired*, December 9, 2011.

____. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York: Broadway Books, 2015.

Zimmerman, R., Jackson, K., Lander, N., Roberts, C., Madden, D., Orrie, R. "Movement and Maneuver: Culture and Competition for Influence Among the U.S. Military Services." Santa Monica, CA: RAND Corporation, 2019.

Zirkle, Daryk. Interview by Sarah White. In person. National Defense University, Washington, D.C. September 26, 2018.

Zirkle, Robert Allen. "Communities Rule: Intra-Service Politics in the United States Army." PhD Dissertation, Massachusetts Institute of Technology, 2008.

Zisk, Kimberly Marten. *Engaging the Enemy: Organization Theory and Soviet Military Innovation 1955-1991.* Princeton: Princeton University Press, 1993.

Zraket, Charles A. and Stanley E. Rose. "The Impact of Command, Control and Communications Technology on Air Warfare." *Air University Review* Vol 29 No 1 (Nov-Dec 1977): 82-97.

Zschirnt, Hans H. "Research in Computer Sciences." *Air University Review* Vol 16 No 1 (Nov-Dec 1964): 47-67.