2020

Ten Years In: Implementing Strategic Approaches to Cyberspace

Jacquelyn G. Schneider

Emily O. Goldman

Michael Warner

Paul M. Nakasone
U.S. Army

Chris C. Demchak

See next page for additional authors

Authors

Jacquelyn G. Schneider, Emily O. Goldman, Michael Warner, Paul M. Nakasone, Chris C. Demchak, Nancy A. Norton, Joshua Rovner, Timothy D. Haugh, William R. Garvey, Erika E. Volvino, Ryan R. Lemmerman, Erica D. Borghard, Shawn W. Lonergan, Timothy J. White, Paul Stanton, Michael Tilton, Peter Dombrowski, and Nina Kollars

NAVAL WAR COLLEGE NEWPORT PAPERS 45

Ten Years In

Implementing Strategic Approaches to Cyberspace

Jacquelyn G. Schneider, Emily O. Goldman,
and Michael Warner, Editors

Ten Years In

Newport Paper No. 45

The Newport Papers are extended research projects that the Director, the Dean of Naval Warfare Studies, and the President of the Naval War College consider of particular interest to policy makers, scholars, and analysts.

The views expressed in the Newport Papers are those of the authors and do not necessarily reflect the opinions of the U.S. Naval War College or the Department of the Navy.

Correspondence concerning the Newport Papers may be addressed to the Director of the Naval War College Press. To request additional copies, back copies, or subscriptions to the series, please either write the President (Code 32S), U.S. Naval War College, 686 Cushing Road, Newport, RI 02841, or contact the Press staff at the telephone, fax, or e-mail addresses given.

U.S. Naval War College
686 Cushing Road
Newport, Rhode Island 02841
https://usnwc.edu

Ten Years In

Implementing Strategic Approaches to Cyberspace

Jacquelyn G. Schneider, Emily O. Goldman,
and Michael Warner, Editors

NAVAL WAR COLLEGE PRESS

Naval War College Press
Newport 02841
Published 2020
Printed in the United States of America

ISSN 1544-6824

ISBN 978-1-935352-73-0 (paperback)

The logo of the U.S. Naval War College authenticates Newport Paper No. 45, *Ten Years In: Implementing Strategic Approaches to Cyberspace,* edited by Jacquelyn G. Schneider, Emily O. Goldman, and Michael Warner, ISBN 978-1-935352-73-0 (paperback), as the official U.S. Naval War College edition of this publication. Use of the U.S. Naval War College logo and ISBN 978-1-935352-73-0 is strictly prohibited without the express written permission of the Editor (or Editor's designee), Naval War College Press.

Naval War College Press
Code 32
686 Cushing Road
Newport, Rhode Island 02841

401.841.2236 telephone
401.841.1071 fax
DSN exchange: 841
press@usnwc.edu

https://usnwc.edu/nwcpress

Contents

Foreword

This book represents a look beyond theories and analogies to examine the challenges of strategy implementation. In the essays that follow, practitioners who are building cyberspace forces at-scale join scholars who study power and force in this new domain to collectively offer a unique perspective on the evolution and future of cyber strategy and operations.

The co-editors of *Ten Years In* compiled it in the tenth year of operations for U.S. Cyber Command. During that decade, the Command worked with the Services and the Coast Guard to build seven component commands, attained unified combatant command status, and matured the Cyber Mission Force's 133 teams. For the Department of Defense cyber enterprise, it has been a decade of operational learning and doctrinal development, culminating in the *DoD Cyber Strategy,* the *U.S. Cyber Command Vision to Achieve and Maintain Cyberspace Superiority,* and the revision of Joint Publication 3-12, *Cyberspace Operations*.

Yet threats to our nation evolved and diversified over this decade as great-power competition spread to cyberspace and intruded on diplomatic relations below the threshold of armed conflict. Such threats now include state-sponsored theft of U.S. intellectual property and personally identifiable information, intrusions in critical infrastructure, and campaigns to influence and intimidate democratic institutions around the world. Cyberspace capabilities are now being integrated with all instruments of national power, to include conventional military operations and information warfare.

The chapters to follow cover opportunities and challenges associated with implementing the principles articulated in national and military strategic guidance. These analyses offer historical perspective on cyber conflict, chart organizational developments, and reflect on challenges such as public-private relationships, manpower and talent, readiness and capabilities, and evolving authorities. In addition, this volume looks to the future with several reflections by promising cyberspace scholars and leaders in the Department of Defense and academia.

I think readers will agree that this volume points to a maturation of cyberspace practice in the Department of Defense. Ten years ago U.S. Cyber Command began the transition from an idea to an institution to the persistent implementation of approaches to safeguard the Department of Defense's Information Networks, to support Joint Force commanders, and to defend the nation from cyberspace threats of strategic

consequence. This volume expands on previous strategic thought to suggest ways in which an emerging cyberspace strategy can be executed to its full potential.

The partnership between the Naval War College's Cyber and Innovation Policy Institute and U.S. Cyber Command represented in this volume illustrates the role that professional military education plays in bridging gaps between practice and scholarship. *Ten Years In* should demonstrate how the Joint Force can profit from the expertise sustained by its professional military education enterprise as well as from the timely knowledge of those confronting the immediate challenges facing the Department of Defense.

General PAUL M. NAKASONE
U.S. Army
Commander, U.S. Cyber Command /
Director, National Security Agency / Chief,
Central Security Service

Preface

Three years have passed since the U.S. *National Security Strategy* called the contest for power a central continuity in history and warned that "the revisionist powers of China and Russia" are "competing against the United States and our allies and partners." In implementing this new national strategy, the *National Defense Strategy* then pivoted its focus from terrorism to long-term, strategic competition and turned to face a new geostrategic and economic competitor in China.

Cyberspace is a key arena in strategic competition, and cybersecurity represents a significant challenge that the United States must address if the *National Security Strategy* is to succeed. China engages in intellectual property theft at scale and uses predatory practices to overcome Western advantages in technology. Russia employs disruptive campaigns to undermine democratic institutions, sow discord in the West, and erode alliance cohesion. Both governments engage in strategic cyber campaigns to defend their regimes and to decrease American power and influence. Their approaches differ, but both view cyberspace as a venue in great-power competition through which they can impair the sources of American power without engaging in armed conflict. What once required a physical invasion to achieve is now being accomplished through continuous campaigns waged in and through cyberspace.

The Department of Defense (DOD) has recognized these trends and shifted from a "be prepared" posture to one of active engagement. The shift, which is still ongoing, reflects a ten-year evolution of DOD cyber capabilities, institutions, and strategies since the creation of U.S. Cyber Command in 2010. The U.S. strategic approach to cyberspace conflict in the years immediately after 2010 applied a "deterrence strategy," conducting the least cyber action necessary to mitigate threats while prioritizing network defense and law enforcement as preferred courses of action. A strategic inflection point came in 2013, however, with more-capable adversaries more boldly operating against corporate and government systems, stealing intellectual property and personally identifiable information at scale, and targeting critical infrastructure. Where once espionage and exploitation had been our major concerns, the shift to disruptions (e.g., the 2012–13 distributed denial-of-service attacks conducted by the Iranians against financial networks in New York), destructive attacks (e.g., the 2014 data-deletion attack by the Iranians against the parent company of a closed U.S. casino and the North Korean attack against Sony Pictures), and corrosive undermining of our democratic institutions (e.g., Russian attempts to influence the 2016 election) represented a crisis for U.S. cyber strategy. By 2016, it was

clear that a deterrence-focused strategy was not stopping attacks below the threshold of armed conflict. Adversaries had found ways to cause effects and exploit our information systems without crossing the "use of armed force" threshold. In short, they had learned to minimize risk to themselves while reaping the gains of their cyber tactics.

U.S. Cyber Command gained experience during the counter-ISIS fight in 2016 and, along with many observers inside and outside the U.S. government, recognized a need for a more active approach to state-sponsored malicious cyber activities. Such an approach guided the command's *Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. Cyber Command* (2018). The cyberspace operational domain, according to the *Vision,* requires a strategy of "persistent engagement"—a use of cyber capabilities in continuous contact with adversaries to generate tactical, operational, and strategic initiative (and thus set the conditions of security in our favor in a constantly changing domain). Gen. Paul Nakasone, Commander, U.S. Cyber Command, has described this pivot from a "response force" to a "persistence force": "USCYBERCOM initially focused on defending DOD networks," he has noted, "executing counterterrorism operations, planning to support conventional forces in crisis scenarios, and maintaining capacity to respond to an 'attack of significant consequence' against our critical infrastructure." The initial "response force" concept—holding forces in reserve for war and responding to attacks after the fact—had proved no match for increasingly capable adversaries operating continuously below the threshold of armed conflict against our critical infrastructure, government networks, defense industries, and private systems.

As we look into the 2020s, therefore, we see a U.S. military that has worked hard at maturation in cyberspace and is now moving into the next decade with a new mandate and strategic guidance. The generation of strategy, however, is only an early step in addressing the challenge of cyber threats in the new decade. How the Department of Defense implements this strategy—how it organizes its forces, readies and manages its talent, plans and conducts operations, develops capabilities, strengthens its partnerships, and uses its new authorities—will determine whether this strategic pivot succeeds. This collection of essays offers an introduction to the evolution of U.S. Cyber Command's strategic approach, an evaluation of the operational requirements for implementing cyberspace strategy, and finally an appraisal of the challenges and opportunities for sustaining success. The authors represent a range of perspectives—those of practitioners currently implementing the strategy, of scholars surveying its history and likely futures, and finally of experts in appraising its implementation in terms of innovation and effectiveness. The result is an informal but informed progress report on that implementation, including some usually neglected but crucial aspects of institutional maturation and success, such as readiness, measures of effectiveness, sustainability, and innovation. As the old saying goes, "Amateurs study tactics; professionals study logistics."

Our volume begins with a strategic overview that illuminates the genesis of the current strategy and vision as well as the evolution of cyber competition. Michael Warner provides a brief history of cyber conflict and concludes that all armed conflicts today have a cyber dimension. Emily Goldman traces the emergence and ascendance of persistent engagement as a new paradigm for cyberspace. Chris Demchak reveals how competition between states has become "cybered conflict"—with existential implications for the survival of democratic societies.

In the following section, essays tackle challenges to strategic implementation at the operational level. Vice Adm. Nancy Norton and her team describe advances in cyber defense. Joshua Rovner examines the role of offensive cyberspace operations in warfighting. Lt. Gen. Timothy Haugh and his team describe the growing importance of the "defend the nation" mission. Erica Borghard and Shawn Lonergan offer recommendations to buttress public-private partnerships in great-power competition.

The final set of essays addresses the sustainment of cyber operations, including manning, readiness, and technological innovation. Vice Adm. Timothy White (USN, Ret.) describes the emergence of a joint operational cyber culture. Jacquelyn Schneider examines the challenges of recruiting cyber talent. Brig. Gen. Paul Stanton and Lt. Col. Michael Tilton describe how U.S. Cyber Command is defining and measuring the readiness of cyber forces. Peter Dombrowski and Nina Kollars examine innovation in cyber capabilities.

Together these essays explain how the Department of Defense and U.S. Cyber Command are implementing changes in cyber strategy. They provide an informative glimpse for security scholars into the challenges that military institutions face in realizing a strategic vision, adding a valuable perspective to the literature on military effectiveness. Finally, the essays offer lessons from history and studies of military effectiveness that can help practitioners understand when and how some military institutions do better at implementing strategies. We hope this volume can help guide cyberspace thought and practice in the United States (and beyond) by documenting a significant example of military innovation at a turning point in international relations.

JACQUELYN G. SCHNEIDER
EMILY O. GOLDMAN
MICHAEL WARNER

Introduction
A Cyber Force for Persistent Operations

PAUL M. NAKASONE

Harvard's Samuel Huntington, then just 27, asked the U.S. Navy in 1954, "What function do you perform which obligates society to assume responsibility for your maintenance?" His seminal article in the U.S. Naval Institute's *Proceedings* argued that the basis of a military Service—or any military element—is its purpose or role in implementing national policy. Huntington called this a Service's "strategic concept," which justifies public support by explaining how, when, and where that military arm expects to protect the Nation.[1]

Huntington's question resonated because the Navy faced a crisis of purpose after World War II. It had helped win the biggest conflict in history, but the Allied victory over the Axis powers was so sweeping that by 1954 the Navy had no viable rivals left to fight at sea. The Navy's longstanding strategic concept as the Nation's first line of defense no longer seemed compelling. In addition, the prospect of nuclear war had shaken strategic assumptions and was reshaping American foreign and defense policies. While no enemies could reach America's shores from the oceans, one adversary—the Soviet Union—could devastate the country from the skies with hydrogen bombs. The Navy's traditional "oceanic" orientation, which had justified powerful fleets, seemingly had little relevance for the application of American power against nuclear-armed land powers in Eurasia.

The Navy subsequently developed a "transoceanic" strategic concept, orienting the Service away from contesting the oceans and toward projecting power across them to distant land masses. In adapting its strategic concept to reflect changes in threats and national policy, the Navy ensured public confidence and support from Congress. The Navy's new strategic role endured through the Cold War, helping the United States maintain the forces that contained Soviet power and ensuring that America (with its

allies) was so strong at sea that Moscow never seriously contemplated building fleets to rival ours.[2]

When our nation asks, "What function does U.S. Cyber Command (USCYBERCOM) perform that obligates society to assume responsibility for its maintenance?" the command can reply that its strategic concept has evolved from a "response force" to a "persistence force." This persistence force will contest our adversaries' efforts in cyberspace to harm Americans and American interests. It will degrade the infrastructure and other resources that enable our adversaries to fight in cyberspace. Over time, a persistence force, operating at scale with U.S. and foreign partners, should raise the costs that our adversaries incur from hacking the United States. To protect our most critical public and private institutions from threats that continue to evolve in cyberspace, we cannot operate episodically.

While we cannot ignore vital cyber defense missions, we must take this fight to the enemy, just as we do in other aspects of conflict. A persistence force has a much higher chance of disrupting adversary plots and protecting Americans, compared with a force that is confined to sporadic reconnaissance. Persistence should not be mistaken for engagement for engagement's sake; instead, it is an approach that empowers U.S. cyber forces to achieve more decisive results in pursuit of objectives set by national leaders. This evolution aligns USCYBERCOM with changes in the strategic environment and in national policy as articulated in the 2017 National Security Strategy and 2018 National Defense Strategy.

Cyberspace and Great Power Competition

The growth of a global, interconnected cyberspace domain represents the biggest strategic development since 9/11. Activities and operations in, through, and from cyberspace now offer states the means to augment their power, degrade or usurp the power of others, and gain strategic advantage through competition *without triggering armed conflict*. Our adversaries have learned this and are leveraging it against us.

When cyberspace went global in the 1990s, its fundamentals seemed to align comfortably with Western values. For this reason, its acceleration of social interaction, economic exchange, scientific progress, and military operations proved troubling to dictators who worried that their hold on power would be undermined by digital-age capabilities empowering civil society. The Arab Spring in 2011 heightened these fears. In response, increasingly cyber-capable governments escalated their operations against their own citizens and ours. They mounted global surveillance of opposing views and are stealing unprecedented quantities of intellectual property and personal data, disrupting democratic processes, holding critical infrastructure at risk, and eroding U.S. power. They

employ technical activities that are individually inconsequential, yet cumulatively set the conditions for decisive advantage in conflict should it occur.

The return of great power competition prompted the authors of the new National Security Strategy to lament that while Americans "took [their] political, economic, and military advantages for granted, other actors steadily implemented their long-term plans to challenge America and to advance agendas opposed to the United States, [its] allies, and our partners." Growing political, economic, and military competitions around the world, according to the National Defense Strategy, are now the central challenge to U.S. security and prosperity. In these competitions, the locus of struggle for power has shifted toward cyberspace, and from open conflict to competitions below the level of armed attack.

Original Concept

USCYBERCOM began operations in 2010 when exploitation and disruption comprised the major cyber threats to Department of Defense (DOD) information networks and the Nation's critical infrastructure. Even though the United States had enjoyed general superiority in cyberspace since the creation of the domain, our competitors had developed and acquired effective, if often rudimentary, capabilities as well. The command's mission was to maintain U.S. superiority by checking the capability development of our competitors. USCYBERCOM initially focused on defending DOD networks and supporting geographic combatant commanders, particularly in Iraq and Afghanistan. USCYBERCOM was thus a *response* force—executing counterterrorism operations, planning to support conventional forces in crisis scenarios, and maintaining capacity to respond to an "attack of significant consequence" against our critical infrastructure.

In 2013, a year that marked a strategic inflection point and the obsolescence of that original strategic concept, surprisingly capable adversaries now operated continuously against critical infrastructure, government networks, defense industries, and academia—both in America and abroad. Cyber-enabled intellectual property theft had long been common, but now state-sponsored malicious activities began to impose significant costs on the Federal Government and private sector. The adversaries mounting these campaigns took care to operate in ways that would not trigger an armed U.S. response. Examples of their assaults included the Iranian denial-of-service attacks against the financial sector (2012–2013) and attack on the Sands Casino (2014), North Korea's attack on Sony Pictures Entertainment (2014), and China's disruption of GitHub (2015) and theft of security-related data from the Office of Personnel Management (2015). Russia raised cyberspace campaigns to a new level of boldness after 2015, launching a series of operations to interfere with the elections of the United States and its allies and sponsoring attacks on the Ukrainian power grid. These campaigns convinced even skeptics that

cyberspace activities over time could cumulatively erode a country's sources of national power.

Today peer- and near-peer competitors operate continuously against us in cyberspace. These activities are not isolated hacks or incidents, but strategic campaigns. Cyberspace provides our adversaries with new ways to mount continuous, nonviolent operations that produce cumulative, strategic impacts by eroding U.S. military, economic, and political power without reaching a threshold that triggers an armed response. In other words, shifts in the global distribution of power can now occur without armed conflict. Hence the strategic concept of a response force—in effect, holding U.S. cyber forces in reserve for kinetic conflicts or responding after-the-fact to cyber attacks on America—resembles the Navy's pre-1945 strategic concept that Huntington critiqued. Worse still, it has had the effect of ceding the strategic initiative in cyberspace to adversaries willing to operate continuously against us. Continuous action in cyberspace for strategic effect has become the norm, and thus the command requires a new strategic concept.

A Cyber Persistence Force

We are learning how cyber capabilities can be employed to advance what the 2018 National Defense Strategy calls our "competition and wartime missions." Our adversaries are learning too, integrating and employing cyberspace capabilities in different ways consistent with their doctrine, strategy, organizational culture, and risk tolerance. History cautions that we should expect the use of new capabilities to evolve as they are introduced in conflicts. Tanks, for instance, developed from infantry support to deep penetration roles, while aircraft progressed from tactical reconnaissance to strategic bombing to unmanned intelligence, surveillance, and reconnaissance. With battlefield experience comes the evolution and maturation of operational concepts and strategic insights. Carl von Clausewitz noted that the "knowledge basic to the art of war is empirical," meaning theory must conform to experience.[3] USCYBERCOM has learned that successful engagement against adversaries in cyberspace requires that we continuously seek tactical, operational, and strategic initiative. Such persistence requires that we remain ahead of them both in knowledge and in action. It also demands that we leverage our strengths across intelligence and operations to achieve this end.

In March 2018, USCYBERCOM's command vision document, *Achieve and Maintain Cyberspace Superiority,* updated the command's strategic concept to align with changes in national strategy and in the cyberspace competition.[4] The document acknowledges that the locus of struggle in the revived great-power competition has shifted toward cyberspace and that decisive action can occur below the level of armed attack. Its strategic concept is "cyber persistence" rather than "cyber response," empowering

USCYBERCOM to compete with and contest adversaries globally, continuously, and at scale, engaging more effectively in the strategic competition that is already under way.

USCYBERCOM's strategic thinking is evolving along with our forces and capabilities. We are accelerating change in the following ways:

- We are shifting our strategic perspective away from viewing war and territorial aggression as the only perils for our national sources of power. A byproduct of successfully deterring conventional and nuclear war is that adversaries now shape America's policy choices through cyberspace operations calibrated to avoid provoking armed responses. Because our adversaries still feel able to operate against the United States and its interests through cyberspace, and because historically there has been little cost imposed for doing so, USCYBERCOM must operate below traditional use-of-force thresholds while also preparing to be a lethal force in conflict.
- We are building relationships with U.S. institutions that are likely to be targets of foreign hacking campaigns—particularly in the Nation's critical infrastructure—before crises develop, replacing transactional relationships with continuous operational collaboration among other departments, agencies, and the private sector. These relationships are crucial to thwarting attackers before they strike and to increasing resilience after a successful breach. Ideally, these partnerships will allow our persistence force to address patterns of malicious cyber behavior before they become attacks.
- We must "defend forward" in cyberspace, as we do in the physical domains. Our naval forces do not defend by staying in port, and our airpower does not remain at airfields. They patrol the seas and skies to ensure they are positioned to defend our country before our borders are crossed. The same logic applies in cyberspace. Persistent engagement of our adversaries in cyberspace cannot be successful if our actions are limited to DOD networks. To defend critical military and national interests, our forces must operate against our enemies on their virtual territory as well. Shifting from a response outlook to a persistence force that defends forward moves our cyber capabilities out of their virtual garrisons, adopting a posture that matches the cyberspace operational environment.
- We have shifted away from the earlier emphasis on holding targets "at risk" for operations at a time and place of our choosing. We will operate continuously to present our decisionmakers with up-to-date options. Cyberspace targets themselves typically amount to computer and data "states," which change constantly in the normal functioning of digital information systems. Successful operations require capabilities and tactics that can rapidly shift from unsuccessful approaches in order to exploit new vulnerabilities and opportunities.

- Finally, we are ensuring our capabilities, operational tempo, decision-making processes, and authorities enable continuous, persistent operations. Adversaries and competitors have responded to our restrained and episodic engagement with cyber aggression that has eroded U.S. military, economic, and diplomatic advantages. Strategic effects in cyberspace come from the use—not the mere possession—of cyber capabilities to gain the initiative over those who mean us harm.

The Value of the Cyber Force

Senior political and military leaders recognize that our military must be able to compete below the level of armed conflict, and this idea is clearly stated in the National Security Strategy: "Our task is to ensure that American military superiority endures, and in combination with other elements of national power, is ready to protect Americans against sophisticated challenges to national security."[5] Nowhere is this requirement greater than in cyberspace, where peer competitors operate continuously against us in search of strategic advantage. To meet this intent, USCYBERCOM will:

- Operate forward and at scale where our adversaries are. This is the primary mission of cyber forces, which gives rise to U.S. Cyber Command's concept of defend forward. Its purpose is to limit the terrain over which the enemy can gain influence or control. We cannot afford to let adversaries breach our networks, systems, and data (intellectual property and personally identifiable information). If we are only defending in "blue space," we have failed. We must instead maneuver seamlessly across the interconnected battlespace, globally, as close as possible to adversaries and their operations, and continuously shape the battlespace to create operational advantage for us while denying the same to our adversaries.
- Assure the joint force can conduct operations securely and reliably. USCYBERCOM defends the DOD Information Network (DODIN), which is the command, control, communications, and data hub for the joint force. It facilitates nearly every phase of operations for the U.S. military. By defending the DODIN, USCYBERCOM has indirectly but strongly supported virtually every U.S. military operation launched since 2010. DOD relies on an increasingly secure and resilient information network to meet its full range of warfighting and enabling functions *because of past and ongoing USCYBERCOM operations.*

Enabling Capabilities for a Persistence Force

We are at a transformational moment for U.S. strategy and operations in cyberspace. Cyberspace represents a new strategic environment through which relative power can be challenged without resorting to armed conflict. Senior political and military leaders recognize that the initial approach that DOD took toward cyberspace aggression—focusing

on resiliency and response actions—in effect committed the fundamental flaw in military operations of holding one's forces in reserve past the point of decision.

Huntington identifies two other important factors that determine the success of a strategic concept: the resources, both human and material, required to implement it, and the organizational structure, which groups the resources allocated by society in a manner that implements the strategic concept. USCYBERCOM is maturing as a combatant command with the teams, infrastructure, tools, accesses, and authorities ready to execute missions. The command is also transitioning from force generation to a sustained readiness approach for persistent engagement with cyber adversaries and increased lethality in war. We continue to evolve the organization based on operational experience, task organizing, and employing small elements of teams in ways never anticipated when we stood them up.

One last factor that is crucial to success of a military element's strategic concept, which Huntington implied in his 1954 essay, is the ability of the commanders and the force itself to instill a sense of confidence among civilian leaders and the larger public that the element has devised an appropriate and viable strategic concept and has the skills to execute it on behalf of the Nation. The actions that follow from the strategic concept of persistent engagement should, over time, allow USCYBERCOM to install that sense of confidence.

Notes

This article was originally published in *Joint Force Quarterly* 92 (1st Quarter 2019), pp. 10–14, and appears by courtesy of the editors.

1. Samuel P. Huntington, "National Policy and the Transoceanic Navy," U.S. Naval Institute *Proceedings* 80, no. 5 (May 1954).
2. The Soviets had built a powerful navy by the 1980s, but they used it to control their local seas and protect their strategic missile submarines—not to contest control of the Atlantic or Pacific.
3. Carl von Clausewitz, *On War,* ed. and trans. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1976), 170.
4. *Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. Cyber Command* (Washington, DC: U.S. Cyber Command, March 2018).
5. *National Security Strategy of the United States of America* (Washington, DC: The White House, December 2017), 3.

List of Acronyms and Abbreviations

A	**ADCON**	administrative control
	AI	artificial intelligence
	APT	advanced persistent threat
C	**CCMD**	[regional] combatant command
	CCORI	Command Cyberspace Operations Readiness Inspection
	CCP	Chinese Communist Party
	CCRI	Command Cyberspace Readiness Inspection
	CERT	computer emergency readiness team
	CFCOE	Cyber Forces Concept of Employment
	CIKR	critical infrastructure and key resources
	CIO	chief information officer
	CIPI	Cyber and Innovation Policy Institute [Naval War College]
	CISA	Cyber and Infrastructure Security Agency
	CMF	Cyber Mission Force
	CNMF	Cyber National Mission Force
	CNMF-HQ	Cyber National Mission Force Headquarters
	CNO	Chief of Naval Operations
	COF	cyberspace operations forces
	CO-IPE	cyberspace operations–integrated planning element
	CORA	cyber operational resilience alliance
	COTS	commercial off-the-shelf
	CSD	Cybersecurity Directorate

D	**DDoS**	distributed denial-of-service
	DHS	Department of Homeland Security
	DIB	defense industrial base
	DISA	Defense Information Systems Agency
	DIU	Defense Innovation Unit
	DOD	Department of Defense
	DODD	Department of Defense Directive
	DODIN	Department of Defense Information Network
F	**FBI**	Federal Bureau of Investigation
	FOC	full operational capability
	FSARC	Financial Systemic Analysis & Resilience Center
	FY	fiscal year
I	**I&W**	indications and warning
	IC	intelligence community
	ICT	information and communications technology
	IOC	initial operational capability
	IP	intellectual property
	(ISC)²	International Information System Security Certification Consortium
	ISIS	Islamic State in Iraq and Syria
	IT	information technology
	IT-RMA	information technology revolution in military affairs
	IW	information warfare
J	**JCS**	U.S. Joint Chiefs of Staff
	JDOC	JFHQ-DODIN Operations Center
	JFCC-NW	Joint Functional Component Command for Network Warfare

	JFHQ	Joint Force Headquarters
	JFHQ-C	Joint Force Headquarters–Cyber
	JFHQ-DODIN	Joint Force Headquarters–Department of Defense Information Network
	JP	Joint Publication
M	**MET**	mission-essential task
N	**NATO**	North Atlantic Treaty Organization
	NDAA	National Defense Authorization Act
	NDISAC	National Defense Information Sharing and Analysis Center
	NSA	National Security Agency
	NSDD	National Security Decision Directive
	NSIB	national security innovation base
O	**OCO**	offensive cyberspace operation(s)
	OECD	Organisation for Economic Co-operation and Development
P	**PLA**	People's Liberation Army
R	**R&D**	research and development
	ROE	rules of engagement
S	**SIGINT**	signals intelligence
	SMS	*Science of Military Strategy* [PLA]
	STEM	science, technology, engineering, and mathematics
	STES	socio-technical-economic system
T	**TTP [singular]**	tactics, techniques, and procedures [plural]
U	**UCP**	Unified Command Plan

USCENTCOM	U.S. Central Command
USCYBERCOM	U.S. Cyber Command
USSTRATCOM	U.S. Strategic Command

CHAPTER ONE

A Brief History of Cyber Conflict

MICHAEL WARNER

"Cyber war" has become a redundant term. Conflict today always has a cyber dimension, with actors on one or both sides either conducting cyberspace operations or using cyber means against their adversaries. Offensive operations "in" and "through" cyberspace are now becoming routine. This routinization, however, does not make offensive cyberspace operations insignificant, still less benign. In recent years it has become possible to cause strategic effects using cyber means both in combat and in competition below the threshold of armed conflict.

Conflict in cyberspace has been an interactive dynamic from its inception. The same can be said about the history of war in general, and thus no armed struggle should be interpreted solely from the perspective of any particular actor, even if one (e.g., the United States) played a starring role in the drama. This is a story that stretches back decades and is still being written today. It is also a complicated story, one that can barely be outlined here, because any mere article can hardly detail even the incidents and actors that have mattered most. Indeed, many of the pertinent decisions and capabilities remain classified information in various capitals. Attempts to sort the mass of media articles, official reports, and memoirs into historically meaningful patterns began a decade ago, but even these were quickly overcome by events and new trends.[1]

The observations that follow seek to chart the milestones that states and cyber actors passed in their parallel paths toward, first, recognizing that cyberspace operations can hold strategic importance and, then, acting to cause (or prevent) such outcomes. While other readings of the history of cyber conflict are certainly possible and needed, this one in particular makes sense of the main trends and suggests paths for future scholarship on the historical and potential strategic implications of offensive cyberspace operations.

In the Beginning Was Information War

The origin of cyberspace as an avenue or means for conflict and competition links to the complicated concept of "information war." A brief look at military history over the last

century clarifies this context. Military operations have had an "information" component at least since it became possible (in World War I) to control forces on a battlefield in real time and beyond line of sight. In that sense, all armed conflict is now information war. Pentagon consultant Thomas Rona in 1976 helped explain what that means. He noted the growing complexity of Cold War weapon systems and explained that with it came the "need to integrate the many sophisticated subsystems [that had] vastly increased the information flow with the weapon system envelope." The performance of all those systems now depended "upon the external information flow" among a weapon, its commander, related sensors, navigation references, and the target itself. This flow could be disrupted, Rona prophesied, and thus the force that could protect its own information flow—and impair its foe's—would gain a potent advantage. Rona forecast that "improvements in information war" would overshadow even the advantages gained from refining the speed, accuracy, and lethality of the actual weapon systems.[2]

What Rona did not yet see was that this military "information flow" would soon become predominantly *digitized*. The information vital to weapon systems' functioning would spend much of its life cycle as data being processed by automatic electronic systems and by programs dependent on still other, externally furnished, data and programs. The provision of data and programs, moreover, would shortly become highly networked, employing global communications links and ubiquitous routing protocols. In short, modern weapons and the people building, deploying, and controlling them would function partly in cyberspace.

Rona's information war, once cyberized, could thus take place both in armed conflict and in normal, albeit coercive, statecraft. And it would proceed with, through, and against *algorithms*—the logical sequences that collect, sort, transmit, and increasingly interpret the cataracts of data that our digital lives now generate. Those algorithms have always controlled far more than weapon systems. And because algorithms can be attacked by other algorithms, a state or an actor seeking to exploit or impair an adversary's "information flow" around its military, political, or economic systems need not employ violent means to do so—and thus need not wage or risk war to exert force, coerce a victim, or plunder another state's wealth.

Those algorithms in their automatic functioning normally do their work in ways that are largely outside human observation, which means their human controllers must invest in them high degrees of implicit faith. That trust itself would also become a military and political target. Adversaries have always tried to confuse one another—and deception, of course, is de rigueur in international politics. Cyberspace, however, gives adversaries an ability to attack trust indirectly by directly compromising the technical means by which foes communicate and manage data.

Dawning Worries

The term "cyberspace" dates from William Gibson's science-fiction thriller *Neuromancer* (1984). Computer pioneers, of course, had glimpsed flashes of the cyber future years before this dystopian classic. A few prophets found opportunities for mischief with computers in the 1960s. Their pranks were private, however, notwithstanding the various sums stolen by computer-room insiders and the earliest online criminals (usually "phreaks" seeking free long-distance calls on time-shared data connections). Even in the 1970s these activities typically wasted relatively little money or time for corporations and consumers, partly by making it harder for them to connect or to trust in the security and privacy of their data.[3]

Cyberspace became a military matter—as opposed to a security concern—as two trends converged. First, governments and institutions began storing and moving wealth and secrets in the form of digital data in and among networked computers having international connections. Second, those same enterprises began *maneuvering* to protect their secrets and wealth against opponents who wanted to steal or impair them.[4]

These trends intersected in the United States, with its large military and government sectors and its leading computer and telecommunications industries. Recognition of their convergence coincidentally came the same year as the publication of *Neuromancer.* President Ronald Reagan in 1984 issued National Security Decision Directive (NSDD) 145 to mitigate the national security implications of the blurring of "traditional distinctions between telecommunications and automated information systems."[5] This convergence held great promise but also created risks for America, said NSDD-145, because "government systems as well as those which process the private or proprietary information of US persons and businesses can become targets for foreign exploitation."[6] Observers today will note that NSDD-145 described an *intelligence* threat in the passage above, warning against data loss to enemies rather than the destruction or manipulation of data and information systems. Yet officials and experts soon recognized that the implications of securing data and systems extended far beyond the precincts of corporate and personal security.

Washington had already realized that U.S. and foreign national security data could be corrupted or destroyed, with strategic effect. Academic observers publicly warned of vulnerabilities in the (precyber) nuclear command-and-control arrangements of both superpowers.[7] Such concerns spread among Department of Defense officials and computer experts, especially after a training tape mistakenly run on North American Defense Command computers in 1979 caused NORAD to alert the White House of an impending Soviet attack.[8] In addition, it is now becoming clear through various declassifications that the Department of Defense in the 1980s pondered how it might

impair Soviet command and control in wartime through means that we might now call cyber attacks.[9] Finally, concerns for the vulnerability of Western telecommunications to computer-enabled disruption increased still more with the problems caused by the Morris Worm, which in 1988 briefly crippled about 10 percent of the entire internet (which was, of course, a much smaller environment than it would soon become).[10]

The Department of Defense by this point had considered the importance of information at the tactical as well as the strategic level of war, concluding that synchronized and sustained attacks on an enemy's command, control, communications, and perceptions could disrupt his situational awareness and debilitate his battlefield performance.[11] The U.S.-led coalition's swift victory in the Persian Gulf War (1991) seemed to vindicate such thinking, and pundits accordingly dubbed it "the first information war."[12] One such observer argued the campaign had "differed fundamentally from any previous conflict" and that its outcome "turned as much on superior management of *knowledge* as it did upon performances of people or weapons."[13]

Deputy Secretary of Defense Donald Atwood drew similar conclusions in 1992, issuing Department of Defense (DOD)–wide guidance on information war just before leaving office at the close of the George H. W. Bush administration. Atwood's directive (DODD TS 3600.1) defined information warfare 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.[14]

Such thinking broke new ground by including both the opportunities and the risks of information warfare in a concept to guide strategists and planners across the joint force. Atwood's directive insisted that commanders understand information warfare's interactive dynamic. They were to be "well-versed in the trade-offs among exploitation, corruption and destruction of adversary information systems; the varying capabilities and vulnerabilities of the various elements of US information systems; and the interaction and interrelationship of the two." DODD TS 3600.1 also noted that adversaries would themselves seek to impair U.S. and allied forces; indeed, friendly forces should learn via realistic simulations to "operate successfully in degraded information and communications environments."[15]

No paradigm shift prevails without misunderstandings. Deputy Secretary Atwood's potentially pathbreaking vision of the future, ironically enough, quickly became obscured by competing ideas. In fact, it was partly eclipsed by the way in which the chairman of the Joint Chiefs of Staff, Gen. Colin Powell, directed its implementation. Chairman Powell fostered doctrine for the integration of information warfare in joint warfighting

operations in a way that significantly expanded information warfare's scope and indeed renamed it "command-and-control warfare."[16] Where Deputy Secretary Atwood's directive had contemplated the offensive and defensive sides of what we now call cyber warfare, Chairman Powell's guidance implicitly classed cyber capabilities with a range of other, noncyber and nonkinetic missions (specifically operations security, military deception, psychological operations, and electronic warfare).[17] Atwood had already left office with the change of administrations, however, so he had no say on whether this expansion of "information warfare" met his intent.

Chairman Powell's guidance would have more short-term influence than Deputy Secretary Atwood's on the individual services' and the combatant commands' decisions for organizing their personnel and functions. The services established separate "information warfare activities" to develop approaches to generating the full panoply of capabilities that Powell had labeled command-and-control warfare.[18] These were accompanied by new doctrine on command-and-control warfare that (following Chairman Powell) grouped computer network operations with classic psychological warfare and deception techniques (whether or not conducted in cyberspace).[19] Hence a certain confusion arose in the U.S. military and among observers of it, who naturally wondered whether "information warfare" now always or only sometimes included what were beginning to be called "computer network operations."

Perhaps the most "cyberish" reflection on this rubric appeared in the U.S. Air Force's 1995 pamphlet *Cornerstones of Information Warfare.* This paper described military cyber attacks against strategic objectives (though without using the words "cyber" or "computer"). *Cornerstones* noted how air strikes could cripple an oil refinery, for example, and then explained that similar effects could one day soon be achieved through "information" missions:

> Like all modern refineries, [our targets] have extensive automated control systems. These extensive information functions offer a potential target for information warfare. Early in the [hypothetical] conflict we performed an offensive counterinformation mission by penetrating and characterizing the refinery's automated control system. In the process, we uncovered several vulnerable information dependencies, giving us the means of affecting the refineries' operations at a time of our choosing. Later in the conflict, combined with interdiction and ground maneuvers, we choose to exploit one of the vulnerabilities. We have just disabled their refineries. This, too, is a classic example of strategic attack.[20]

At the same time, however, American experts grasped that other nations could themselves employ such "strategic information warfare" against the United States. A tabletop exercise at the RAND Corporation in early 1995 showed that America, with its "complex, interconnected control systems for such necessities as oil and gas pipelines, electric grids, etc.," had become vulnerable even to foes with inferior militaries who were nonetheless willing to utilize cyber techniques to leapfrog U.S. forces and hit America's

critical infrastructure. "In sum," RAND's report concluded, "the US homeland may no longer provide a sanctuary from outside attack."[21]

Information Operations

The prospect of strategic information warfare proved so concerning to policy makers in Washington that in 1996 they renamed it. The United States at that time enjoyed military overmatch over any potential opponent, and the administration of President William Clinton saw no call to be advertising the Pentagon's dominance in a new military field. Accordingly, "information warfare" and "command-and-control warfare" overnight became the less bellicose "information operations," in a then-classified DOD-wide directive (DODD S-3600.1). While the new directive's content was little changed from that of Chairman Powell's 1993 guidance, it did help clarify matters by adding the concept of "computer network attack," which it defined as "operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."[22] This definition became public with the Joint Staff's publication of *Joint Doctrine for Information Operations,* Joint Publication (JP) 3-13, in October 1998. The release of JP 3-13 told readers what many had already surmised: that information ~~warfare~~ operations included cyber attacks on enemy networks.[23]

A pair of regional conflicts over the next few years reinforced perceptions that the United States was perfecting strategic cyber capabilities—but not calling them such. Having created the field of information warfare and then renamed it "information operations," the United States employed it on dictators in Yugoslavia and then in Iraq. The attacks by NATO (under Operation Allied Force) on supporters of Yugoslav strongman Slobodan Milošević to force a Serbian withdrawal from Kosovo in 1999 focused on "the control system that is used to manipulate the military and security forces," said a NATO spokesman.[24] Air strikes were only part of the campaign to isolate Milošević from his henchmen, however, as President Clinton's national security advisor Samuel "Sandy" Berger publicly explained. Coalition leaders and planners, he commented just after the campaign's successful conclusion, had known that Milošević "was not immune to pressure from within." Hence the coalition had

> employed other means—enforcing tough economic sanctions; tightening travel restrictions; freezing financial holdings; making it difficult for Serbia's privileged class to go abroad, move money around, or plan their exits. . . . Such developments raised the level of anxiety and discontent within Belgrade's power circles. . . . Many around Milosevic came to see the futility—and the risks—of his intransigence.[25]

The U.S.-led coalition that invaded Iraq in 2003 seems to have employed similar information operations. Professor Richard Andres has noted that the speed, power, and precision of the coalition's offensive confronted Iraq's Saddam Hussein with cascading command dilemmas, making it impossible for him to know where to counterattack

and depriving his generals of the confidence to seize tactical advantages.[26] The coalition campaign also focused a variety of methods against the cohesion and morale of Iraq's political and military leadership, directing faxes and phone calls to Iraqi leaders and commanders in the hope of inducing defections while provoking Saddam's ruthless security services to fear coup plots everywhere. This latter measure made the restrictions on military initiative even worse.[27] Andres called the result a "top-down" collapse of Iraqi forces leading to a swift coalition conquest of Baghdad.

Potential adversaries observed the campaigns in Iraq and the Balkans and apparently drew their own conclusions about strategic information operations and computer network attacks. Actually, the offensive cyberspace capabilities the American military in fact possessed were distinctly limited, as we shall see, and the only evidence on whether and how they might have been employed in Yugoslavia and Iraq emerged in a few speculative press stories.[28] This was not, however, how foreign observers viewed the situation. Potential adversaries seemed to have assumed the worst and to have decided that "information operations" equaled secretive but strategically deadly cyber attacks capable of toppling a target regime.

New Opportunities—and Risks

The Pentagon had not long before begun a multiyear debate over how offensive cyberspace operations might be built and employed at scale in conjunction with other capabilities in the joint force. The Clinton administration had initiated this process in 2000 by merging the military's defensive cyber operators with the computer-network-attack planners in a joint task force under U.S. Space Command. Secretary of Defense Donald Rumsfeld two years later shifted the unit into the reorganized U.S. Strategic Command (USSTRATCOM). The resulting Joint Task Force–Computer Network Operations was small, with a $26 million budget and 122 positions to cover offensive and defensive operations, making it roughly the size of an infantry company in the U.S. Army. Its offensive mission was to "coordinate and, when directed, conduct computer network attack in support of combatant commanders' and national objectives."[29] In 2005 the task force's offensive cyberspace operations personnel were transferred to a new Joint Functional Component Command for Network Warfare (JFCC-NW) in USSTRATCOM. JFCC-NW's commander, Lt. Gen. Michael Hayden of the U.S. Air Force, served simultaneously as "dual-hatted" director of the National Security Agency. Despite his enthusiasm for offensive cyberspace operations, Lieutenant General Hayden later conceded that their effects by 2005 had been trivial—the equivalent of "spray painting virtual graffiti on digital subway cars."[30]

JFCC-NW's first operations, ironically, entailed not state-on-state engagements but missions in conjunction with the fight for Iraq against al-Qaeda and its local affiliates.

Concern mounted in the West as jihadists went online, using websites to proselytize and raise funds. The director of Britain's Security Service (MI5), for instance, publicly noted in 2006 that an increasing number of Britons were being radicalized "through chat rooms and websites on the Internet."[31] Jihadist online propaganda was also growing more sophisticated. Attacks on coalition forces and Iraqi troops, she explained, were "regularly videoed and the footage downloaded onto the Internet within 30 minutes" for viewing by a worldwide audience.[32] Such propaganda was not harmless; it helped prompt terror attacks in America and Europe.[33]

The question was what to do about online jihad. Gen. John Abizaid, commander of U.S. Central Command, wanted someone to strike al-Qaeda servers hosted even in neutral countries and sought "authority to operate in the internet space aggressively, because we believed that the internet space, the cyberworld, was an area that Al Qaeda was excelling in."[34] Yet the U.S. response apparently involved considerable deliberation: "It took years and very, very tough discussions" to gain approval for contesting al-Qaeda online, complained Abizaid.[35] The Joint Chiefs finally authorized "action to counter adversary use of the Internet," which eventually led to JFCC-NW, now under the command of Lt. Gen. Keith B. Alexander, U.S. Army, making several al-Qaeda websites inaccessible.[36]

The United States by then was not the only state employing cyber techniques to influence foreign actors. Massive denial-of-service attacks against Estonian cyberspace briefly crippled the government there in 2007 after the Estonians moved a Soviet-era war memorial in a gesture that Moscow deemed disrespectful; the attacks originated in Russia, although the Kremlin's role remains unclear.[37] Russian forces tangled with Georgian troops the following year over the status of two disputed provinces, and this time Russian armor and infantry benefited from synchronized attacks by nominally independent "cyber militias" against websites of Georgian government offices, news media, and banks.[38]

The evolving standards of cyber conflict soon produced something even more ominous. In 2010 independent researchers discovered and publicized a cyber weapon they dubbed "Stuxnet." The story broke in spring 2012 when David Sanger of the *New York Times* claimed that the United States and Israel had created Stuxnet to attack Iran's covert nuclear weapons program with a cyber weapon.[39] Michael Hayden, now retired, deduced the significance of this find. In his view, a state actor "had just used a weapon composed of ones and zeros, during a time of peace, to destroy what another nation could only describe as critical infrastructure. . . . Someone had crossed a Rubicon. A legion was now permanently on the other side of the river. We were in a new military age."[40]

An Unexpected Change

But what sort of military age? As noted, the U.S. military originally viewed cyberspace as a venue specifically for state-on-state conflict. We know less about what other Western forces thought about the unfolding events, but we have little evidence that their views diverged much from the American perspective. Some outside observers warned of a "cyber Pearl Harbor," while others sought to calm such fears. The evidence could be read in various ways. An academic database of cyber operations mounted between 2000 and 2016 found "272 documented cyber operations between rival states," and its compilers argued that many of those constituted cyber espionage (as opposed to disruption and degradation). That trend suggested "a restrained domain with few aggressive attacks that seek a dramatic impact," yet it might have been cold comfort to states on the receiving end of aggressive cyber attacks to know they were merely exceptions to the rule.[41]

Nor were the direct victims of targeted cyberspace operations the only ones feeling victimized by foreign activities in the cyber domain. Regimes that felt endangered by the global spread of the internet and its domination by Western interests and values viewed cyberspace as an avenue and a means for undermining that dominance. Western governments, corporations, and activists could now communicate directly via cyberspace with the populations of many dictatorships. America's new secretary of state, Hillary Clinton, described the implications of this fear in her landmark speech on internet freedom in January 2010: "Some countries have erected electronic barriers that prevent their people from accessing portions of the world's networks. They've expunged words, names, and phrases from search engine results. They have violated the privacy of citizens who engage in non-violent political speech. . . . With the spread of these restrictive practices, a new information curtain is descending across much of the world."[42]

Secretary Clinton nevertheless saw the expansion of global civil society via the internet as a key element of American foreign policy. Thus regimes seeking to shield their subjects from the internet had their efforts frustrated by the United States, Clinton later explained. Her State Department countered such restrictions by, for instance, training citizen activists under oppressive regimes to employ cyber tools that could "protect their privacy and anonymity online and thwart restrictive government firewalls." By 2011 she could write that "we had invested more than $45 million in tools to help keep dissidents safe online and trained more than five thousand activists worldwide, who turned around and trained thousands more." Clinton herself visited one of these training sessions that year in Lithuania, not far from Vladimir Putin's Russia.[43]

The watershed event for the future of cyber conflict became the Arab Spring that swept North Africa and the Middle East in 2011. Regimes that felt threatened by social media and an open internet now had to respond. They did so clumsily at first, trying to close

down internet service providers or block social media sites.[44] The smarter ones, like Iran, quickly learned to hunt on the web to find adversaries and monitor their planning. "The new technologies allow us to identify conspirators and those who are violating the law, without having to control all people individually," boasted Iran's top policeman, Esmail Ahmadi-Moghaddam, in early 2010.[45]

The possibility of an Arab Spring in Russia occurred to Gen. Valery Gerasimov, chief of the General Staff, in 2013. He saw in this a watershed in military history. Wars in the new century, he noted, "are no longer declared and, having begun, proceed according to an unfamiliar template."[46] Yet contemporary struggles are no less deadly for unready regimes, explained Gerasimov: "The experience of military conflicts—including those connected with the so-called [color] revolutions in north Africa and the Middle East—confirm that a perfectly thriving state can, in a matter of months and even days, be transformed into an arena of fierce armed conflict, become a victim of foreign intervention, and sink into a web of chaos, humanitarian catastrophe, and civil war."[47] Such crises might indeed become "typical of warfare in the 21st century." Gerasimov perceived in the Arab Spring "the use of technologies for influencing state structures and the population with the help of information networks." Such nonmilitary means of achieving strategic goals often exceeded "the power of force of weapons in their effectiveness," for such "methods of conflict" as "political, economic, informational, humanitarian, and other non-military measures" could now be "applied in coordination with the protest potential of the population."[48]

Similar reasoning appeared to guide actions of several regimes as they commenced offensive cyberspace operations to harass Western governments and corporations. Regimes that felt threatened by internet-based subversion decided to counterattack by disrupting and intimidating their real and alleged opponents online. This was a turning point, which as such could have pivoted in a different direction (i.e., toward less rather than more cyber conflict, if the affected regimes had chosen purely defensive responses to what they publicly called Western aggression). We do not yet know precisely how several dictatorships decided at around the same historical moment to begin employing cyber weapons against Western institutions, but the evidence is clear that they did.

Iranian officials, for example, vowed revenge for Stuxnet and other perceived cyber assaults on Iran's economy in spring 2012.[49] Iranian hackers in 2012 and 2013 attacked American financial companies, according to indictments of seven Iranians won by the Justice Department in March 2016: "Using botnets and other malicious computer code, the individuals—employed by two Iran-based computer companies sponsored and directed by the Iranian government—engaged in a systematic campaign of distributed denial of service (DDoS) attacks against nearly 50 institutions in the U.S. financial

sector."[50] Their coordinated attacks disabled bank websites, frustrated customers, and "collectively required tens of millions of dollars to mitigate."[51]

North Korea entered the fray the following year, attacking Sony Pictures Entertainment for releasing an otherwise forgettable satire about an assassination attempt on North Korea's dictator Kim Jong-un. Secretary of State John Kerry condemned North Korea's "cyber-attack targeting Sony Pictures Entertainment and the unacceptable threats against movie theatres and moviegoers." Kerry called the attacks "a brazen attempt by an isolated regime to suppress free speech and stifle the creative expression of artists beyond the borders of its own country."[52]

China joined in as well. In March 2015, for instance, someone attacked the website of GreatFire for hosting material that would help computer users avoid official censorship. Independent researchers at the University of Toronto's Citizen Lab found that the new weapon that had been used rested on China's so-called Great Firewall. Citizen Lab called this capability "the Great Cannon" and noted its sinister novelty: "The operational deployment of the Great Cannon represents a significant escalation in state-level information control: the normalization of widespread use of an attack tool to enforce censorship by weaponizing users. Specifically, the Cannon manipulates the traffic of 'bystander' systems outside China, silently programming their browsers to create a massive [distributed denial-of-service] attack."[53]

The most significant campaign, however, would be the Russian efforts to confuse and provoke American voters in the 2016 election. According to the indictment of thirteen Russians handed up by Special Counsel Robert Mueller's investigation in February 2018, Moscow mounted a covert campaign to get Americans arguing with one another. A Russian organization called the Internet Research Agency "as early as 2014 . . . began operations to interfere with the U.S. political system, including the 2016 U.S. presidential election," noted the indictment.[54] The Russians employed classic divide-and-conquer tactics, attacking the presidential candidates that they (along with most American experts) considered strongest while ignoring their apparently weaker challengers. Russian agents

> engaged in operations primarily intended to communicate derogatory information about Hillary Clinton, to denigrate other candidates such as Ted Cruz and Marco Rubio, and to support Bernie Sanders and then-candidate Donald Trump. . . . On or about February 10, 2016, Defendants and their co-conspirators internally circulated an outline of themes for future content to be posted to [Internet Research Agency]–controlled social media accounts. Specialists were instructed to post content that focused on "politics in the USA" and to "use any opportunity to criticize Hillary and the rest (except Sanders and Trump—we support them)."[55]

As the world saw in 2016, such targeting of individuals and societies via the "information space" could have widespread effects. Cyber campaigns backed by massive arsenals

looked formidable by 2017, but their success was not assured. Indeed, a brazen but hasty cyber campaign to sabotage candidate Emmanuel Macron in France's presidential election that spring failed, apparently in part because Macron's campaign (having watched the American elections a few months earlier) was ready for the assault.[56] This development, however, would not mean that the Russians had given up. British leaders late that year warned of Russian cyber and electoral disruption backed by powerful conventional and even nuclear forces. Prime Minister Theresa May noted that Moscow had "mounted a sustained campaign of cyber-espionage and disruption."[57] Its tactics, she claimed, "included meddling in elections and hacking the Danish Ministry of Defence and the [German] Bundestag among many others." A few days later, Ciaran Martin, chief of Britain's new National Cyber Security Centre, accused Russia of attacking Britain's media, telecommunications, and energy sectors and of "seeking to undermine the international system."[58]

War Zones

As these events unfolded, the U.S. military quietly learned to build and employ military cyberspace operations "at scale" in the Middle East in the struggle against the soi-disant Islamic State. Well before the international coalition to defeat ISIS hit its stride, the Department of Defense had created U.S. Cyber Command, which in turn was busy building its Cyber Mission Force to operate in cyberspace. Senior Defense Department leaders grew less reticent in describing its operations. Deputy Secretary Robert Work told reporters the U.S. military was dropping "cyber bombs" on ISIS in April 2016.[59]

The effort received mixed reviews. Secretary of Defense Ashton Carter discounted the initial cyberspace campaign: "I was largely disappointed in Cyber Command's effectiveness against ISIS. It never really produced any effective cyber weapons or techniques." This was not wholly the fault of USCYBERCOM, Carter added. When the command finally produced "something useful, the intelligence community tended to delay or try to prevent its use, claiming cyber operations would hinder intelligence collection"; thus "none of our agencies showed very well in the cyber fight." Secretary Carter did, however, suggest that cyberspace operations assisted the information warfare aspect of the struggle: "One exception was an international effort to combat ISIS's hateful online presence with counter-messaging, an effort that did achieve significant reach and had a real impact."[60] Gen. Joseph L. Votel, commander of U.S. Central Command, was more direct in his praise for the support his forces received:

> At the tactical level, we have integrated [cyberspace operations] and fielded cyberspace capabilities to support Special Forces and, more recently, conventional ground forces. These tactical cyberspace and [electronic warfare] capabilities are synchronized with the ground scheme of maneuver providing an additional level of force protection to the warfighter by disrupting the adversaries' ability to command and control their forces in the battlespace. During our operations to defeat ISIS, our

> first success at true multi-domain operations through synchronized lethal and non-lethal effects was against ISIS's critical media operatives; we denied key infrastructure and degraded their ability to execute external operations through social media. These operations against ISIS have informed efforts across [Central Command] as well as other Combatant Commands.[61]

General Votel's comments suggest that the proliferating accounts and debates regarding the character and results of military cyberspace operations mark a certain maturation in their authorities, sustainment, and employment. A four-star combatant commander can now mention in public that cyber effects are making a difference on the battlefield.

Cyber operations continued in other quarters as well but still could not be discussed in detail. Then–national security advisor John Bolton in October 2018 issued a public but terse warning that the United States had mounted cyber attacks to defend its upcoming midterm elections from hostile actors.[62] The public was then left to fill in the details of these efforts from newspaper articles. The Director of National Intelligence, then Daniel R. Coats, confirmed in December that "Russia, and other foreign countries, including China and Iran," had interfered in the elections by conducting "influence activities and messaging campaigns targeted at the United States to promote their strategic interests."[63] The *New York Times* reported Coats's statement that same day, adding that Russian activity had been less than anticipated and noting that unnamed officials credited the decline in part to efforts by U.S. Cyber Command and other U.S. agencies collaborating with technology companies to warn off Russian cyber actors and restrict their social media accounts.[64] "US officials believe the [American] disruption effort," observed David Ignatius in the *Washington Post,* "has frazzled some of the Russian targets and may have deterred some interference during the midterms."[65]

Conclusion

Several tentative conclusions and judgments emerge from the history at hand. First, the only certain constant is surprise. We have seen forty-plus years of confounded expectations since Thomas Rona's prophecy in 1976. Cyber conflict has unfolded in ways that neither Rona nor later observers (either proponents or skeptics) expected. Originally seen as adjuncts to state-on-state war, cyber operations were next perceived as an asymmetric tool for terrorists and small states to employ against critical infrastructure, and then (among other things) became in some minds an all-powerful instrument of social control and coercion. None of these perceptions or fears were groundless, and all were to some extent true, but all proved to be exaggerated. Which of our current concerns about cyber conflict will also prove mistaken?

Second, all wars are now cyber wars. "Cyber war" became a redundant term over the last decade as modern militaries (and even nonstate actors) sought to supplement their

conventional capabilities with cyber effects. But cyber conflict expands beyond the violent use of arms, and cyber operations are also becoming a standard tool in coercive diplomacy and strategic competition between states.

Third, cyber operations can now cause strategic effects, with or without bloodshed or even armed attacks. Since strategic effects are now possible without the risks of war, states and nonstates will seek more of them, whether we respond or not. Operations below the use-of-force threshold may be just as effective as, and are surely less risky than, open war. The three strategic prizes of cyberspace competition are (1) legitimacy, the ability of a sovereign power to justify itself to its people, partners, and creditors; (2) intellectual property, to include the algorithms by which value is stored and created; and (3) privacy, individuals' capacity to control information about themselves. States and international actors will compete in cyberspace to preserve these prizes and to imperil their adversaries' hold on them.

Fourth, and finally, we can see the future only dimly, despite the confidence implied in the first three points above. Cyberspace will presumably become more contested, so how should we build forces? If wars are now cyber wars, then where are wars going in the future? If competition below the use-of-force threshold can now cause strategic effects, will actual war play an increasingly smaller role in shifts in the international distribution of power? Here is where tomorrow's scholars can contribute. We need declassification, to be sure, but we also need to take advantage of the wealth of sources, material, and historical actors (many of them barely middle-aged) already more or less available to researchers.

Notes

1. See, for instance, the essays collected in Jason Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986–2012* (Arlington, VA: Cyber Conflict Studies Association, 2013), and Fred Kaplan, *Dark Territory: The Secret History of Cyber War* (New York: Simon & Schuster, 2016).
2. Thomas P. Rona, *Weapon Systems and Information War* (Seattle, WA: Boeing Corporation, for the Office of the Secretary of Defense, 1 July 1976), pp. vi, 1–4, 40, https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Science_and_Technology/09-F-0070-Weapon-Systems-and-Information-War.pdf.
3. For a congressional perspective on the trends and their impact on the federal government, see U.S. Senate, Committee on Government Operations, *Staff Study of Computer Security in Federal Programs,* 95th Cong., 1st sess., February 1977, Committee Print 80-246, esp. p. 138, babel.hathitrust.org/.
4. The *DOD* [Department of Defense] *Dictionary of Military and Associated Terms* defines *maneuver* in several complementary ways, including as the "employment of forces in the operational area through movement in combination with fires to achieve a position of advantage in respect to the enemy." *DOD Dictionary of Military and Associated Terms* (Washington, DC: U.S. Defense Dept.,

October 2018), p. 135, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf.

5. Ronald Reagan, *National Policy on Telecommunications and Automated Information Systems Security,* National Security Decision Directive [NSDD] 145 (Washington, DC: White House, 17 September 1984), https://www.fas.org/irp/offdocs/nsdd145.htm. NSDD-145 was originally top secret but is now declassified.
6. Ibid.
7. See, for instance, Bruce G. Blair, *Strategic Command and Control: Redefining the Nuclear Threat* (Washington, DC: Brookings Institution, 1985), p. 283. See also Ashton B. Carter, John D. Steinbruner, and Charles A. Zraket, eds., *Managing Nuclear Operations* (Washington, DC: Brookings Institution, 1987), pp. 2–3, 11.
8. Comptroller General of the United States, *NORAD's Missile Warning System: What Went Wrong?,* MASAD-81-30 (Washington, DC: General Accounting Office, 15 May 1981), p. 13, archive.gao.gov/f0102/115265.pdf.
9. See Craig J. Wiener, "Penetrate, Exploit, Disrupt, Destroy: The Rise of Computer Network Operations as a Major Military Innovation" (unpublished PhD dissertation, George Mason Univ., Fairfax, VA, 2016), pp. 93–105, hdl.handle.net/1920/10613.
10. Jerilynn B. Hoy, Mary T. Brewer, Beverly A. Peterson, Gwendolyn Dittmer, et al., *Computer Security: Virus Highlights Need for Improving Internet Management,* GAO/IMTEC-89-57 (Washington, DC: General Accounting Office, June 1989), https://apps.dtic.mil/dtic/tr/fulltext/u2/a344751.pdf.
11. U.S. Joint Chiefs of Staff, *Command, Control, and Communications Countermeasures,* Joint Publication 3-13 (Washington, DC, 10 September 1987). See also Christopher W. Lowe, "From 'Battle' to the 'Battle of Ideas': The Meaning and Misunderstanding of Information Operations" (School of Advanced Military Studies monograph, U.S. Army Command and General Staff College, Fort Leavenworth, KS, 10 December 2010), pp. 17–25.
12. Alan D. Campen, ed., *The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War* (Fairfax, VA: AFCEA International, 1992), pp. vii, ix, 172.
13. Ibid. [emphasis original].
14. Donald J. Atwood, *Information Warfare,* DOD Directive TS 3600.1 (Washington, DC: U.S. Defense Dept., 21 December 1992), https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Other/14-F-0492_doc_01_Directive_TS-3600-1.pdf. DOD's Freedom of Information Act office posted this document with redactions on 20 June 2014.
15. Ibid.
16. U.S. Joint Chiefs of Staff, *Command and Control Warfare,* Memorandum of Policy 30 (Washington, DC, March 1993), https://archive.org/. For more on the divergence between the two documents, see Michael Warner, "Notes on Military Doctrine for Cyberspace Operations in the United States, 1992–2014," U.S. Military Academy / Army Cyber Institute *Cyber Defense Review* (online version) (27 August 2015), https://cyberdefensereview.army.mil/.
17. U.S. Joint Chiefs of Staff, *Command and Control Warfare*.
18. See their descriptions in U.S. Joint Chiefs of Staff, *Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance,* 2nd ed. (Washington, DC, 4 July 1996), pp. A-32 to A-61.
19. U.S. Joint Chiefs of Staff, *Joint Doctrine for Command and Control Warfare (C2W),* Joint Publication 3-13.1 (Washington, DC, 7 February 1996), www.iwar.org.uk/rma/resources/c4i/jp3_13_1.pdf [hereafter Joint Publication 3-13.1].
20. The pamphlet was signed by Secretary of the Air Force Sheila E. Widnall and Chief of Staff of the Air Force Gen. Ronald R. Fogleman, giving it the public imprimatur of the service's most senior civilian and military leaders, respectively. U.S. Air Force, *Cornerstones of Information Warfare* (Washington, DC, 1995), www.c4i.org/cornerstones.html.
21. The exercise, based on a hypothetical clash with Iran, was described at length in Roger C. Molander, Andrew S. Riddile, and Peter A. Wilson, *Strategic Information Warfare: A New Face of War,* MR-661-OSD (Santa Monica, CA: RAND, 1996), pp. xii, xvii, https://www.rand.org/.
22. John P. White, *Information Operations,* DOD Directive S-3600.1 (Washington, DC: U.S. Defense Dept., 9 December 1996),

https://archive.org/details/DODD_S3600.1. This superseded TS 3600.1 and was originally classified but later publicly released with redactions.

23. Joint Publication 3-13.1.
24. Quoted in United Nations International Criminal Tribunal for the former Yugoslavia, "Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign against the Federal Republic of Yugoslavia," 13 June 2000, www.icty.org/. See also Hugh Shelton, Ronald Levinson, and Malcolm McConnell, *Without Hesitation: The Odyssey of an American Warrior* (New York: St. Martin's Griffin, 2011 [2010]), pp. 370–73.
25. Samuel R. Berger, "Winning the Peace in Kosovo" (remarks, Council on Foreign Relations, Washington, DC, 26 July 1999), https://www.mtholyoke.edu/acad/intrel/berkos.htm. See also Shelton, Levinson, and McConnell, *Without Hesitation,* p. 381.
26. Richard B. Andres, "Deep Attack against Iraq," in *War in Iraq: Planning and Execution,* ed. Thomas G. Mahnken and Thomas A. Keaney (London: Routledge, 2007), pp. 70, 82.
27. Kevin M. Woods, with Michael R. Pease et al., *Iraqi Perspectives Project: A View of Operation Iraqi Freedom from Saddam's Senior Leadership* (Norfolk, VA: U.S. Joint Forces Command, 2006), p. 95, https://apps.dtic.mil/dtic/tr/fulltext/u2/a446305.pdf.
28. See, for instance, "When Cyberwar Comes of Age," *Federal Computer Week,* 3 October 1999, https://fcw.com/. See also David A. Fulghum, "Frustrations and Backlogs: Preparations for Conflict in Iraq Involve Complications," *Aviation Week & Space Technology,* 10 March 2003, freerepublic.com/.
29. U.S. Strategic Command Public Affairs, "Joint Task Force–Computer Network Operations," press release, February 2003, www.iwar.org.uk/.
30. Michael V. Hayden, *Playing to the Edge: American Intelligence in the Age of Terror* (New York: Free Press, 2016), p. 148.
31. Eliza Manningham-Buller, "The International Terrorist Threat to the UK" (speech, Queen Mary's College, London, 9 November 2006), https://www.mi5.gov.uk/.
32. Ibid.
33. Joseph I. Lieberman and Susan M. Collins, *A Ticking Time Bomb: Counterterrorism Lessons from the U.S. Government's Failure to Prevent the Fort Hood Attack* (Washington, DC: U.S. Senate Committee on Homeland Security and Governmental Affairs, 3 February 2011), p. 18, https://www.hsgac.senate.gov/imo/media/doc/Fort_Hood/FortHoodReport.pdf. See also Seth G. Jones, *Hunting in the Shadows: The Pursuit of Al Qa'ida since 9/11* (New York: W. W. Norton, 2012), pp. 149–50, 341–44.
34. Abizaid was interviewed for and quoted by Eric Schmitt and Thom Shanker, *Counterstrike: The Untold Story of America's Secret Campaign against Al Qaeda* (New York: Times Books, 2011), pp. 132–35.
35. Ibid.
36. Hayden, who was at this time the CIA director, was not happy with this result, arguing in his memoir that the offensive cyberspace missions inflicted collateral damage on intelligence operations. Hayden, *Playing to the Edge,* pp. 148–50.
37. Andreas Schmidt, "The Estonian Cyberattacks," in Healey, *Fierce Domain,* pp. 188–89. See also Noah Shachtman, "Kremlin Kids: We Launched the Estonian Cyber War," *Wired,* 11 March 2009, https://www.wired.com/.
38. Andreas Hagen, "The Russo-Georgian War 2008," in Healey, *Fierce Domain,* pp. 196–204. See also David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal,* 6 January 2011, https://smallwarsjournal.com/.
39. David Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (New York: Crown, 2012), pp. 188–93, 200.
40. Hayden, *Playing to the Edge,* pp. 151–52.
41. Brandon Valeriano and Benjamin Jensen, *The Myth of the Cyber Offense: The Case for Restraint,* Policy Analysis no. 862 (Washington, DC: Cato Institute, 15 January 2019), https://www.cato.org/.
42. Hillary Rodham Clinton, "Remarks on Internet Freedom" (delivered at the Newseum, Washington, DC, 21 January 2010), https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm.
43. Hillary Rodham Clinton, *Hard Choices* (New York: Simon & Schuster, 2014), pp. 545, 548, 549.
44. Philip N. Howard and Muzammil M. Hussain, "Egypt and Tunisia: The Role of Digital Media," in *Liberation Technology: Social Media and the Struggle for Democracy,* ed. Larry

Diamond and Marc F. Plattner (Baltimore, MD: Johns Hopkins Univ. Press, 2013), pp. 111–13.

45. "Iran's Police Vow No Tolerance towards Protesters," Reuters, 6 February 2010, https://www.reuters.com/.
46. Valery Gerasimov, "The Value of Science in Prediction" [in Russian], *Military-Industrial Kurier,* 27 February 2013, trans. Robert Coalson in Mark Galeotti, "The 'Gerasimov Doctrine' and Russian Non-linear War," *In Moscow's Shadows* (blog), 6 July 2014, https://inmoscowsshadows.wordpress.com/, repr. Robert Coalson, "Top Russian General Lays Bare Putin's Plan for Ukraine," *Huffington Post,* 2 September 2014, https://www.huffingtonpost.com/.
47. Coalson, "Top Russian General."
48. Ibid.
49. "Iran Says New Cyber Warfare Is Attack on Economy," *American Thinker,* 1 May 2012, https://www.americanthinker.com/.
50. U.S. Federal Bureau of Investigation, "Iranians Charged with Hacking U.S. Financial Sector," press release, 24 March 2016, https://www.fbi.gov/. See also Office of Public Affairs, "Seven Iranians Working for Islamic Revolutionary Guard Corps–Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks against U.S. Financial Sector," *United States Department of Justice,* 24 March 2016, https://www.justice.gov/.
51. U.S. Federal Bureau of Investigation, "Iranians Charged with Hacking U.S. Financial Sector."
52. John Kerry, "Condemning Cyber-Attack by North Korea," press statement, 19 December 2014, https://2009-2017.state.gov/secretary/remarks/2014/12/235444.htm.
53. Bill Marczak et al., "An Analysis of China's 'Great Cannon'" (presentation, 5th USENIX Workshop on Free and Open Communications on the Internet, Washington, DC, 10 August 2015), https://www.usenix.org/system/files/conference/foci15/foci15-paper-marczak.pdf.
54. United States of America v. Internet Research Agency et al., U.S. District Court for the District of Columbia, 16 February 2018, p. 3, https://www.justice.gov/.
55. Ibid., p. 17. See also Scott Shane, "These Are the Ads Russia Bought on Facebook in 2016," *New York Times,* 1 November 2017.
56. Adam Nossiter, David E. Sanger, and Nicole Perlroth, "Hackers Came: But the French Were Prepared," *New York Times,* 9 May 2017.
57. "Theresa May Accuses Vladimir Putin of Election Meddling," *BBC,* 14 November 2017.
58. "UK Cyber-Defence Chief Accuses Russia of Hack Attacks," *BBC,* 15 November 2017.
59. Deputy Secretary Work "said U.S. and coalition forces were putting pressure on Islamic State from all directions, using every possible military capability, including cyber attacks, to defeat the group." See "US Military Says Using Cyber Capabilities against Islamic State," Reuters, 12 April 2016, https://www.reuters.com/.
60. Ash Carter, *A Lasting Defeat: The Campaign to Destroy ISIS,* Belfer Center Report (Cambridge, MA: Harvard Univ., October 2017), p. 33, https://www.belfercenter.org/.
61. Joseph L. Votel, David J. Julazadeh, and Weilun Lin, "Operationalizing the Information Environment: Lessons Learned from Cyber Integration in the USCENTCOM AOR," U.S. Military Academy / Army Cyber Institute *Cyber Defense Review* 3 (Fall 2018), p. 18, https://cyberdefensereview.army.mil/.
62. Ellen Nakashima and Paul Sonne, "Bolton Says U.S. Is Conducting 'Offensive Cyber' Action to Thwart Would-Be Election Disrupters," *Washington Post,* 31 October 2018.
63. Dan Coats, "DNI Coats Statement on the Intelligence Community's Response to Executive Order 13848 on Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election," press release, 21 December 2018, https://www.dni.gov/.
64. Julian E. Barnes, "Russians Tried, but Were Unable to Compromise Midterm Elections," *New York Times,* 21 December 2018.
65. David Ignatius, "The Best Cyberdefense? A Good Cyberoffense," *Washington Post,* 8 February 2019.

CHAPTER TWO

The Cyber Paradigm Shift

EMILY O. GOLDMAN

The evolution of U.S. Cyber Command has been accompanied by the ascendance of a new paradigm theory for cyberspace. By 2016, there was widespread recognition that existing U.S. cyber strategy and its deterrence-theory underpinnings were not stemming the onslaught of cyberspace aggression below the threshold of armed conflict. The 2018 Command Vision *was the first official public statement of a new theory of the cyber strategic environment, one that calls for a strategy of cyber persistence.*

New Thinking Taking Root

The essays in this volume describe ways in which U.S. Cyber Command (USCYBERCOM) has evolved over the decade since Secretary of Defense Robert Gates directed its establishment in June 2009. Its current commander, Gen. Paul Nakasone, divides the history of the command into overlapping chapters, or "acts." Act 1 was standing up the command in May 2010. Act 2 was the team-building phase. In 2012, the Department of Defense (DOD) began building 133 teams—6,187 people, both military and civilian. Over the ensuing four years, the Cyber Mission Force increased its capacity and capability, reaching full operational capability in 2018. During act 3, those teams were employed. While still building the force in 2016, Joint Task Force–Ares supported U.S. Central Command and U.S. Special Operations Command by conducting operations to defeat ISIS in virtual space. In 2018, the Russia Small Group, a USCYBERCOM partnership with the National Security Agency, in coordination with other members of the interagency community, assisted in securing the 2018 midterm elections.[1]

These organizational and operational milestones have been accompanied by an equally important "conceptual" transformation, characterized by General Nakasone in his 2019 *Joint Force Quarterly* article as a pivot from a "response force" to a "persistence force." The commander writes, "USCYBERCOM initially focused on defending DOD networks[,] . . . executing counterterrorism operations, planning to support conventional forces in crisis scenarios, and maintaining capacity to respond to an 'attack of significant consequence' against our critical infrastructure."[2] The response-force concept—holding

forces in reserve for war or responding to attacks after the fact—proved to be no match for increasingly capable adversaries operating continuously below the threshold of armed conflict against our critical infrastructure, government networks, defense industries, and academia. "A persistence force has a much higher chance of disrupting adversary plots and protecting Americans, compared with a force that is confined to sporadic reconnaissance" and episodic engagement.[3]

The intellectual foundations of this evolution in USCYBERCOM's strategic concept reflect a paradigm shift that is under way across the community of cyberspace theorists and practitioners.[4] This shift is the subject of this essay. It is more than academic and semantic. It has far-reaching implications for military requirements, force posture, planning, team employment, target selection, operational tempo, and assessment—as well as for broader U.S. cyberspace strategy.

Paradigm Shifts

The term "paradigm shift" was coined by physicist and historian of science Thomas Kuhn in his influential 1962 work *The Structure of Scientific Revolutions*.[5] Paradigm shifts occur when one paradigm theory displaces another. Shifts take time, because we tend to see what we expect and try to explain anomalies in terms of the established paradigm theory and its conceptual scheme.[6] Moreover, competing paradigms can coexist, much as the nuclear and conventional paradigms coexisted for much of the Cold War.[7] Richard Harknett explains,

> What is intriguing about the first fifty years of the nuclear era is that both the nuclear and conventional paradigms on war coexisted simultaneously. Superpower relations were conditioned by the existence of assured destruction capabilities. These relations, however, were conducted in an international system in which conventional forces were prevalent and conventional notions of security were dominant. While superpower relations were captured by the logic of the nuclear paradigm, they were not immune from the applications and thinking dominant in the conventional paradigm.[8]

Similarly, today cyberspace strategy, planning, and operations are being forged in a security environment where deterrence thinking still dominates, even as it fails to account for much of the cyberspace behavior that is occurring.

Kuhn's framework of anomaly, crisis, and paradigm shift makes the current debates over cyberspace strategy more intelligible, much in the way that an earlier discourse on military change provided greater clarity on an ongoing transformation in warfare. Writing about the "information" revolution in military affairs in 2003, the late Andrew Marshall, Director of Net Assessment, Office of the Secretary of Defense, remarked that there had been a number of significant changes in warfare over the last five centuries, each taking place over several decades; thus, changes in warfare were not new. "What is new is that—because of the work of Western military historians since the 1950s, and the use of this concept of revolutions in military affairs by Soviet military theorists

beginning in their 1960's discussion of the impact on warfare of nuclear weapons and ballistic missiles—we are more self-aware about the process than were most generations who had this experience."[9]

As the concepts of "military revolution" and "revolutions in military affairs" gave form and logic to the information transformation in warfare, Kuhn's concept of paradigm shift provides a conceptual anchor for increasing our awareness of the intellectual changes occurring in parallel with, and undergirding, USCYBERCOM's organizational and operational evolution.

The Deterrence Paradigm

Kuhn defined a scientific paradigm as a "universally recognized scientific achievement that, for a time, provides model problems and solutions for a community of practitioners."[10] A paradigm theory provides a scientific community with its basic assumptions, key concepts, and methodology. It gives its research general direction and goals.

"Paradigms gain their status because they are more successful than their competitors in solving a few problems that the group of practitioners has come to recognize as acute."[11] This again ushers in a new period of "normal" science—"research firmly based upon one or more past scientific achievements, achievements that some particular scientific community acknowledges for a time as supplying the foundation for its further practice."[12] Paradigms share two characteristics: they are "sufficiently unprecedented to attract an enduring group of adherents" away from what has been going on, and they are open-ended, implying plenty of problems for the "redefined group of practitioners to resolve."[13]

Deterrence theory met these criteria during the Cold War. It addressed an acute problem: how to secure when you cannot defend. Its ideas were counterintuitive and challenged the lessons of thousands of years of warfare. It was revolutionary to assert that security rested not in one's own hands but in the mind of the opponent. It raised a host of new questions and concepts to occupy theorists and practitioners. These included questions of extended deterrence, crisis stability, strategic interaction (bargaining and escalation dominance), arms control (versus disarmament), counterforce and countervalue, assured destruction, limited war, and balance of terror.[14] Over the decades it proved to be conceptually well aligned with the new strategic environment. Nuclear deterrence was associated with the strategic stability and absence of major war between the United States and the Soviet Union during the unprecedented historical period from the end of World War II through the Cold War, what John Lewis Gaddis calls the "Long Peace."[15] It thus attracted an enduring group of adherents in the international-relations

and security-studies communities away from competing modes of scientific activity—from examining questions of how to fight and win war toward those of how to deter war.

Key to the ascendance and development of the deterrence paradigm was the role of social scientists who developed the intellectual underpinnings and derived the strategic implications of the nuclear revolution. In 1946, the year after the military use of the atomic bomb, a group of social scientists produced *The Absolute Weapon: Atomic Power and World Order,* which captured the core aspect of the atomic weapon and offered the essential strategic response—the concept of deterrence.[16] Deterrence logic was revolutionary—just like the distinctive nuclear strategic environment that bred it. Civilians such as Bernard Brodie, William Kaufmann, Albert Wohlstetter, Thomas Schelling, and Herman Kahn understood that it was not possible to import the tactics, operations, and strategies that had brought victory in the Second World War to the nuclear era. They articulated a compelling logic of why this was the case and gave birth to the field of nuclear deterrence strategy.[17] Policy makers, to be clear, professed rhetorical acceptance of the nuclear paradigm's logic while still relying on conventional notions of security to guide nuclear policy. Yet at the same time, serious debates about nuclear war could not escape the logic of assured-destruction capabilities.

The elements of a "deterrence strategy" were explicitly applied to cyber in the G. W. Bush administration and in the Obama years were reinforced with the 2011 *International Strategy for Cyberspace* and the 2015 *DOD Cyber Strategy*. The adoption of the deterrence paradigm was facilitated by Cold War veterans, who naturally defaulted to past experience. As evidence began mounting after 2013, however, that deterrence strategies were ineffective against the vast majority of cyber aggression, which was taking place below the threshold of armed attack, USCYBERCOM grew frustrated with the paradigm—although it did not begin to define an alternative until late 2016–early 2017.[18]

Anomalies and Crisis

A paradigm shift reflects a fundamental change in the basic concepts and experimental practices of a scientific discipline or, more broadly, in its view of how things work in the world. This occurs when anomalies arise that cannot be fully explained within the dominant paradigm, causing a "crisis" that creates opportunity for the emergence of a new paradigm. A crisis involves a period of "extraordinary," rather than "normal," research and is marked by a "proliferation of competing articulations, the willingness to try anything, the expression of explicit discontent, the recourse to philosophy and to debate over fundamentals."[19]

The applicability of deterrence strategy to cyberspace was questioned even before "cyber" entered the common lexicon. In 1996, National Defense University convened a

roundtable on deterrence. In those early days, attendees were still calling cyber "information warfare" (IW). In their conclusion on applying deterrence theory to cyberspace, they wrote,

> With the dawn of the atomic age came the recognition that developing strategies for deterrence and counter proliferation needed to be pursued with a sense of the utmost urgency. IW differs from atomic warfare in a number of significant ways and therefore lessons learned from our experience in developing a workable strategy for deterrence may not apply directly to the problem of deterrence of IW attacks, but certainly may provide a starting point or checklist for consideration.[20]

Deterrence theory and its application to the nuclear problem remain deeply entwined with cyber policy, strategy, and lexicon. A review of policy and strategy statements and documents, executive orders, reports, congressional acts, think-tank initiatives, Defense Science Board studies, and security-studies research testifies to the impact of deterrence thinking on the cyber policy and scholarly communities.[21] Harknett reflected on this "paradigm lock" in a 2017 interview:

> For several millennia prior to 1945, the capacity to secure oneself territorially rested in your hands—offense versus defense. Bernard Brodie and others quickly realized that "one plane, one bomb, one city" meant that security could not be found in defense, so they introduced the radical idea that our security would rest in the minds of our opponents, and the purpose of possessing military capability, nukes, was to never actually use them. We have become very comfortable with this framework because it worked in the nuclear environment and still does. But this was a specific strategic response to a specific strategic environment, and it does not hold that it will be universally effective across all weapon types.[22]

Kuhn saw that crisis and theory change go hand in hand. The crisis at hand is the fact that the United States is losing ground in cyberspace. The first quarter of 2018 saw a staggering 32 percent increase in the total number of cyber attacks compared with the same period the year before. In March 2018, Symantec concluded that "with each passing year, not only has the sheer volume of threats increased, but the threat landscape has become more diverse, with attackers working harder to discover new avenues of attack and cover their tracks while doing so."[23] By 2023, it is predicted, half of all data breaches globally will occur in the United States, because of the vast amount of consumer and corporate data stored across the country.[24] The United States is also the number one target for state-sponsored cyber attacks. On the basis of publicly available information on cyber espionage and cyber warfare, excluding cyber crime, the Center for Strategic and International Studies has concluded that the United States by far was the single most victimized state in 2018, nearly four times as likely to be targeted as number two, India.[25]

The crisis is not defined only by increasing numbers of attacks. The type of cyber aggression too has evolved. Where once espionage and exploitation were the major concerns, the shift to disruptive (e.g., the 2012–13 distributed-denial-of-service attacks conducted by the Iranians against the financial networks in New York), destructive (e.g.,

the 2014 data-deletion attack by the Iranians against a U.S. casino corporation and the North Korean attack against Sony Pictures), and corrosive attacks against our democratic institutions (e.g., Russian attempts to influence the 2016 election) represents a crisis for U.S. cyber strategy.

To be precise, the frustration (crisis) was not that deterrence was not working at all but that it was not stopping the burgeoning numbers of attacks below the threshold of armed conflict and that these attacks cumulatively were leading to relative power loss. Deterrence arguably has been effective in the cyber strategic space of armed conflict. States, it would appear, are choosing to abide by conventions codified in United Nations Charter articles 2(4) and 51, which speak to the use of force and the right of self-defense in the event of armed attack. They also recognize that the United States can respond across domains (using its advantages) to a cyber attack should they violate those conventions.

The failures have been in assuming that deterrence would also be successful in the strategic space short of armed conflict and, more fundamentally, in not understanding that those two strategic spaces even existed. Decision makers needed a paradigm shift to recognize the existence of distinct strategic spaces that had opened a seam in great-power competition that in turn others were exploiting, to explain why this dynamic came about, and to offer a new strategy better aligned to cyberspace's structural and operational imperatives.

Kuhn explains that defenders of a former paradigm, when confronted with anomalies, "devise numerous articulations and ad hoc modifications of their theory in order to eliminate any apparent conflict."[26] Harknett saw that published writings were tinkering with the deterrence paradigm theory to explain away cyber anomalies—an indicator of a paradigm crisis. "All the reasons why deterrence is not working in the cyber domain are discussed, the concept of deterrence is stretched, and a conclusion is then offered that we need to keep working the problem."[27] An example is Joseph Nye's January 2017 article in *International Security,* "Deterrence and Dissuasion in Cyberspace." Nye acknowledges difficulties in applying deterrence to cyberspace, then extends the concept to include "entanglement" and norms. Still dissatisfied, he concludes that deterrence in the Cold War was not as good as scholars and policy makers think it was, so perhaps cyber deterrence is being held to an illusionary standard. Nye then calls for more work to be done on cyber deterrence.[28] A similar pattern is present in the practitioner community. The February 2017 Defense Science Board task force report on cyber deterrence conceded that measures taken to date had not advanced security or "established effective deterrence of future cyber attacks and costly cyber intrusions."[29] Yet the report recommends "tailoring" deterrence and improving source attribution.

In his rejoinder to Nye, Harknett concludes that "using a legacy construct of deterrence, whose measure of effectiveness is the absence of action, to explain an environment of constant action will not take us where we need to be. Like our predecessors of the 1940s/50s, we need new intellectual constructs to understand the real-world strategic interaction and to shape policy effectively toward a more secure cyber-enabled global system."[30]

Paradigms are not only collective frameworks that define intellectual discourse and shape scientific progress; they represent professional investment by committed problem solvers. This is why challenging a paradigm theory requires an alternative logic, one that takes root and offers novel solutions to the crisis at hand. To return to the theory of paradigm shifts, Kuhn insists that "the decision to reject one paradigm is always simultaneously the decision to accept another, and the judgment leading to that decision involves comparison of both paradigms with nature *and* with each other."[31] He further concludes that "once it has achieved the status of paradigm, a scientific theory is declared invalid only if an alternate candidate is available to take its place."[32]

Changes in Worldview

Social scientists have been helping articulate a new paradigm theory for cyberspace. In 2012, USCYBERCOM convened a group of experts and launched the Cyber Analogies Project to enrich the discourse on cyber strategy, doctrine, and policy.[33] In retrospect, analogical searching was a precursor to the paradigm shift that would soon be under way. It represented a search for conceptual anchors to make sense of what was occurring in cyberspace. The project emerged on the heels of the Arab Spring—a revelation of how cyberspace could be used to topple regimes, which spurred dictators to escalate cyberspace operations against their own citizens and ours.

Analogies, of course, are not paradigms. Paradigms legitimate puzzles and problems on which a community works and promise novel solutions. They proffer unanswered questions, which give purpose and direction to disciples. Analogies serve a different purpose. "People use analogies, metaphors, and parables, both explicitly and implicitly, to link what is new to what is already known, as a bridge between the familiar and the new."[34] Kuhn observed that when confronted with a previously unobserved activity, we apply general categorical terms, because "what we are seeing bears a close family resemblance to a number of the activities that we have previously learned to call by that name."[35] Natural analogies and resemblances are abundant and can be found within almost any group of items.[36] Analogies at their best facilitate communication across diverse communities. Yet there are too many to define a tradition or on which to model future practice.

By 2016, frustration in Congress and the broader policy community with our country's approach to cyberspace aggression was palpable. But no alternative to the language of deterrence yet existed. Political leaders, particularly in Congress, clamored for more cyber deterrence, to include a strategy and options, to halt the barrage of intrusions and attacks across government, industry, and academia. One of the most vocal and persistent critics was the chairman of the Senate Armed Services Committee at the time, Senator John McCain. He pushed the government relentlessly to develop a comprehensive cyber deterrence strategy and equally chastised the Obama and Trump administrations for not delivering a cyber deterrence policy.[37] During a March 2017 hearing, McCain complained that the United States was still "treating every [cyber] attack on a case-by-case" basis and projected weakness in cyberspace that "has emboldened our adversaries."[38] He continued, "As America's enemies seized the initiative in cyberspace, the last administration offered no serious cyber deterrence policy and strategy."[39]

The recognition of anomalies troubled the military and intelligence communities, arguably because so much of the empirical evidence of cyberspace aggression is, by necessity, restrictively classified. A turning point in the articulation of an alternative paradigm theory was the decision by USCYBERCOM to establish a "scholar in residence" program and to bring in a deterrence expert who could provide a theory and lexicon to explain what the operational community was observing. The 2017 publication of "Deterrence Is Not a Credible Strategy for Cyberspace" marked a direct challenge to deterrence theory as the paradigm theory for cyberspace.[40] In the article, Michael Fischerkeller and Richard Harknett offer an alternative theory of "cyberspace persistence," one that applies to the growing strategic space of cyber competition below the threshold of armed conflict.

In a nutshell, the theory of cyber persistence argues that strategic frameworks must map to the realities of strategic environments. The unique characteristics of cyberspace such as interconnectedness and constant contact, the combination of which induces an imperative for persistent action, are mismatched with a strategy of deterrence, which is based on operational restraint and coercive threats. The cyberspace operational domain calls for a strategy of cyber persistence—use of cyber capabilities in persistent operational contact to generate continuous tactical, operational, and strategic advantage and thus achieve the ability to deliver effects in, through, and from cyberspace at a time and place of one's choosing. Deterrence theory applies to cyber "armed attack"–equivalent operations—that is, in the cyber strategic space of armed conflict—but it must be complemented by persistence theory to ensure security in the cyber strategic competitive space below the threshold of armed attack.

Coterminous with this theoretical and more academic debate, an internal project was under way to socialize the nature, logic, and implications of a theory of persistence for the practitioner community within the command, across its cyber service components,

in the Joint Staff, in policy offices across the Department of Defense, and on Capitol Hill.[41] As perhaps was to have been expected, those closest to the problem—cyber force commanders and operators—were early adopters of the logic of and advocates for a new paradigm theory. They helped to refine and operationalize it, define metrics, and incorporate it into plans, operational orders, and tactics.

By 2017, the two critical components of a paradigm shift were present: anomalies and, in cyber persistence, an alternative theory. In March 2018, Cyber Command published its command vision, *Achieve and Maintain Cyberspace Superiority,* declaring its pivot to seizing and maintaining the initiative through "persistent engagement"—the continuous execution of the full spectrum of cyberspace operations to achieve and maintain cyberspace superiority, build resilience at home, defend forward, and contest adversary campaigns and objectives.

The language of persistence theory entered other official defense policy guidance, including the *DOD Cyber Strategy,* released in September 2018; the classified *Cyber Posture Review* that followed, reviewing the department's cyber posture and ability to execute the strategy; and the *National Military Strategy* released in December 2018. The *DOD Cyber Strategy* declares, "We will defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict." It also places "compete" on an equal footing with "deter" and directs the DOD to "persistently contest malicious cyber activity in day-to-day competition: The Department will counter cyber campaigns threatening U.S. military advantage by defending forward to intercept and halt cyber threats." Persistence terminology has also informed congressional deliberations. Section 1652 of the 2018 National Defense Authorization Act directs the formation of a Cyberspace Solarium Commission to evaluate strategic approaches to cyberspace and calls out "persistent engagement" as one of three approaches.[42] The use of new language is an important step in recasting how we perceive the world and, therefore, how we operate in it.

Persuasion

The single most "prevalent claim advanced by the proponents of a new paradigm is that they can solve the problems that have led the old one to crisis."[43] Persistence theory views as normal certain occurrences that would be failures for deterrence theory. Cyber aggression below the threshold of armed attack is not an anomaly but rather a signal of the emergence of a new competitive space wherein "agreement over the substantive character of acceptable and unacceptable behaviors . . . is currently immature."[44] Thus, what is "normal" must be recast. Deterrence and persistence theorists observe the same reality through distinct conceptual lenses. Aristotle, watching a stone swinging at the end of a rope, would see the stone trying to reach its natural state, that of lying at rest;

Galileo, observing the same thing, would see a pendulum, a body repeating the same motion ad infinitum; and Newton would see a stone obeying the laws of gravity and energy transference.[45]

Paradigm shifts open up new questions, require different metrics, and introduce different languages. Kuhn recognized that a revolution changes even the very language in which we speak about some aspect of nature.[46] The lexicon of persistence theory is one of "campaigns," not incidents, intrusions, or hacks; "interaction," not escalation; "rules of engagement," not contingency planning options; "seizing targets of opportunity," rather than holding targets at risk; and "initiative," rather than restraint and response. Persistent engagement views activity as "continuous," not episodic; costs and benefits as "cumulative," not event based; operations as "exploitative," not coercive; and competition below the level of armed conflict as just as strategically consequential as war and territorial aggression.[47]

Kuhn maintains that proofs, the methods of normal science (empirics, data, metrics), are rarely sufficient to persuade.[48] This is because "reality cannot be described independently of the conceptual schemes through which we observe it. Paradigm theories are part of our conceptual schemes. So, when a paradigm shift occurs, in some sense the *world* changes. Or to put it another way, scientists working under different paradigms are studying different worlds."[49] Thus, the issue "in paradigm debates is which in the future should guide research on problems many of which neither competitor can yet claim to resolve completely."[50] Kuhn observes that "since no paradigm ever solves all the problems it defines and since no two paradigms leave all the same problems unsolved, paradigm debates always involve the question: Which problems is it more significant to have solved?"[51]

The core research question for the deterrence paradigm is how to deter cyber attacks when you cannot reliably defend against them. The core question for the persistence paradigm is how to secure when you cannot deter. Deterrence is not an end in itself but a means to an end—security. The deterrence paradigm presumes the answer to this question a priori and proceeds to what Kuhn would consider the problem-solving stage of normal science—devising "tailored deterrence strategies" for specific adversaries, building playbooks of options, and improving attribution (identification of the actor responsible for an attack). The persistence paradigm posits a wider set of research questions: What are the foundational characteristics of the cyber strategic space? How are they similar to, and different from, physical spaces, particularly nuclear? What are the roles for defense, offense, and deterrence? The persistence paradigm theory does not preclude deterrence strategies, just restricts them to where they logically apply—cyber operations equivalent to armed attacks. One indicator of a paradigm shift, which Kuhn

predicted, is a substantial change in topics studied, accompanied by abandonment of old topics and concepts.[52] Max Smeets and Herb Lin have already called for "systematic research on how persistent engagement and defend forward may play out" through case studies of how adversaries and allies might respond to a change in U.S. strategy.[53]

Conclusion

The emergence of persistence theory as a paradigm theory for cyberspace strategic behavior is well under way, despite the fact that persistence is at times described in the language of deterrence theory.[54] The talk is of war, rather than competition. Persistence and defending forward are conflated with offense, overlooking the large defensive role in a strategy of persistent engagement. Concerns with escalation and escalation dominance are often raised, presuming a spiraling interaction dynamic. References to "significant cyber incidents" hark back to the model of episodic contact, in contrast to that of constant contact in cyberspace, where "strategic significance" is not the result of any single event but rather emerges from the cumulative effect of a campaign comprising many individually less consequential operations/activities carried out toward a coherent strategic end.

There is an understandable frustration across a community steeped for decades in deterrence theory that many of the questions raised by persistence theory are not yet answered—such as how it produces stability. How can one shift allegiance to a theory not fully developed? No single convincing argument will be persuasive to all cyber scholars and practitioners; different arguments will persuade different individuals. Kuhn believed that neither proof nor error could account for the transfer of allegiance from one paradigm to another. Rather, change is more akin to a conversion experience, a product of persuasion rather than proof. It gradually spreads across a community, beginning with a few scientists who sense that their new paradigm is on the right track.[55] It is these initial supporters "who will develop it to the point where hardheaded arguments can be produced and multiplied," resulting in not a single group conversion but rather in "an increasing shift in the distribution of professional allegiances."[56]

Kuhn also coined the dictum that "revolutions progress away from previous conceptions of the world that have run into cataclysmic difficulties. This is not progress toward a pre-established goal. It is progress away from what once worked well, but no longer handles its own new problems."[57] In his essay "Cyber Threats, Nuclear Analogies?" Steven Miller notes that Bernard Brodie's *Strategy in the Missile Age* and Thomas Schelling's *Arms and Influence* did not appear until fifteen or twenty years after the detonations at Hiroshima and Nagasaki. Moreover, debates over deterrence requirements raged throughout the Cold War. Miller predicts that while deterrence theory may prove useful in some contexts, "it will be at best a partial solution to the problem of cyber threats."[58]

The persuasion project is in full swing. The cyber paradigm debate is now occurring in academic journals, blog posts, and major newspapers.[59] It informs policy deliberations in the Departments of Defense, State, and Homeland Security and the White House. These conversations are being driven by a recognition that aggression has raged in cyberspace for a decade or so despite the absence of major-state conflict. Kuhn maintains that

> if the paradigm is one destined to win its fight, the number and strength of the persuasive arguments in its favor will increase. More scientists will then be converted, and the exploration of the new paradigm will go on. Gradually the number of experiments, instruments, articles, and books based upon the paradigm will multiply. Still more [people], convinced of the new view's fruitfulness, will adopt the new mode of practicing normal science.[60]

The taken-for-granted framework of deterrence has been called into question, but we are still in the early stages of thinking through the fundamentals of cyberspace strategy. The history of paradigm shifts cautions us not to expect the path forward to be easy, linear, or without resistance. But change is indeed discernible, above all in the recently released Cyberspace Solarium Commission report, where the language and constructs of deterrence theory—cost imposition, deterrence by denial, signaling, attacks of significant consequence, response—sit side by side with those of cyber persistence—defend forward, persistent engagement, proactive, continuous. The commissioners assert that "deterrence is an enduring American strategy, but it must be adapted to address how adversaries leverage new technology and connectivity to attack the United States. . . . Therefore, the concept of deterrence must evolve to address this new strategic landscape."[61] More accurately, our "strategy" must evolve, and this means augmenting the repertoire of concepts—offense, defense, deterrence—that were derived from the conventional and nuclear environments with a new strategic construct—persistence—derived from the cyberspace strategic environment.

Notes

1. "An Interview with Paul M. Nakasone," *Joint Force Quarterly* 92 (1st Quarter 2019), p. 7.
2. Paul M. Nakasone, "A Cyber Force for Persistent Operations," *Joint Force Quarterly* 92 (1st Quarter 2019), p. 11. The article is reprinted as the introduction to this book.
3. Ibid.
4. The idea of a military component's "strategic concept" is developed in Samuel P. Huntington, "National Policy and the Transoceanic Navy," U.S. Naval Institute *Proceedings* 80 (May 1954), pp. 483–94.
5. Thomas S. Kuhn, *The Structure of Scientific Revolutions,* 4th ed. (Chicago: Univ. of Chicago Press, 2012).
6. Ibid., p. xxvi.
7. Richard J. Harknett, "State Preferences, Systemic Constraints, and the Absolute Weapon," in *The Absolute Weapon Revisited: Nuclear Arms and the Emerging International Order,* ed. T. V. Paul, Richard J. Harknett, and James J. Wirtz (Ann Arbor: Univ. of Michigan Press, 1998), pp. 47–49.
8. Ibid., p. 48.
9. Andrew W. Marshall, foreword to Emily O. Goldman and Leslie C. Eliason, *The Diffusion*

of Military Technology and Ideas (Palo Alto, CA: Stanford Univ. Press, 2003), p. xiii.

10. Thomas S. Kuhn, *The Structure of Scientific Revolutions,* 2nd ed. (Chicago: Univ. of Chicago Press, 1970), p. viii.
11. Kuhn, *Structure of Scientific Revolutions,* 4th ed., p. 24.
12. Ibid., pp. 10–11.
13. Ibid., p. 11.
14. Lawrence Freedman, *The Evolution of Nuclear Strategy* (New York: St. Martin's, 1981).
15. John Lewis Gaddis, *The Long Peace: Inquiries into the History of the Cold War* (New York: Oxford Univ. Press, 1987).
16. Bernard Brodie, ed., *The Absolute Weapon: Atomic Power and World Order* (New York: Harcourt Brace, 1946).
17. Fred Kaplan, *The Wizards of Armageddon* (New York: Simon & Schuster, 1983); Freedman, *Evolution of Nuclear Strategy*.
18. "White House Report to Congress on Cyber Deterrence Policy," *Federal News Network,* 29 December 2015, federalnewsnetwork.com/; Mark Pomerleau, "White House Promotes Whole-of-Nation Cyber Deterrence Strategy," *Defense Systems,* 23 December 2015, https://defensesystems.com/; *National Cyber Strategy* (Washington, DC: White House, September 2018), p. 21, https://www.whitehouse.gov/; *Fact Sheet on Presidential Policy Directive (PPD) 20* (Washington, DC: White House, January 2013), https://fas.org/irp/offdocs/ppd/ppd-20-fs.pdf. PPD-20 established a doctrine of restraint, mandating the least amount of action necessary. The 2015 *DOD Cyber Strategy* formalized the "doctrine of restraint" to "protect human lives and prevent the destruction of property."
19. Kuhn, *Structure of Scientific Revolutions,* 4th ed., p. 91. See also Richard J. Harknett and Emily O. Goldman, "The Search for Cyber Fundamentals," *Journal of Information Warfare* 15, no. 2 (Spring 2016), pp. 81–88.
20. Gary F. Wheatley and Richard E. Hayes, *Information Warfare and Deterrence* (Washington, DC: National Defense Univ. Press, December 1996), p. 62, www.dodccrp.org/files/Wheatley_Deterrence.pdf.
21. Senator John McCain long pressed the Pentagon to produce a cyber deterrence strategy and inserted language in a 2016 defense policy bill withholding $10 million in funding until the policy was produced; Joseph Marks, "Shoddy U.S. Cyber Deterrence Policy Emboldens Adversaries, Lawmakers Say," *Nextgov,* 2 March 2017, https://www.nextgov.com/. See also Scott Maucione, "White House Finally Acquiesces to Congress on Cyber Deterrence Policy," *Federal News Network,* 29 December 2015, https://federalnewsnetwork.com/; Office of the Coordinator for Cyber Issues, *Recommendations to the President on Deterring Adversaries and Better Protecting the American People from Cyber Threats* (Washington, DC: U.S. State Dept., 31 May 2018), https://www.state.gov/; and *Defense Science Board Task Force on Cyber Deterrence* (Washington, DC: U.S. Defense Dept., February 2017), https://apps.dtic.mil/dtic/tr/fulltext/u2/1028516.pdf.
22. Brad D. Williams, "Meet the Scholar Challenging the Cyber Deterrence Paradigm," *Fifth Domain,* 19 July 2017, https://www.fifthdomain.com/. Harknett and his coauthor Michael Fischerkeller have since refined their contention that "cyber operations actually preclude deterrence" by acknowledging that "a strategy of deterrence could be effective against a potential cyber action that is equivalent to armed conflict," although not in the strategic competitive space below the threshold of armed conflict. Michael P. Fischerkeller, Richard J. Harknett, and Jelena Vićić, "The Limits of Deterrence and the Need for Persistence," in *The Cyber Deterrence Problem,* ed. Aaron F. Brantly (London: Rowman & Littlefield, 2020).
23. Symantec *Internet Security Threat Report* 23 (March 2018), p. 5, https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf.
24. "Emerging Threats: 10 Cyber Security Facts and Statistics for 2018," *Norton,* [2018], https://us.norton.com/.
25. "Significant Cyber Incidents," *Center for Strategic and International Studies,* [2020], https://www.csis.org/.
26. Kuhn, *Structure of Scientific Revolutions,* 4th ed., p. 78.
27. Harknett, private correspondence.
28. Joseph S. Nye Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (Winter 2016/17), pp. 44–71.
29. *Defense Science Board Task Force on Cyber Deterrence,* p. 3.

30. Richard J. Harknett, "Is Deterrence Possible in Cyberspace? Correspondence with Joseph Nye," *International Security* 42, no. 2 (Fall 2017), pp. 196–99.
31. Kuhn, *Structure of Scientific Revolutions,* 4th ed., pp. xxvii, 78.
32. Ibid., p. 77.
33. Emily O. Goldman and John Arquilla, eds., *Cyber Analogies,* Technical Report NPS-DA-14-001 (Monterey, CA: Naval Postgraduate School, 2014).
34. Ibid., p. 5.
35. Kuhn, *Structure of Scientific Revolutions,* 4th ed., p. 45.
36. Ibid.
37. Andrew Blake, "John McCain Says White House's Cyber Deterrence Policy Comes Up Short," *Washington Times,* 15 January 2016.
38. Joseph Marks, "McCain Leaves a Rich Cyber Legacy," *Nextgov,* 27 August 2018, https://www.nextgov.com/.
39. Morgan Chalfant, "McCain Hits Trump over Lack of Cyber Policy," *The Hill,* 23 August 2017, https://thehill.com/.
40. Michael P. Fischerkeller and Richard J. Harknett, "Deterrence Is Not a Credible Strategy for Cyberspace," *Orbis* 63, no. 1 (Summer 2017), pp. 381–93.
41. Kuhn, *Structure of Scientific Revolutions,* 4th ed., p. 94.
42. The other two approaches are deterrence and norms-based regimes.
43. Kuhn, *Structure of Scientific Revolutions,* 4th ed., p. 152.
44. Michael P. Fischerkeller and Richard J. Harknett, *Agreed Competition in Cyberspace: What It Is and Is Not,* NSD-10415 (Alexandria, VA: Institute for Defense Analyses, January 2019), p. 3. Fischerkeller and Harknett argue that "cyber actors appear to have tacitly agreed on lower and upper bounds of the cyber strategic competitive space short of armed conflict—the operational space inclusive of and above operational restraint (i.e., inactivity) and exclusive of and below operations generating armed-attack equivalent effects." See also Michael P. Fischerkeller and Richard J. Harknett, "What Is Agreed Competition in Cyberspace?," *Lawfare* (blog), 19 February 2019, https://www.lawfareblog.com/; Michael P. Fischerkeller and Richard J. Harknett, *Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics, and Escalation,* NSD-9076 (Alexandria, VA: Institute for Defense Analyses, May 2018); and Michael P. Fischerkeller and Richard J. Harknett, "Persistent Engagement and Tacit Bargaining: A Path toward Constructing Norms in Cyberspace," *Lawfare* (blog), 9 November 2018, https://www.lawfareblog.com/.
45. Kuhn, *Structure of Scientific Revolutions,* 4th ed., pp. 119–23.
46. Ibid., pp. 128–32, 148.
47. Michael P. Fischerkeller and Richard J. Harknett, "A Response on Persistent Engagement and Agreed Competition," *Lawfare* (blog), 27 June 2019, https://www.lawfareblog.com/.
48. Kuhn, *Structure of Scientific Revolutions,* 4th ed., p. 153.
49. Emrys Westacott, "What Is a Paradigm Shift?," *ThoughtCo,* updated 12 October 2019, https://www.thoughtco.com/.
50. Kuhn, *Structure of Scientific Revolutions,* 4th ed., p. 156.
51. Ibid., p. 109.
52. Ibid., p. xxxiv.
53. Max Smeets and Herb Lin, "An Outcome-Based Analysis of U.S. Cyber Strategy of Persistence & Defend Forward," *Lawfare* (blog), 28 November 2018, https://www.lawfareblog.com/.
54. See Jonathan Reiber, "What Happens When the US Starts to 'Defend Forward' in Cyberspace?," *Defense One,* 5 November 2018, https://www.defenseone.com/; Ben Buchanan, "The Implications of Defending Forward in the New Pentagon Cyber Strategy," *Council on Foreign Relations* (blog), 25 September 2018, https://www.cfr.org/; Nina Kollars and Jacquelyn Schneider, "Defending Forward: The 2018 Cyber Strategy Is Here," *War on the Rocks,* 20 September 2018, https://warontherocks.com/; Dave Weinstein, "The Pentagon's New Cyber Strategy: Defend Forward," *Lawfare* (blog), 21 September 2018, https://www.lawfareblog.com/; Jason Healey, "US Cyber Command: 'When Faced with a Bully . . . Hit Him Harder,'" *Cipher Brief,* 26 February 2018, https://www.thecipherbrief.com/; Brandon Valeriano and Benjamin Jensen, *The Myth of the Cyber Offense: The Case for Restraint,* Policy Analysis 862 (Washington, DC: Cato

Institute, 15 January 2019), https://www.cato.org/; Mark Pomerleau, "Why Cyberspace Demands an Always-On Approach," *Fifth Domain,* 26 November 2018, https://www.fifthdomain.com/; Lyu Jinghua, "What Really Matters in 'Defending Forward'?," *Lawfare* (blog), 26 November 2018, https://www.lawfareblog.com/; Ben Buchanan and Robert D. Williams, "A Deepening U.S.-China Cybersecurity Dilemma," *Lawfare* (blog), 24 October 2018, https://www.lawfareblog.com/; Robert Chesney, "An American Perspective on a Chinese Perspective on the Defense Department's Cyber Strategy and 'Defending Forward,'" *Lawfare* (blog), 23 October 2018, https://www.lawfareblog.com/; Josephine Wolff, "Trump's Reckless Cybersecurity Strategy," *New York Times,* 2 October 2018; Elias Groll, "Trump Has a New Weapon to Cause 'the Cyber' Mayhem," *Foreign Policy,* 21 September 2018; "Pentagon Puts Cyberwarriors on the Offensive, Increasing the Risk of Conflict," *New York Times,* 17 June 2018; and Joe Uchill, "How Cyber's Forward Defense Could Backfire," *Axios,* 19 June 2018, https://www.axios.com/.

55. Kuhn, *Structure of Scientific Revolutions,* 4th ed., pp. 150–51.
56. Ibid., p. 157; Fischerkeller and Harknett, "Persistent Engagement and Tacit Bargaining."
57. Kuhn, *Structure of Scientific Revolutions,* 4th ed., p. xxxiv.
58. Steven E. Miller, "Cyber Threats, Nuclear Analogies?," in *Understanding Cyber Conflict: 14 Analogies,* ed. George Perkovich and Ariel E. Levite (Washington, DC: Georgetown Univ. Press, 2017), p. 171.
59. "Pentagon Puts Cyberwarriors on the Offensive"; Ellen Nakashima, "U.S. Cyber Force Credited with Helping Stop Russia from Undermining Midterms," *Washington Post,* 14 February 2019; Ellen Nakashima, "U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms," *Washington Post,* 27 February 2019.
60. Kuhn, *Structure of Scientific Revolutions,* 4th ed., p. 158.
61. "(Final) Report," *Cyberspace Solarium Commission,* March 2020, p. 27, https://www.solarium.gov/report.

CHAPTER THREE

Cyber Competition to Cybered Conflict

CHRIS C. DEMCHAK

Over the course of a decade, American leaders have pivoted cyber strategy closer to what would be needed for whole-of-society, systemic defense of democratic civil society in a rapidly digitizing but increasingly authoritarian-leaning and (in a phrase becoming familiar to specialists) "post-Western" world. This essay reviews how the expected "benign" competition among states became cybered conflict, *with its bleak global-order implications for consolidated democratic civil societies. It explains the creation of cybered conflict and the challenges of achieving robust cyber power across a nation's complex "socio-technical-economic systems." It describes what democratic civil societies must do to survive through a shared* cyber operational resilience alliance. *It concludes with recommendations for the Department of Defense and the services to build on the strategic learning that underlies the 2018* DOD Cyber Strategy.

Ten Years On: Strategic Learning

For a decade, the global environment has been evolving away from the civil-society dream of permanent international liberal markets buttressed by a borderless, near-free, open, worldwide internet. The rise of a large-scale authoritarian state as a central economic and technological node is moving the global cyber substrate toward authoritarian preferences, including bordered, highly censored networks and widespread disregard for civil-society norms and rules on information exchange or exploitation. Westernized political and economic leaders continue to struggle to accept that the new information age is moving rapidly out of their realm of influence and preferred modes of operation. Former president Barack Obama recognized national cyber insecurity as a tier-one threat to national security, but his administration's response was to reinforce the globally open internet ideal envisioned by highly optimistic Westernized democracies and their information technology (IT) capital-goods sectors. Their strategic approach was in large measure reactive: diplomatic exhortations, numerous multi-stakeholder conferences on voluntary international norms, and strengthened defenses of nations' military and government networks. Despite acknowledging a changing international environment

that is more conflictual and nationally sovereign, the 2015 *Department of Defense Cyber Strategy* doubled down on an internationalist and mostly reactive approach.[1]

Since 2015, bipartisan congressional concern with Chinese behavior has grown to converge with the Trump administration's preferences to reorient U.S. foreign policy around renewed great-power competition. A more confrontational approach toward a rising China that violates international rules of free trade and promotes radically different cyberspace values now has produced a much-changed *National Cyber Strategy* in 2018. The new document acknowledged that the world was more demonstrably aggressive in cyberspace. By the early 2010s, leaders of China and Russia had become confident enough to declare publicly their rejection of Western civil-society values, the open Westernized internet, and American hegemony. The 2018 *DOD Cyber Strategy* calls for proactive steps to address cyber insecurity and digital aggression.[2] Military cyber assets would now operate beyond Department of Defense (DOD) information networks to defend critical infrastructure and respond to major economic events. With this strategy, the official American approach evolved from seeking to preserve cyberspace as a purely commercial space with occasional crises to recognizing that the benign internet "competition" among states had evolved into a persistent cybered conflict.

Shoddy Cyber Substrate Creates Offense Advantages Globally

Effusively promising global prosperity and democracy everywhere, the early promoters of the internet in America were naive and arrogant, and greedy and dismissive. They were prone to hubris about their nation's superiority; the United States had "won" the Cold War.[3] For them, the information age would eliminate the need for governments while providing universally free (implicitly accurate) information to all people. Serious scholars heralded a future legal regime that would spontaneously emerge from the global internet, one separate from all existing legal or governance systems.[4]

Unfortunately, the basic internet technology that underlay this vision was exceptionally shoddily constructed and remains so; it was designed to respond rapidly to commercial needs without attention to quality coding or security. The early internet spread explosively, owing to widespread optimistic promotion and the use of quick-to-produce, insecure, typo-tolerant languages that supported short deadlines, high-volume sales, and large profits.[5] At the same time, the easily hacked cyber substrate connected many smaller complex systems within a country, making the larger state a *national socio-technical-economic system* (STES) in which small failures could cascade widely.[6] This rising potential for systemic harm to the national STES in democratic states has been largely ignored.[7]

The global spread of a shoddily built cyberspace expanded conflict among groups and states by increasing the availability—and reducing the costs—of five offense advantages. Now anyone can afford an army at any chosen size *(scale of organization),* obtain high-value critical intelligence from any distance *(proximity),* cheaply and easily choose across weapons and campaign types *(precision),* hide the choices to keep surprise or reuse options available for other targets or campaigns *(deception in tools),* and avoid retaliation for any and all attacks for some time *(opaqueness in origins).* Across history, only wealthy emperors or superpowers could leverage such advantages, dampening systemic conflict. Rarely could middle-sized to small or geographically widely separated nations—let alone individuals—afford the resources or foreknowledge to wage systemic conflict. Now, however, gathering accurate foreknowledge of a potential opponent and massing resources are no longer major constraints.[8] Advanced information about targets is available at minimal expense to anyone connected to the global internet.

The widespread ability to leverage these five offense advantages has resulted in cybered conflict, in which cyberspace is now a central pillar across all forms of transnational system contestation. Cybered conflict allows a mass of actors to roam freely from covert espionage and criminal theft through large-scale economic looting and massive information extraction to cyber-kinetic action, often simultaneously.[9] A global underground cybercrime market sells the tools needed to attack precisely and detect others' poorly masked tools.[10] The complexity of this system and absence of governance have increased the potential harm to integrated national systems.

Sources of Systemic Surprise and Cyber Power

Before these offense advantages emerged, two major systemic sources of potential societal surprise from complex technologies were already developing.[11] The first was the centrally positioned single large-scale enterprise from which unintended adverse outcomes enabled by its internal sociotechnical complexity could ripple out to harm other systems. The 1979 accident at the Three Mile Island nuclear energy plant is an example.[12] Equally, a single and unique technology used ubiquitously could provide the same critical vulnerability across a multitude of otherwise independent firms or institutions.[13] This is the industry "standardization trap," in which a widely used critical technology can become a national Achilles' heel if multiple unrelated institutions simultaneously suffer the same failure by accident or sabotage. An example is the installation by the entire gas and oil industry of hundreds of thousands of putatively updated valves with the manufacturer's standard hard-coded (read: unchangeable) password to be used over unsecured internet connections for central monitoring and control of critical national energy pipelines.[14] In the precybered era, there were natural geographical "edges" across the wider social system that dampened the systemic effects such failures could impose.

A second major source of systemic surprise is large-scale collections of enterprises deeply interlinked in operations and often representing critical infrastructure of the nation. As these firms have digitized, their networks, software, equipment, and talent have frequently been shared, mirrored, or made mutually dependent on some third-party node. For example, Amazon's third-party cloud services failed for four hours in 2017 because of a mistyped debug command that put a wide variety of enterprises, whose services and products are essential to a large portion of the population, off-line, costing hundreds of millions of dollars.[15] When one of the most critical infrastructure sectors is disrupted by a nasty, complex system surprise, it often takes down others.[16] When electrical power fails across a wide swath of territory, the loss of energy disrupts food supply (no refrigeration or cash registers), transportation (no electric buses, light rail, or streetlights), and, of course, telecommunications (no internet or mobile-phone towers).[17] These conglomerated infrastructural sectors have also lost their "natural edges" with the advent of cyberspace; they once tended to be regional, limiting harm to their respective regions. Now the harm reaches globally.

It takes adversaries and access, however, to make those ugly organizational surprises into national security threats and profoundly reduce the effectiveness of any remaining natural edges in impeding the spread of a major disruption. The advent of global cyberspace provided two additional adversarial sources of systemic surprise. One is the global mass of moderately skilled, increasingly organized "bad actors." The second is the smaller community of highly skilled "wicked" actors, or "wizards," employed by states or transnational criminal organizations.[18] Bad actors—criminals, hacktivists, and malicious experimenters—use the five offense advantages to reach into other nations' enterprises, civil organizations, homes, networks, services, and products at will.[19] The multiplicity of access points, motivations, and actors involved and dispersion of targets significantly increase the potential for harm.

The wicked actors, the wizards, are even more dangerous as sources of societal surprise. This subset of bad actors is exceptionally skilled and, being employed by state or transnational criminal organizations, financially secure. Wizards skillfully roam through critical infrastructure, governments, and economic sectors, anywhere in the target nation's systems, often for years and if their effects are eliminated often return.[20]

Given these four major sources of societal surprise, societies now face potential cascades in which a containable failure can be deliberately stimulated or enhanced into a rogue nasty outcome threatening the entire nation's socio-technical-economic system, as well as those of allied or connected states. These bad and wizard actors have already reached into the online connections of critical social, technical, or economic systems. For example, systemic harm has come from indiscriminate blackmailing for cash (WannaCry), targeted disruption of services to bully the providers or their state leaders

(BlackEnergy), and wide destruction of files, desktops, and services to clients (NotPetya, Shamoon).[21]

Many states now employ these offense advantages and incorporate the acquired foreknowledge of an adversary state's societal-surprise sources into their cybered-conflict campaigns for economic, technological, and political advantage. The very recent explosion of public revelations about Huawei demonstrates this exploitation. In Huawei's case, its public veneer as solely a successful, commercial international corporation has been challenged by its now-public ties to the ruling Chinese Communist Party (CCP) and the Chinese Ministry of State Security, as well as leaked e-mails demonstrating corporation-wide intellectual property–theft bonuses for Huawei employees worldwide.[22] For democratic civil societies, by 2014 alone the costs of these campaigns constituted the "greatest transfer of wealth in human history," a great deal of it due directly to Chinese wicked actors in state institutions or otherwise internationally accepted corporate offices.[23]

Thus, the four sources of societal surprise and the offense advantages of the shoddy cyber substrate challenge the cyber power of any nation. A robust cyber power addresses all four sources of surprise in a whole-of-society strategy. Acting at the correct scale in a strategically and institutionally coherent defense, such a nation ensures systemic resilience across the first three sources of surprise and uses forward disruption directly against the wizards. A weak cyber power leaves one or more of its sources of surprise unprotected, usually private-sector enterprises. Democratic governments are more reluctant to intervene in the operations of private enterprises—even to improve their cyber resilience—than are their authoritarian counterparts. To date, no state has demonstrated sufficient strategic coherence across all four sources of surprise to be considered a robust cyber power. However, some governments are experimenting more than others, and they are mostly authoritarian.

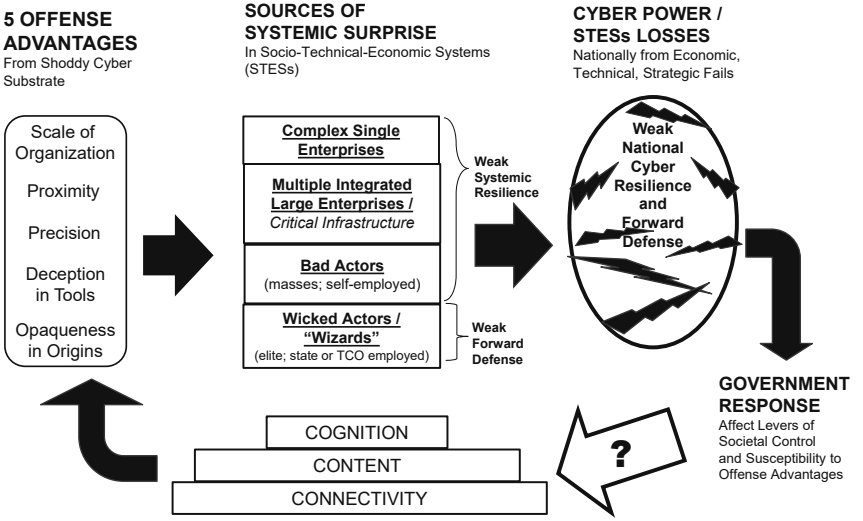
Governance Responses to Societal Surprise

National cyber power depends on how the state balances its responses to the sources of systemic surprise. The current structure of cyberspace offers three broad levers of societal control for this purpose.[24] First, a government can throttle network *connectivity* across specific regions, groups, software combinations, or equipment across its nation. Second, authorities can regulate the *content* traveling across networks, from software to media. Third, using their control of connectivity and content, officials can strongly influence *cognition* away from what is commonly believed to be true but considered undesirable by the authorities and alter the automated processes that sustain those beliefs digitally. Figure 1 shows the complete model in which the five offense advantages

enhance the four sources of societal surprises and subsequent losses in national cyber power, thereby inducing government responses across three levers of societal control to curtail these losses and systemic surprises.

FIGURE 1

Cybered Conflict Potential Model



TCO = transnational criminal organization

Authoritarian and democratic states disagree on whether such levers are legitimate, effective, or feasible. Authoritarian leaders tend to view all three as arenas for government action to maintain regime control. For these leaders, the main question has always been feasibility—Do they have the tools to control circumstances and prevent rebellion? In the precyber era, it was routine for governments to own the telecommunications sectors of their nations, using monopoly control of the underlying physical connectivity and manipulation of content to control cognition in the "mind of the people." China, in particular, has shown that even a prosperous state, well on its way to cyber superpower status, may yet continually seek to strengthen central (in this case party) control of the connectivity and content of its national networks to manipulate the cognitive biases of its population.[25] "Taking away developing countries' ability to control public opinion through internet controls and surveillance would result not in more openness, but instead in 'blood' and 'hatred,'" stated one former senior People's Liberation Army officer in 2015.[26]

The "China model" emphasizes national internet sovereignty, and the CCP continues to advance its methods for screening its internet for politically unacceptable content,

routinely manipulating connectivity and content to control the cognition of its own citizens as well as of its overseas economic targets and partners. As a strict regulator of the national cyber backbone, the party has dampened and redirected any citizen demand for internet political freedom.

The CCP is also using the offense advantages and associated tools against Westernized businesses and governments, both opportunistically and in campaigns.[27] China is seeking to be the global leader in artificial intelligence (AI) and quantum calculations of "big data." It envisions fully automated systems led by AI learning and operating at quantum speeds in the future. The transition to a digitized, centralized, and automated control of all three societal control levers makes the export of control tools to allied authoritarian nations easier.[28]

In contrast, consolidated democracies view some aspects of societal interaction as off-limits for their governments, including the cognition and (generally) the content levers. Their defense strategies tend to focus narrowly on more-technical questions of the safety of connectivity from criminals or malicious actors and online privacy of citizens. Malfeasance by other states or advanced criminal actors, not deviance or dissent among their citizens, has been their main concern for two decades. Until very recently, content online in democracies is usually of governmental interest only to the extent that it is manipulated by organized bad actors. Law enforcement has the lead here against the massive bad-actor source of surprise. Government cyber, military, or signals intelligence (SIGINT) agencies focus on wizard campaigns from state-level adversaries and also do not see content manipulation as a legitimate lever to be used domestically in response to nation-state sources of societal surprise.[29] This deeply embedded legitimacy limit is one reason democracies are struggling with election tampering; it is content manipulation by authoritarian adversaries who are well practiced in such campaigns, unlike the democratic defenders.

Rising Multiple Internets

From these differing responses to the offense advantages and systemic surprises of cyberspace have evolved two incompatible domestic approaches to cybered governance now contending for global primacy.[30] No single international governance system can easily accommodate leaders who routinely seek to control all three levers as well as leaders who refuse to do so. Because the main competitors perceive that there needs to be only one form of governance of the global internet, the result is a system-versus-system struggle. As the global web is currently architectured and coded, it appears that the international cyber substrate can accommodate the China model inside that nation and the democratic, civil-society model inside established democracies but not both in a unified global regime.

On one side, it has been exceptionally difficult for established democracies to give up the early dreams of one, open, free, borderless internet. These communities have a "survival algorithm" that embraces transparency, tolerance, and trust. Their cultures encourage the free flow of information that they consider essential to modern, open democratic societies.[31] This bias toward open exchange discourages content and cognition manipulation as a response to what is often viewed as criminal, rather than adversarial, cyber behaviors.[32] From the internet's outset, the then-dominant Western civil societies demanded an open, global cyberspace—both inside and outside national borders—unfettered by states with sharply different notions of governance and its restraints, especially China. The more the internet's embedded presumptions and openness to abuse induced these societies' STESs to integrate globally, the more these basic incompatibilities were fated to be in friction and to spill over into cybered conflict.[33]

It is difficult to imagine China giving up its ambition to be the central cyber power, guiding the world's technological and economic sectors. Leaders of this rising state have, as noted, explicitly rejected Western civil-society values and internet openness. Their officials and state champions are actively seeking allies, ports, economic client states, complicit autocrats, and coercive influence over the developing world to achieve the influence, respect, and access to resources accorded a great power.[34] They openly speak of using their economic, demographic, and growing cyber power—overwhelming in its scale to those of nearly all other nations—as global leverage.[35] China since 2013 has accelerated domination of its own systems across all three elements of cyber control, and Xi Jinping speaks of his desire to "reform the global governance system" according to Chinese preferences.[36] In the past few years, Xi's representatives have declared that China wishes to be a "rule maker, not rule taker."[37]

In this quest for global dominance, China possesses two major advantages over any other single nation, to include the United States: demographic and economic scale, and strategic coherence in its pursuit of superpower status. China has four times the population of the United States and annually produces eight times more science, technology, engineering, and mathematics (STEM) graduates. Moreover, over 40 percent of STEM students graduating from American schools come from other nations (including China). China invests 80 percent of its government research-and-development (R&D) expenditures in advanced experimental research—compared with the U.S. 62 percent. While the two countries are currently roughly even in their national expenditures on R&D, the U.S. rate appeared to plateau in 2015, while the Chinese rate has been on a steady upward trend since 2001.[38] China is seeking both foreknowledge and resources by leveraging the offense advantages, its scale, and strategic determination. Its efforts have been paying off well for two decades.

Today, as the preeminent *authoritarian anchor-state,* China has squared off with the key *democratic anchor-state* (the United States) in an accelerated cybered conflict. It is a peace-to-war spectrum of system-versus-system contestation, based on the shoddiness of cyberspace and a nonstop "SIGINT struggle for position combined with market share capture to provide R&D flows leading to recurring technological gains, which, in turn, can be converted to leadership of other economic sectors and to military advantages."[39] The implications for future conflict are profound, as economic and political power shifts between them.[40] The United States has accused China of deliberately stealing intellectual property to fund and further its meteoric advance economically and technically. "Nations continually try to change the rules or regimes governing international economic relations in order to benefit themselves disproportionately with respect to other economic powers."[41] The friction is worse when the competing states have been locked into an integrated global system. Neither the United States nor China is able simply to acquiesce to the other's vision for cyberspace.

Fully blending these cybered national systems using a democratic-civil-society global regime and rules-based governance model is, as noted, not an option. With every major state increasingly feeling under cyber siege and interested in defending its "own" cyberspace, the "globally integrated" cyberspace is dividing into national jurisdictions—a "Cyber Westphalia."[42] But over two hundred nations with their own cyberspaces will not survive long in the international jostling for power, influence, and control. Only peers can negotiate, coexist, and mutually constrain. With no peers, the larger and unified actor, ceteris paribus, is likely to determine the nature of relationships and the direction of benefits.[43] Chinese scholars are increasingly predicting an "inevitable" structural change in the global regime and a shift toward Chinese preferences, a prospect that portends unavoidable conflict between the United States and China.[44] The scale imbalance, coupled with China's strategic dedication to economic exploitation of democratic socio-technical-economic systems, increases the chances of escalation, to include physical attacks.[45]

Democratic Response: Cyber Operational Resilience Alliance

Conflicting approaches to global governance for a deeply digitized world have created a cybered "battleground short of traditional war" between the established democracies and the rising authoritarianism of the rest of the world, stimulated by the successful China model. Command of the technologies, operations, transparency, trustworthiness, coercive possibilities, and economic value creation of the underlying cyberspace substrate is at stake.[46] In many ways, China has already excelled in using its scale, strategic coherence, and internal and external leverage of the five offense advantages and levers of state societal control against democratic economies and their global influence. Its state

champions, most notably Huawei, have engaged in massive deceptive and R&D extractive campaigns for years, as well as bribing, bullying, and blackmailing individuals and firms in order to displace Western corporations in global markets, while its hackers conduct "patriotic hacking" on foreign firms. China-based cyber warriors use the noise of the global mass of bad actors, as well as their tools, to operate inside democratic states for espionage, extraction, and preparation of future leverage against economic and network dependencies. Meanwhile it continues to use AI surveillance research and, in such test cases as the Uyghur province, to increase its strategic command of its internal three levers of cyber control, experimenting with how to deflect foreign intrusions, impose control, and export the tools for so doing to the leaders of smaller allied states, such as Zambia.[47]

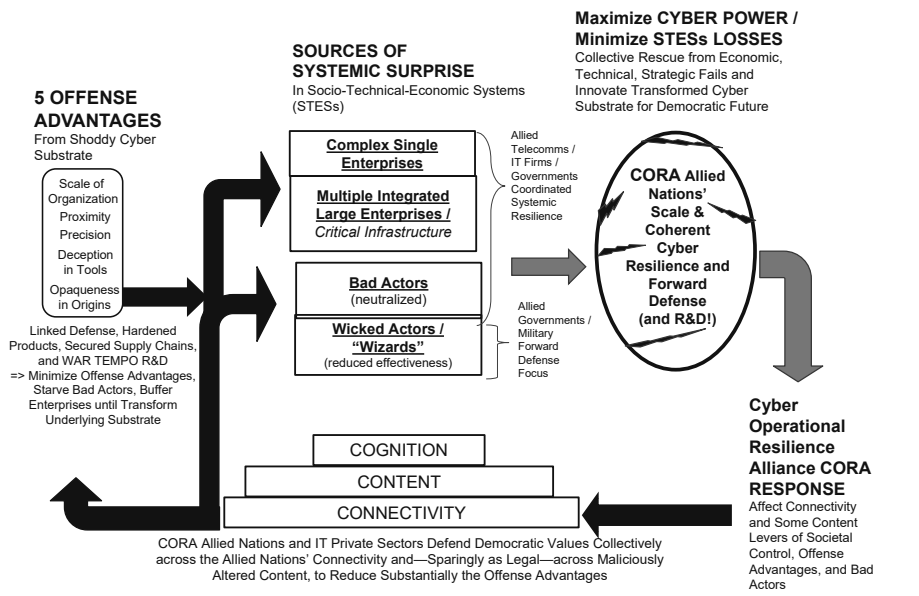
There are few easy options for democracies, with their open internet and their private or public enterprises, but there are indicators of what is needed if they are to change the current negative trends. Consolidated democratic civil societies need commensurate scale and strategic coherence, built on robust cyber power, to defend their economic well-being and combined technological generativity going forward. They need to transform the underlying cyberspace into what it was intended to be: a securable interactive space operating under democratic rules of governance. First and foremost they need to accept a different narrative: that they will have to survive as a minority group of states in a much larger, cyber-hostile, authoritarian world increasingly answering to the preferences of the largest actor (China). Second but no less important, this community of about forty established democratic states must unite so as to scale up to demographic, economic, and technological peer status with China. They need to combine in such a way that adversarial and criminal uses of the five offense advantages are profoundly mitigated in the process.

This community does, however, have one large usable advantage—a shared cultural legacy that encourages cooperation, not just coexistence.[48] Its members have seventy years of collective defense, market, and shared professional institutions. The established democracies also have a solid basis on which to build and from which to share a securable, rule of law–driven internet. Taking the established democracies alone, there are over nine hundred million educated citizens well embedded in the new digitized world. These nations host among them a large community of private-sector actors in their telecommunications and IT capital-goods sectors who are the victims of Chinese theft of product value and control and who face increasingly grim futures as the large Chinese state champions eliminate their global and often domestic market viability. The futures of the democracies around these private-sector actors will determine their own futures as well; they too can participate in—and benefit from—the national cyber defense and the cyber transformation process collectively.

To mitigate the full set of offense advantages at the scale and with the strategic coherence needed and to become robust cyber powers despite being minority states, the consolidated democracies need to join in a *cyber operational resilience alliance* (CORA), a structure that cooperatively ensures the community's whole-of-society cyber defense in the near term and its longer-term cyberspace transformation. The CORA's goals would be to defend now against the permeation of Chinese preferences across global cyber and economic space and so buy time to achieve the ultimate diminution of the sources of cyber systemic surprise without having to use all three levers of societal control. That is, the ultimate purpose of the CORA is to keep these economies and democracies healthy and defended while enacting the complete transformation of the underlying internet into something secured and democratic for the longer term.

The CORA is not a debating forum. It operationally blends the cyber defenses (involving uniformed and government civilians) of aligned nations with the telecommunications that are the cyber backbones to these nations and with the critical IT capital-goods industries that provide the tools, talent, and equipment enabling national cyberspaces to function.[49] The national cyber assets of allied governments operate closely with those of others to generate complementary legal regimes, shared surveillance, and direct-response assets. Figure 2 shows the areas of operation of the CORA.

FIGURE 2
Cybered Conflict Whole-of-Society Adaptation Model—CORA



To address all four sources of systemic surprise and produce robust cyber power for all member nations, the CORA embraces the private sector. That sector's institutional architecture ensures trade with the rest of the world while engaging the telecommunications sectors and IT capital-goods industries across nations in the collective defense of their societies. Key to the private sector's buy-in is widespread recognition among IT capital-goods industry leaders that just as Huawei looted and displaced the formerly large telecommunications equipment firm Nortel, China's state champions, with their IT/AI/quantum policies, have no intention of allowing the Westernized firms to play major roles in global markets over the long term.[50] As witnessed by the rapid displacement of local firms inside democracies by the Chinese in the solar panel market in a few short years, Westernized firms have no great future potential if authoritarian states succeed in dominating markets within the democracies themselves.[51] One may compete vigorously in markets in the rest of the world, but it is no longer possible to embark safely in small joint ventures with any of the rising cyber hegemon's IT-related firms, given the current shoddy internet.

These telecommunications and IT capital-goods firms, being defended by the CORA as well as defending it, are considered "allied protected sectors." They and their governments invest in operational coverage of gaps in the defenses of the telecommunications backbone, networks, and endpoints and in the creation of secured basic technologies. In return, they are provided the single democratic community market, more than nine hundred million strong, free of authoritarian-proxy corporate subversion, ownership, or tainted competition.

The allies must use the time that the CORA buys them to invest in basic R&D to build a democratic, secured, advanced foundation for the future democratic cyberspace. Whatever the longer-term and most effective path for this small community of consolidated democracies may prove to be, it will certainly be aimed at reducing the authoritarian abuse of the community's shared cyber substrate, the key to its societal functions and well-being. Cybered conflict is challenging for any state: an arena of easy offense, multiple systemic surprise sources, gaps in control-lever defenses, incompatible state-systemic cultural instincts and governance preferences, and an inherent and heavy scale advantage for a regime-disruptive rising state. The CORA countries will be institutionally preparing the considerable technological innovation for this new post-Western internet age, even if its benefits are limited at first to member countries of the alliance. CORA buys a chance to make up for two squandered decades of rising cybered conflict in which leverage was ceded to authoritarian regimes, a chance to develop, concertedly and collectively, a securable cyberspace along democratic values.

DOD Strategic Learning and Recommendations

Implementation of a CORA has different implications for the roles that military services may play in various nations, depending on their current ones. If a military is the central locus of computer knowledge in a government, then its forces will play a larger role than that of a nation in which a civilian signals intelligence agency or a police agency has that distinction.[52] In the United States, the Department of Defense—containing both the National Security Agency and U.S. Cyber Command—directly influences the strength of the nation's cyber power. So long, however, as DOD's military role was confined to defending its own networks and reacting to—rather than disrupting—wizards, the U.S. government could not employ that critical source of scarce capabilities for defense across all four sources of surprise. This narrow view dominated until the end of the first decade of this century, reflecting a dated understanding of the whole-of-society cyber defense that a new reality demands.

The 2018 *DOD Cyber Strategy* evidences strategic learning about the nature of rising authoritarianism and a conflictual, digitized world. The unclassified summary states, "We will defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict. We will strengthen the security and resilience of networks and systems that contribute to current and future U.S. military advantages. We will collaborate with our interagency, industry, and international partners to advance our mutual interests."[53]

In a welcome addition to the language of its 2015 predecessor, this strategy also offers to help defend a critical portion of the interdependent enterprise: "The Department seeks to preempt, defeat, or deter malicious cyber activity targeting critical American infrastructure that could cause a significant cyber incident regardless of whether that incident would impact DOD's warfighting readiness or capability."[54] The unclassified summary acknowledges wicked actors as collectively a major source of societal surprise, one that must be disrupted, deterred, or pursued *persistently* and in ways different from those by which the global mass of bad actors is opposed.[55] DOD also sees its defense role more expansively, with a mission to defend the nation, including key domestic (and likely private-sector) portions beyond those critical to its warfighting capacity. The central challenges born of a flawed and adversary-exploited cyberspace substrate underpinning the entire nation have thus been recognized by a government that traditionally has preferred the clarity of wartime (kinetic) versus peacetime, of military operations separate from civilian activity, and of foreign security as distinct from domestic struggles.

Gaps in learning remain, especially with respect to achieving the scale and strategic coherence needed to match Chinese ambitions. The CORA represents a collective response, but its implications for militaries are only just emerging. While the 2018 *DOD*

Cyber Strategy leans far forward of its predecessors with respect to whole-of-society defense, American military leaders still struggle to accept the existential challenge, particularly the reality of China's scale and the fact that democracies are a minority of states globally.[56] In fact, the document treats China and Russia as if they pose challenges of the same type. Yet only China possesses the scale and strategic coherence to change the global system.[57] This strategy document does not acknowledge the unique existential threat presented by China or extend defense obligations to all parts of democratic society. This broader narrative is necessary to update the expectations of conflict for a military facing new systemic roles no less critical than have been their kinetic roles. Figure 3 captures alternative futures.

FIGURE 3
CORA: Scale and Strategic Coherence Survival Imperative for Allied Democracies

SCALE (IN SOURCES OF SYSTEMIC FOREKNOWLEDGE)	STRATEGIC COHERENCE (ACROSS CYBER JURISDICTION[S])	
	LIMITED	SYSTEM-WIDE
INDIVIDUAL Democratic civil society	**cyber status quo,** and rising cyber vassaldom	**Cyber Westphalia** and more slowly rising cyber economic vassaldom
COLLECTIVE Democratic civil societies	*Western global cyber domination led by U.S. preferences, anticipated from 1990s on (expired option)*	**cyber operational resilience alliance (CORA**)

While the *DOD Cyber Strategy* summary calls for expanding partnerships and alliances, the language suggests a narrow view of both allies and private-sector partners.[58] To wit, "the Department will build trusted relationships with private-sector entities that are critical enablers *of military operations*."[59] Shortly thereafter, the summary document highlights the reinforcement of civil-society norms in global cyberspace as a military obligation. While the former is too little, the latter is a distraction. The CORA concept presumes that global norms have already passed out of the hands of democratic nations, including the United States, and will eventually reflect Chinese or more generally authoritarian preferences. There is no particular role for any single democratic nation's military in changing that reality. Rather, it is only with a CORA that the already roughly agreed-upon democratic norms continue to exist among the members banding together to make it so for themselves.

Furthermore, private-sector entities dedicated to supporting military operations are already under considerable regulation in most democracies. It is the sectors that are not currently viewed as critical to military operations but that are vastly important to

wider society that need more reciprocal and collaborative relationships with their nation's defenders. Two sectors in particular are exceptionally critical to the survival of the nation and its CORA allies: telecommunications and IT capital goods. It is through relationships with these nontraditional partners that the military's capacities, missions, and resources will collaboratively and persistently ensure the defense of the entire nation. In short, allies are neither secondary nor backups, and private-sector partners are not limited participants in national defense. Both are existentially critical in a cybered-conflict-ridden and largely authoritarian world.

To judge by the *Cyber Strategy*'s summary, the underlying document is missing appropriate emphasis on types of adaptations and innovations needed to prepare the military to defend from a minority position in a post-Western, deeply digitized world. It makes the perennial call for more cyber talent and in-house use of more secure or advanced technologies, including clouds, scalable computing, and crowdsourcing. However, the document also reiterates the 1990s mantra that commercial off-the-shelf (COTS) acquisition will reduce expense and difficulty in maintenance and upgrades. Ironically, a COTS preference could be justifiable but only in a CORA world where the IT capital-goods industry was a full partner in the defense of the member states, engaged in collective defense as well as vigorous international trade, generativity, innovation testing, contributions to wider R&D learning, and production. If Apple's iPhone was made within CORA member states, it would not have, as it does today, a Chinese-required chip enabling government surveillance were that phone to enter China.[60] However, the CORA is not yet established, and the way forward begins with the recognition that reliance on a highly insecure cyberspace built on COTS is in large measure what made the Department of Defense as vulnerable as it has proved to be. Preparing the organization for different relationships with allies and private-sector enterprises is a critical strategic need.

The Cyber Operational Resilience Alliance is meant to buy time to remake the underlying technology of cyberspace with a massive effort in R&D jointly pursued by IT capital-goods players, universities, start-ups, enterprises, and governments (including their militaries). The Defense Department should begin now to work out systemic and specific solutions with private- and public-sector partners, working jointly on testing, refining, implementing, and assessing the fruits of this transformational R&D for the whole society and across the alliance. DOD cannot regain the singular role it had in the history of computing in the Westernized world. But neither should it abandon the defense of the nation to the vagaries of commercial budgets and profit-focused leaders of IT enterprises. It has the wizard capabilities, foreknowledge, and resources to do otherwise.

Above all, organizational reform must be guided by a strategy for collective survival. Otherwise, well-intentioned military leaders may evolve strategies, capabilities, and institutions that are incompatible with a CORA. Reforms, technology updates, operational innovations, and institutional learning need to proceed on the basis of a vision of democracies united operationally in cyberspace. The scale of threats in the future world will be unlike that of any the United States has faced since the Revolutionary War.[61] Then, only by combining efforts did the individually weak thirteen states prevail. Today there are about forty consolidated democracies constituting about 10 percent of a much larger global population that is steadily becoming more digitized and more authoritarian. If democracies are to survive, they must work operationally and persistently in a CORA. They need to partner with their private sectors to transform, at a wartime tempo, the underlying cyber substrate into one that is securable, generative, and imbued with democratic values of openness, transparency, and trust. Military strategies of democratic states across all domains—cyber, maritime, air, space, and land—will need to evolve toward this collective reality to survive.[62]

Notes

The ideas in this chapter are solely those of the author and do not reflect the positions of the U.S. government, the U.S. Navy, or the U.S. Naval War College.

1. *Department of Defense Cyber Strategy* (Washington, DC: U.S. Defense Dept., April 2015), https://archive.defense.gov/.
2. U.S. Department of Defense [hereafter DOD], *Summary [of the] Department of Defense Cyber Strategy 2018* (Washington, DC, 2018), https://media.defense.gov/.
3. For more on the naiveté, see A. Boulanger, "Open-Source versus Proprietary Software: Is One More Reliable and Secure than the Other?," *IBM Systems Journal* 44, no. 2 (2005), pp. 239–48; Rob Frieden, "Without Public Peer: The Potential Regulatory and Universal Service Consequences of Internet Balkanization," *Virginia Journal of Law and Technology* 3 (1998), p. 1; and Timothy S. Wu, "Cyberspace Sovereignty: The Internet and the International System," *Harvard Journal of Law and Technology* 10 (1996), p. 647. For more on greed and dismissive attitudes, see Bala Iyer, Chi-Hyon Lee, and N. Venkatraman, "Managing in a 'Small World Ecosystem': Lessons from the Software Sector," *California Management Review* 48, no. 3 (2006), pp. 28–47; K. Munro, "Safe to Shelter under a Mac?," *Infosecurity Today* 3, no. 5 (2006), p. 40; Daniel Geer et al., "Cyberinsecurity: The Cost of Monopoly; How the Dominance of Microsoft's Products Poses a Risk to Security," *Computer and Communications Industry Association (CCIA),* 2003, www.ccianet.org/papers/cyberinsecurity.pdf, reposted *CyberInsecurity Reports,* www.totse2.net/totse/en/technology/computer_technology/cyberinsecurit171812.html; and Charles Arthur, *Digital Wars: Apple, Google, Microsoft and the Battle for the Internet* (London: Kogan Page, 2014). For more on this hubris, see William Pfaff, *The Irony of Manifest Destiny: The Tragedy of America's Foreign Policy* (New York: Bloomsbury USA, 2010), and M. Scheuer, *Imperial Hubris: Why the West Is Losing the War on Terror* (Dulles, VA: Brassey's, 2004).
4. See David R. Johnson and David Post, "Law and Borders: The Rise of Law in Cyberspace," *Stanford Law Review* 48, no. 5 (1996). This claim has emerged also in the passionate

embrace of "blockchain" technology and "smart contract." See Shermin Voshmgir, "Disrupting Governance with Blockchains and Smart Contracts," *Strategic Change* 26, no. 5 (2017).

5. It is difficult to overstate the twenty-plus-year love affair of Western democratic political and corporate leaders—and IT community—with the internet or how rose-colored their vision of it was. See J. P. Barlow, "A Declaration of the Independence of Cyberspace," *Electronic Frontier Foundation,* 1996, https://www.eff.org/, and "The Future of the Internet: A Virtual Counter-Revolution," *The Economist,* 2 September 2010. For elaboration on this see Chris C. Demchak, "Uncivil and Post-Western Cyber Westphalia: Changing Interstate Power Relations of the Cybered Age," *Cyber Defense Review* 1, no. 1 (2016).
6. The acronym "STES" was devised by the author as an attempt to capture how the integration of cyber offense into the modern world forced the reelevation of economics—formerly dismissed by key post–World War II international relations scholars as "low politics"—into the top tier of national security concerns. Jean-Marc F. Blanchard, Edward D. Mansfield, and Norrin M. Ripsman, "The Political Economy of National Security: Economic Statecraft, Interdependence, and International Conflict," *Security Studies* 9, nos. 1–2 (1999), pp. 1–14; Robert D. Blackwill and Jennifer M. Harris, *War by Other Means* (Cambridge, MA: Harvard Univ. Press, 2016).
7. Peter Dombrowski and Chris C. Demchak, "Thinking Systemically about Security and Resilience in an Era of Cybered Conflict," in *Cybersecurity Policies and Strategies for Cyberwarfare Prevention,* ed. Jean-Loup Richet (Hershey, PA: Information Science Reference, 2015).
8. John Keegan, *Intelligence in War: Knowledge of the Enemy from Napoleon to Al-Qaeda* (New York: Random House, 2004).
9. Chris C. Demchak, "Cybered Conflict vs. Cyber War," *New Atlanticist* (blog), 20 October 2010, https://www.atlanticcouncil.org/.
10. It is massive, international, and now highly professionalized. There are maintenance contracts like mainstream software services, reliability ratings much like Yelp, and even job and topic specializations among operators and coders. See Parmy Olson, *We Are Anonymous: Inside the Hacker World of Lulzsec, Anonymous, and the Global Cyber Insurgency* (New York: Hachette Digital, 2012), and Misha Glenny, *Dark Market* (New York: Random House, 2011).
11. J. L. Casti, *Complexification: Explaining a Paradoxical World through the Science of Surprise* (New York: Abacus, 1994). There is a healthy literature on "surprise and sociotechnical systems"—a human-oriented subset of "complex adaptive systems" literature. For a seminal work, see T. R. La Porte, *Organized Social Complexity: Challenge to Politics and Policy* (Princeton, NJ: Princeton Univ. Press, 1975), and J. H. Miller and S. E. Page, *Complex Adaptive Systems* (Princeton, NJ: Princeton Univ. Press, 2007).
12. C. Perrow, "The President's Commission and the Normal Accident," in *Accident at Three Mile Island: The Human Dimensions,* ed. David L. Sills, C. P. Wolf, and Vivien B. Shelanski (Boulder, CO: Westview, 1982).
13. See G. Rochlin, *Trapped in the Net: The Unanticipated Consequences of Computerization* (Princeton, NJ: Princeton Univ. Press, 1997).
14. For more, see Patrick Tucker, "Hacking Critical Infrastructure: A How-to Guide," *DefenseOne,* 31 July 2015.
15. Yevgeniy Sverdlik, "AWS Outage That Broke the Internet Caused by Mistyped Command: Amazon Says Tuesday's Mayhem Resulted from Mistake during a Routine Debugging Exercise," *Data Center Knowledge,* 2 March 2017.
16. Melissa Hathaway has argued that there are only three critical infrastructures, on which all others now depend: energy, finance, and telecommunications. See UN University, "The Future of Cybersecurity: A Conversation with Melissa Hathaway," YouTube, 11 October 2017, video, 22:48, https://www.youtube.com/; and Melissa Hathaway, *Cyber Readiness Index 2.0: A Plan for Cyber Readiness; A Baseline and an Index* (Arlington, VA: Potomac Institute for Policy Studies, November 2015), https://potomacinstitute.org/.
17. Hurricane Katrina in 2006 was a classic example of this rippling effect. Midwestern and Northeast blizzards often have similar patterns as well.
18. The term is borrowed from the mathematical concept of "wicked" problems, whose solution is extremely hard or complex. This author is moving to the term "wizard," since all robust cyber powers, including democracies, have them. The IT community prefers the latter. For use of the phrase in more formal work, see "Emerging Trends and Threats for 2013," *NYS*

Office of Cyber Security Monthly Security Tips 8, no. 1 (January 2013), https://its.ny.gov/sites/default/files/documents/2013-01.pdf.

19. A common concern in the early cybersecurity industry was the motivation of malicious hackers. By 2014, however, senior cyber experts, including Gen. Keith Alexander, commander of U.S. Cyber Command, were characterizing all but the most sophisticated actors as hacking "just because they can."

20. The generally accepted name is "advanced persistent threat" (APT), but often the nicknames reflect their origins and the cybersecurity vendors who are publicly following their successes. For example, CrowdStrike uses the following lexicon—"bear" (as in Fancy Bear) for Russian groups, "panda" (as in Deep Panda) for Chinese groups, and "kitten" (as in Charming Kitten) for Iranian finance groups, while Mandiant merely numbers the groups, such as APT19 for Deep Panda. Florian Roth, "The Newcomer's Guide to Cyber Threat Actor Naming," *Medium Online,* [2018], https://medium.com/.

21. Respectively, see Charles H. Romine, *Bolstering Government Cybersecurity Lessons Learned from WannaCry,* testimony before the U.S. House of Representatives Committee on Science, Space, and Technology Subcommittee on Oversight and Subcommittee on Research and Technology, 2017, available from www.nist.gov/; Daniel Wagner, "Infrastructure under Attack," *Risk Management* 63, no. 8 (2016); Iain Thomson, "Everything You Need to Know about the Petya, Er, NotPetya Nasty Trashing PCs Worldwide: This Isn't Ransomware—It's Merry Chaos," *Register Online* (2017), https://www.theregister.com/; and Christopher Bronk and Eneken Tikk-Ringas, "The Cyber Attack on Saudi Aramco," *Survival* 55, no. 2 (2013).

22. So many of these bonuses have recently been reported that it is difficult to identify one or two better-informed sources. See Robin Emmott, "U.S. Warns European Allies Not to Use Chinese Gear for 5G Networks," Reuters, 5 February 2019, https://www.reuters.com/, and David Bond and James Kynge, "Huawei under Fire as Politicians Fret over 5G Security," *Financial Times,* 2 December 2018.

23. Pierluigi Paganini, "Cyber-Espionage: The Greatest Transfer of Wealth in History," *H+ Magazine,* 1 March 2013.

24. Dan Kuehl, "The Information Revolution and the Transformation of Warfare," in *The History of Information Security: A Comprehensive Handbook,* ed. K. de Leeuw (Amsterdam, Neth.: Elsevier Science, 2007).

25. Greg Austin, *Cyber Policy in China* (Marblehead, MA: Wiley, 2014); Florian Schneider, "China's 'Info-Web': How Beijing Governs Online Political Communication about Japan," *New Media & Society* (2015).

26. Hao Yeli, vice chair, China Institute for Innovation Development Strategy, former senior officer PLA General Staff, speech, September 2015. See Paul Mozur, "Chinese Official Faults U.S. Internet Security Policy [Ms. Hao Yeli]," *New York Times,* 29 September 2015.

27. For an exceptional overview of China as a rising cyber power, see Nigel Inkster, *China's Cyber Power* (London: Routledge, 2018).

28. For an externalized expression of internal content with cognition effects by China, see Frank Langfitt, "How China's Censors Influence Hollywood," *NPR Morning Edition,* aired 18 May 2015.

29. There are exceptions, such as child sex trafficking and Nazism in Germany, and today there is serious concern with "inauthentic" news intended to alter elections.

30. Even the terms for what is emerging differ starkly—*cybered conflict,* "cyber war," the Russian "hybrid war," and even the Chinese "wars under conditions of informatization." All reflect highly variable approaches to cybered conflict among, and response levers available for use by, states in a deeply cybered, non-Westernized world. See Christopher S. Chivvis, *Understanding Russian "Hybrid Warfare" and What Can Be Done about It,* testimony presented before the House Armed Services Committee, 22 March 2017, Washington, DC, https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf; Kevin L. Pollpeter, Michael Chase, and Eric Heginbotham, *The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations* (Santa Monica, CA: RAND, 2017); and Elsa B. Kania and John K. Costello, "The Strategic Support Force and the Future of Chinese Information Operations," *Cyber Defense Review* 3, no. 1 (2018).

31. "Culture is the collective programming of the mind that distinguishes the members of one group or category of people from others." Geert Hofstede and Gert Jan Hofstede,

Cultures and Organizations: Software of the Mind (New York: McGraw-Hill, 1991), p. 5.

32. Tomas Englund, "Deliberative Communication: A Pragmatist Proposal," *Journal of Curriculum Studies* 38, no. 5 (2006). It is important to note that there are other cultural traits not included in this discussion—such as collectivism versus individualism and aggressiveness versus nurturing. For example, see Peter Magnusson et al., "Breaking through the Cultural Clutter: A Comparative Assessment of Multiple Cultural and Institutional Frameworks," *International Marketing Review* 25, no. 2 (2008).
33. Josh Chin, "The Internet, Divided between the U.S. and China, Has Become a Battleground," *Wall Street Journal,* 9 February 2019.
34. Liu Lin, "Strategic Strongpoints along the 'Belt and Road' and Building Military Diplomacy ["一带一路"沿线战略支点与军事外交建设]," *World Affairs* [世界知识], no. 17 (2017).
35. James Reilly, "China's Economic Statecraft: Turning Wealth into Power," *Lowy Institute,* 27 November 2013, lowyinstitute.org/.
36. Ibid.
37. It is not clear who first said this; however, it has been prominently used in the past several years. See Zhaohui Wang, "The Economic Rise of China: Rule-Taker, Rule-Maker, or Rule-Breaker?," *Asian Survey* 57, no. 4 (2017).
38. For population differences, see "Population," *United Nations,* https://www.un.org/en/sections/issues-depth/population/index.html. For STEM graduation rates, see "Human Capital Report 2016," *World Economic Forum,* [2016], www3.weforum.org/; and HSBC Bank USA, "China's Journey from Factory to Forerunner," *Bloomberg,* 5 December 2017, https://sponsored.bloomberg.com/. For the difference in experimental research, see CSIS China Power Project, "China Power: Is China a Global Leader in Research and Development?," *China Power,* https://chinapower.csis.org/. For GDP and R&D figures, see "Research and Development Expenditure (% of GDP)," *The World Bank,* 2019, https://data.worldbank.org/indicator/GB.XPD.RSDV.GD.ZS. The United States appears to have plateaued in 2015 at 2.8 percent, while Chinese investment has been steadily rising since 2001.
39. John Mallery, MIT research scientist, private observation, February 2019.
40. Goldman has an excellent discussion of the struggles between rising and declining powers in digitized modern times. Emily O. Goldman, *Power in Uncertain Times: Strategy in the Fog of Peace* (Palo Alto, CA: Stanford Univ. Press, 2010).
41. Robert Gilpin, *The Political Economy of International Relations* (Princeton, NJ: Princeton Univ. Press, 1987), p. 33.
42. The logic of this fragmentation was obvious a decade ago; Chris C. Demchak and Peter J. Dombrowski, "Rise of a Cybered Westphalian Age," *Strategic Studies Quarterly* 5, no. 1 (2011). China has made it clear for some time that it wants to control fully its sovereign cyber jurisdiction. Russia has recently announced that it will have the ability to cut itself off from the rest of the global web at will. Gaycken argued early on for a consideration of "IT sovereignty" by the democracies, especially Germany. Sandro Gaycken, "Does Not Compute: Old Security vs New Threats," *Datenschutz und Datensicherheit—DuD* 36, no. 9 (2012).
43. "Throughout history, the larger configurations of world politics and state interests have in large measure determined the framework of the international economy." Robert Gilpin, "Three Models of the Future," *International Organization* 29, no. 1 (1975).
44. Ibid.
45. A rise in the destructiveness of allegedly interstate campaigns is worth noting. Nobutaka Kawaguchi et al., "Locating Victims of Destructive Targeted Attacks Based on Suspicious Activity Spike Train" (paper presented at the 2017 IEEE Symposium on Computers and Communications [ISCC], 2017), and Kutub Thakur et al., "Impact of Cyber-Attacks on Critical Infrastructure" (paper presented at the 2016 IEEE 2nd International Conference on Big Data Security on Cloud [BigDataSecurity], IEEE International Conference on High Performance and Smart Computing [HPSC], and IEEE International Conference on Intelligent Data and Security [IDS], 2016).
46. "As China and the West race for 5G dominance, two digital powers with very different approaches to technology are staking out their corners." Chin, "The Internet, Divided between the U.S. and China."
47. Sheridan Prasso, "China's Digital Silk Road Is Looking More Like an Iron Curtain: The Funding of Tech Projects in Dozens of

Countries May Well Divide the World [Case of Zambia]," *Bloomberg News,* 10 January 2019.

48. Joseph S. Nye Jr., "Will the Liberal Order Survive?," *Foreign Affairs* 96, no. 1 (January/February 2017), p. 10.
49. For an interesting Chinese perspective on the use of military forces in cyber defense, see a piece written by two authors at the Air Force Engineering University, Xi'an, China. Weiwei Wang and Lan Wu, "Military Participation: The Necessary Way to Maintain Network Sovereignty," in *Recent Developments in Intelligent Computing, Communication and Devices,* ed. Srikanta Patnaik and Vipul Jain (Singapore: Springer, 2019), pp. 627–31.
50. Ibid.; Julian E. Barnes and Josh Chin, "The AI Arms Race: China Is Making Big Investments in Artificial Intelligence and Related Technologies, Looking for Military Advantage—While the Pentagon Is Determined to Keep Its Edge," *Wall Street Journal Saturday,* 3 March 2018.
51. Louise Curran, "The Impact of Trade Policy on Global Production Networks: The Solar Panel Case," *Review of International Political Economy* 22, no. 5 (2015).
52. For example, respectively, in the United Kingdom with the Government Communications Headquarters and in Sweden with the national-level police.
53. DOD, *Summary DOD Cyber Strategy 2018,* p. 1.
54. Ibid., p. 2.
55. "Persistent engagement, in other words, means that the newly elevated Cyber Command will be everywhere, all the time and in all ways." See Jacquelyn G. Schneider, "Persistent Engagement: Foundation, Evolution and Evaluation of a Strategy," *Lawfare* (blog), 10 May 2019, https://www.lawfareblog.com/.
56. Warner argues persuasively that over the course of the internet's history, American leaders have had one key insight per decade, the latest being that adversaries could do to us what we can do to them. This piece argues that it is time for another insight—that the adversaries able to harm us also outnumber us and that the coming international system will hang each of us separately if we do not hang together effectively, operationally, and innovatively. See Michael Warner, "Cybersecurity: A Pre-history," *Intelligence and National Security* 27, no. 5 (2012).
57. Prasso, "China's Digital Silk Road Is Looking More Like an Iron Curtain."
58. DOD, *Summary DOD Cyber Strategy 2018*.
59. Ibid., p. 4 [emphasis added].
60. Scott Kennedy, "The Political Economy of Standards Coalitions: Explaining China's Involvement in High-Tech Standards Wars," *Asia Policy* 2, no. 1 (2006); Mingzhi Li, Xinrui Liu, and Kai Reimers, "Emerging Mobile Platform Competition in China's 3G Era and Beyond" (paper presented at the 8th International Conference on Service Systems and Service Management [ICSSSM], Tianjin, China, 25–27 June 2011).
61. On every aspect of their collective STES, the thirteen colonies were underdogs in the Revolutionary War with Britain. However, the United States was not so economically or strategically vulnerable in World War II, its other major shooting war, or in the Cold War, its only major nonkinetic competition until now. In the former, one had oceans to protect the continent and knew roughly what war would look like; hence, one prepared. Plus, "war" had to be "declared" to force concessions from adversaries. With the advent of the nuclear age, war was anticipated to be different in speed and the extent of fallout versus traditional assaults and ground competition (plus the likelihood of Pyrrhic outcomes). But one knew what bombs and missiles did, hence, by extension, what nuclear weapons could do. The current age is one in which the democracies are outnumbered in a new form of truly systemic conflict that they have only belatedly started recognizing. Their political and economic leaders are still having considerable trouble accepting what year-on-year economic losses in peacetime will mean for their nations' futures as a global minority. The Soviet Union as an economic challenger never had the global ubiquity, determination, or technological capacity of China. However ideological the Cold War, it did not actually intrude on the economic lifeblood of democratic societies as the Revolutionary War most certainly did for the emerging United States. Marc Egnal and Joseph A. Ernst, "An Economic Interpretation of the American Revolution," *William and Mary Quarterly* 29, no. 1 (1972; repr. 1995).
62. For application of this perspective to the maritime domain in particular, see Peter Dombrowski and Chris C. Demchak, "Cyber War, Cybered Conflict, and the Maritime Domain," *Naval War College Review* 67, no. 2 (2014).

CHAPTER FOUR

Advances in Defense

VICE ADM. NANCY A. NORTON, USN, ET AL.

Defensive cyber is a dynamic field. This chapter takes a high-level view and provides vital context for understanding how the defensive cyberspace mission area evolves and outpaces policy, doctrine, and bureaucratic procedures. The U.S. Department of Defense's flexibility in addressing these challenges enables the men and women dedicated to strengthening cyber defense to succeed in protecting the military's information, weapon systems, and technology assets, which are fundamental to national defense and security.

A 2015 intrusion into Pentagon unclassified e-mail accounts caused a temporary shutdown of Joint Staff e-mail service affecting about 4,200 accounts.[1] At the time, U.S. Cyber Command (USCYBERCOM) commander Adm. Michael Rogers said the sophisticated phishing attack was aggressive and showed the adversary's ability to adjust tactics rapidly.[2] Monitoring and quick action caught the cyber attack before serious widespread compromise could take place and allowed the U.S. Department of Defense (DOD) to examine the adversary's campaign-style movements while it adjusted its network security.[3] Two years later, the WannaCry ransomware and NotPetya malware attacks caused billions of dollars in damage worldwide. DOD escaped unharmed.[4] The saving grace in these events was DOD's organized, unified action and active layered defense. These examples shine a light on significant advances over the last ten years in the U.S. military's defensive cyber capabilities and the importance of operating with a warfighter mind-set as a unified joint force within the cyberspace warfighting domain.

DOD has come to appreciate the power achieved by aligning all forty-three DOD components with over 250,000 defensive cyber operators to work as a unified joint force in the cyber fight.[5] Developing a shared understanding of DOD's cyber terrain across components and making priority decisions on the basis of the criticality of military missions and capabilities underpin USCYBERCOM advances in defense.

Global Responsibility with a Warfighter Mind-set

The imperative is to stay ahead of the adversary. Cyberspace provides a sense of anonymity, deniability, flexibility in timing, and a high degree of maneuverability for deceptive actions that attempt to create confusion and erode the strategic position of the United States and its bonds of trust with allies.[6] Given the threat and persistent cyber warfighting environment, USCYBERCOM has integrated assertive defense activities throughout its full-spectrum cyberspace mission areas to protect the Department of Defense Information Network (DODIN).[7]

This comprehensive view starts with understanding that cyber defense goes beyond the administration of technology and networks. It is about protecting national interests and preserving vital partnerships that enable the American military's long-term competitive advantage. Defending networks, on and off the DODIN, translates into protecting the mission supported by the technology. This is the warfighter mind-set.[8]

USCYBERCOM's global responsibility, and specifically that of Joint Force Headquarters–DODIN (JFHQ-DODIN) as the primary synchronizer for defense, influences operations and mission-essential tasks across all four DOD core functions—combatant command warfighting, the services' "organize/man/train/equip," intelligence activities, and business operations.[9] Every DOD function relies on the DODIN in some way.[10]

DODIN operations and defense constitute a layered, or tiered, framework in which individuals, organizations, and categories of organizations play active roles. The DODIN is DOD's complex, classified and unclassified, federation of thousands of networks, information-technology equipment, tools and applications, weapon system technologies, and data. It comprises service-, agency-, and combatant command–constructed networks; the equipment and tools used by those organizations, including mobile devices, internet access points, and connections with nonmilitary entities; the various platform information technologies; programs of record, industrial control systems / supervisory control, and data acquisition; the rapidly emerging cloud environment; and other elements. It encompasses the enterprise, base, post, camp, and station levels.[11] The Defense Information Systems Network, managed by the Defense Information Systems Agency (DISA), serves as the DODIN backbone.[12]

The scope, scale, complexity, and span of control of the DODIN are striking. JFHQ-DODIN's command-and-control mission, along with the necessary authorities, enables the ability to secure, operate, and defend the DODIN and reinforces resiliency in the persistently contested cyber environment. Along with JFHQ-DODIN, there is the Cyber National Mission Force Headquarters (CNMF-HQ), focused on defense of the nation, and Joint Force Headquarters–Cyber (JFHQ-C), focused on supporting combatant commands with offensive cyberspace operations.[13]

Laying the Groundwork for Defensive Cyber: Complexity and a Sense of Order

USCYBERCOM as the Cornerstone for Advances in Defense

U.S. Cyber Command's transition in May 2018 from a subordinate command under U.S. Strategic Command (USSTRATCOM) to an independent command gives the Commander, USCYBERCOM authority to plan and execute operations, actions, and activities for the entire cyberspace warfighting domain. The foundational defensive cyberspace advancement in the last decade is thus USCYBERCOM's designation as the tenth combatant command. This includes authority to direct all DOD components, establish priorities for offensive and defensive operations, and manage operational risk related to cyber.[14] The responsibility and authority cross geographic, functional, service, and DOD agency boundaries with focus on all cyberspace operations simultaneously, as a supported or supporting command.[15]

Command and control, identifying and articulating cyber-related requirements, partnerships, and advocacy are all critical aspects of USCYBERCOM's full-spectrum operations at the strategic level.[16] While the idea of comprehensive cyber operations has been part of the strategic conversation for decades, it was not until the early years of this century that traction was gained. Dramatic changes in information-technology capabilities, an escalation of expectations for speed and access, and diverse ways in which operators pursued cyber defense given the competitive environment with adversaries all contributed to the need for a different organizational construct and approach.

By late 2018, USCYBERCOM had matured its efforts and coalesced its activities into three main pursuits: persistent engagement, persistent presence, and persistent innovation.[17] This strategy centers on leveraging operational information and intelligence from diverse areas to reinforce action as close to the source of malicious activity as possible. The need to be proactive underpins the defend-forward concept, as well as DODIN operations and defense on a daily basis.[18]

A Brief Look Back: Shaping Full-Spectrum Cyberspace Operations

Early perspectives about DOD's information technology focused largely on creating efficiencies and office automation. Over time, dependence on the DODIN as an operational warfighting capability affirmed that the strength of the DODIN is directly related to risk to mission, risk to forces, and operational outcomes.[19] DOD officials realized that while few, if any, competitors could fight and win a conventional fight with the United States, they could conduct asymmetric attacks against the DODIN to disrupt, deny, and in some cases destroy DODIN-enabled capabilities or corrupt, distort, or steal sensitive data and information.[20] DOD's initial focus was to improve the defensive posture of the DODIN.[21] These initial efforts were characterized as "computer-network defense" and

"information-assurance" actions and centered on inspections related to administrative compliance in network changes, such as software programs, updates, patches, and technical actions, and they relied on individual organizations to decide whether, how, and when they would proceed.[22]

Several realities—competition in a new environment, persistent and continuous assault, magnitude of the problem, and scope of vulnerability for the United States—led DOD to name cyberspace a critical part of the global battlespace in the 2004 *National Military Strategy,* which led to deliberate actions to organize cyberspace as an operational warfighting domain by 2009. In part, this included a Joint Staff capabilities-gap analysis, decisions by the Deputy's Management Action Group, and inclusion of cyberspace as a formal operational warfighting domain in the Unified Command Plan (UCP), with the mission assigned to a combatant command having the authority to execute the cyberspace operations mission, and it was followed by establishment of an operational command framework.[23]

USCYBERCOM's early years focused on building out the mission areas for defending the nation and supporting combatant commands. Although the USSTRATCOM commander identified the need in 2011, completing the defensive aspect of the cyberspace framework came in November 2014, when the secretary of defense directed the commander of USSTRATCOM to establish JFHQ-DODIN as a subordinate command to USCYBERCOM. The new entity's purpose was to operate at the operational level of warfare and function as a command-and-control headquarters aligned to the "secure, operate, and defend the DODIN" mission area.[24] The mission assigned to JFHQ-DODIN was to achieve unity of command over all DOD components that conduct DODIN operations or defensive cyberspace operations. This enabled the delegation of the authority to execute three UCP-assigned responsibilities inherent in full-spectrum cyberspace operations: to direct network operations, network security, and network-defense operations across the totality of the DODIN. The establishment of the "secure, operate, and defend the DODIN" mission area established lineage for DODIN operations, security, and defense operations from the UCP-assigned mission, through the combatant commander assigned the UCP mission, through USCYBERCOM, and ultimately through JFHQ-DODIN to all DOD components that conduct DODIN operations, security, and defense operations.

Organizing the Cyberspace Warfighting Domain Operational Framework

Once JFHQ-DODIN was established as a component command under USCYBERCOM to serve at the operational level of warfare, its command became a dual-hat responsibility for the DISA director. Thus, this three-star-level position has two distinct and separate sets of responsibilities to fulfill and organizations to oversee. Administrative support

became DISA's responsibility. DISA, a combat support agency, falls under the purview of the DOD chief information officer (CIO). USCYBERCOM's responsibilities fall under the Goldwater-Nichols Act, and the DOD CIO falls under the Clinger-Cohen Act, which sometimes have differing priorities.[25] However, the JFHQ-DODIN commander's dual hat gives the advantage of direct involvement with and insight from both the CIO policy and acquisition community and the strategic and operational warfighter community. It allows the commander to bridge across policy, acquisition, and advocacy for cyberspace warfighter requirements.

JFHQ-DODIN was empowered, as noted, to achieve unity of command with directive authority for cyberspace operations. This authority is different from all other command authorities, because it is agnostic with respect to the core mission of the organization to which it is applied but is constrained to DODIN operations and defensive cyberspace operations.[26]

In 2017, as JFHQ-DODIN worked toward full operational capability, the organization initiated an effort to define the cyber battlefield and terrain. That same year, Operation Gladiator Shield marked the first time DOD coordinated efforts to organize and direct defensive cyberspace operations for sustained and persistent conflict. JFHQ-DODIN identified forty-three areas of operation on the DODIN and named a commander or director of a DOD component responsible for each.[27]

With the help of JFHQ-DODIN, the components continue to define their areas of operation, the priorities for protection (networks/systems/information), the interdependencies, and the operational-risk assessments. This allows commanders and directors to know their organizations' security risks and understand how the cyber risks affect their mission-essential objectives and assets. Additionally, this information gives JFHQ-DODIN the necessary information for a deeper and broader understanding of the risks to the DODIN as a whole.

Overall, Operation Gladiator Shield created the conditions for seamless and trusted unified action by DOD components in defensive cyberspace operations.

Understanding the Threat Environment: What It Means to Advances in Defense

With cyber as the ultimate asymmetric weapon, cyber defenders naturally look at the threat environment from a broad perspective, considering external and internal conditions and adversaries. Tactics, techniques, and procedures change rapidly, and attempted intrusions often appear from multiple points simultaneously. The nature of the cyberspace environment gives adversaries flexibility, in timing and pace of attacks, that allows for sophisticated campaigns over time. This translates into a high demand

on DOD to ensure that defensive efforts are proactive at every level. The imperative is twofold: first, continuously identify vulnerabilities to networks, systems, and processes; and second, undertake assertive defend-forward actions. Speed and ability to prioritize threats are top requirements for cyber defenders.

External Threats

> *Competitors deterred from engaging the United States and our allies in an armed conflict are using cyberspace operations to steal our technology, disrupt our government and commerce, challenge our democratic processes, and threaten our critical infrastructure.*
>
> SUMMARY DEPARTMENT OF DEFENSE CYBER STRATEGY 2018

Reliance on networked systems, technologies, and instantaneous global communications has created new challenges for DOD as governments, nonstate actors, criminals, extremists, and lone individuals persistently and maliciously exploit cyberspace, targeting individuals and organizations. While adversaries' capabilities, intent, and motivations vary, all can pose threats to the nation's interests and military posture.

As adversary techniques and tools evolve, the divide between state and nonstate actors narrows. The proliferation of malware complicates attribution. Revolutionary advancements in malware influence how adversaries attempt to exploit systems and how network defenders posture to defend.[28] The deployment of new technologies, such as the Internet of Things, Internet Protocol version 6, and 5G telecommunications, increases the number of systems requiring defense and the complexity of cyber defense requirements.

Over the past fifteen years, the cyber and intelligence communities have developed frameworks to analyze adversary cyberspace activity, to assist with attribution, and to understand the adversary's intent, capabilities, and end state. Armed with this analysis, defenders are more prepared to react to adversary activities and future events.[29] The sheer volume and velocity of available data require technical capabilities to process, store, and analyze threat reporting and network data to facilitate a holistic threat picture.

Internal Threats

> *What Snowden taught the NSA [National Security Agency]—and perhaps many people watching NSA—is that it's probably very likely we underestimated the probability and the consequences of an insider.*
>
> CHRIS INGLIS, FORMER DEPUTY DIRECTOR, NSA

Several incidents in recent years involved serious insider-enabled theft of large volumes of classified and sensitive data. Insiders use authorized access and can, wittingly or unwittingly, harm the security of the United States. Malicious insiders include disgruntled employees or former employees motivated by revenge, financial gain, or ideology. These individuals may act alone or may enable activities by others. These actors do not have to possess advanced technical skills, as their regular access may enable malicious activity. Spear phishing and other social engineering–based activity capitalize on unwitting insiders. Less malicious security incidents triggered by unwitting insiders occur frequently and can enable adversaries to exploit vulnerabilities and bypass an organization's layered defenses. The use of unauthorized hardware or software, improper transmission of sensitive data, and the misconfiguration of systems are examples of insider activity that may enable adversary activities. Insider action or inaction conservatively enables 30 percent of all successful adversary activity.[30]

DOD has an Insider Threat Program requiring organizations to establish monitoring programs to help identify and neutralize malicious insider threats. When combined with user training, compliance monitoring, and the inculcation of a cybersecurity culture, the program reduces unwitting insider threats.

In 2015, DOD published the "Department of Defense Cybersecurity Culture and Compliance Initiative (DC3I)" memorandum. The memo recognized that "roughly 80 percent of incidents in the cyber domain can be traced to three factors: poor user practices, poor network and data management practices, and poor implementation of network architecture."[31] The memorandum called for a change in DOD's cyber culture and introduced principles and policies for all personnel accessing, operating, or utilizing DOD information networks.[32] This initiative was one impetus for efforts within DOD that continue today, including enhanced training, more rigorous compliance-based reporting and inspections, and synchronization of defensive efforts under JFHQ-DODIN, with the appropriate authorities to compel action by DOD components.

Big Years, 2017 and 2018: Key Secure, Operate, and Defend Advances

Several advances emerged from Operation Gladiator Shield 2017 or reflect a continual push toward unity of command and control for the cyber domain.

Integrated Campaign Approach. USCYBERCOM and JFHQ-DODIN's campaign approach to planning emphasizes flexibility for integrating military capabilities with interorganizational and multinational partner capabilities. The idea is to analyze and interpret the operating environment and emerging patterns to plan comprehensive responses for effective results.[33] JFHQ-DODIN's first five-year *Subordinate Campaign Plan for Defensive Cyberspace Operations and Internal Defensive Measures,* signed in

December 2017, aligns to USCYBERCOM's Campaign Plan.[34] JFHQ-DODIN's annual orders operationalize long-term plans by focusing attention on near-term objectives. For example, the USCYBERCOM commander approved a twenty-six-point "Fight the DODIN" concept, with several objectives included in the 2019 annual order. The full concept extends into the future and covers tasks for the entire DODIN at all layered-defense tiers.[35]

Cyber Tasking Cycle and Defensive Cyberspace Priorities. In 2018, JFHQ-DODIN implemented a Cyber Tasking Cycle to establish priorities for whole-of-the-DODIN defensive cyber standards across DOD.[36] This is accomplished through daily, weekly, monthly, and quarterly interactions with all forty-three DOD components. The Cyber Tasking Cycle engages cyber operators at all levels—watchstanders in component operations centers, directors of cyber and information-technology operations centers, and deputy and principal commanders and directors of the components. This effort creates shared understanding about defensive cyber priorities at all levels of the DODIN's layered-defense construct and then translates priorities into timely action. Commander- and director-level involvement is key to the success of this effort. Senior executives are part of strategic and operational conversations on policy, operations, and resources. As of early 2019, JFHQ-DODIN's Cyber Tasking Cycle is the only DOD-wide effort with such inclusive and active participation.

JFHQ-DODIN Operations Center. When JFHQ-DODIN transitioned from initial operational capability in January 2015 to full operational capability in January 2018, it shared space with DISA's command center. In August 2018 the USCYBERCOM commander, Gen. Paul M. Nakasone, commissioned a new JFHQ-DODIN Operations Center (JDOC) to bolster the command's capability in fusing operations and intelligence. By late 2018, the JDOC had emerged as the heartbeat of command and control for DOD's defensive cyberspace operations. No other entity has the reach or timely impact of JFHQ-DODIN for DODIN operations and defensive cyber operations. Components gain insight from data collected and analyzed in the JDOC and bolstered by input from other elements of the command. These "fused" data become critical information for overarching defensive operations at all levels within the DODIN tiered construct.[37]

Operational Readiness Inspections, Audits, and Assessments. In October 2017, the JFHQ-DODIN commander and DISA director transferred the DODIN Readiness and Security Inspections directorate from DISA to JFHQ-DODIN, to reorient from a focus on compliance toward operational mission–based, threat-focused assessment. This comprehensive new approach includes Command Cyberspace Readiness Inspections (CCRIs), Command Cyberspace Operations Readiness Inspections (CCORIs), Cyber Security Service Provider Assessments, DOD and Network Security Service Public Key Infrastructure Audits, and security assessments for information networks and systems

throughout DOD, other federal agencies, and selected coalition partners connected to the DODIN. With the USCYBERCOM commander's guidance, JFHQ-DODIN began training components to pick up the compliance responsibility to allow for increased attention to operational risk and mitigation. Initial feedback from components that have gone through the CCRI/CCORI processes has been positive. CCORIs provide new insights into how an organization influences and is influenced by others—revealing critical aspects of interdependencies in cyberspace.[38]

Defensive Cyberspace Fixed and Maneuver Forces. DOD's defensive cyberspace personnel number more than 240,000. These forces represent capabilities across all DOD components working at all levels in the layered-defense construct. They are a globally dispersed, diverse force defending all DOD mission areas.[39] Included in this number are USCYBERCOM forces as well as those within combatant commands, services, and DOD agencies and field activities. USCYBERCOM's 133-team Cyber Mission Force—cyber protection teams, combat mission teams, and national mission teams through CNMF-HQ and JFHQ-C, and cyber operations–integrated planning elements (CO-IPEs) at each combatant command—focuses on full-spectrum cyber operations with a preponderance of effort toward off-DODIN offensive and defensive activities for the "defending the nation" mission area and support to combatant commands, respectively.[40] Other cyber defenders across DOD include incident response teams, red (simulated aggressor) teams, sensor teams, cybersecurity service providers, organic service providers, network operations centers, computer emergency response teams, and blue (simulated defender) teams. JFHQ-DODIN has six cyber-protection teams that deploy to address prioritized vulnerabilities and special defense-related initiatives.

Warfighter Integrated Cyberspace Operations. As of late 2019, CO-IPEs were still in the development phase but were under way serving as the forward extensions of JFHQ-DODIN and a JFHQ-C. Their purpose is to help combatant commanders to plan, synchronize, integrate, and deconflict offensive operations, defensive cyber operations, response actions, and defensive cyberspace operations. Their activities include situational monitoring of DODIN dependencies, joint planning, intelligence, DODIN operations and defensive internal measures, coordination with the JFHQ-DODIN Operations Center, and engagement with crisis action planning and response.[41]

Full-Spectrum Thinking for Assertive Action. As the capabilities for offensive cyber and defensive cyber have matured over the last ten years, USCYBERCOM presses for seamless collaboration between the two communities. This includes enhancing relationships with federal law-enforcement, intelligence, and homeland-security agencies where efforts to leverage and share information have been considered successful. Efforts to protect the American 2018 and 2020 elections are examples of organizations—to include

state-level entities—sharing information and coordinating defensive cyber efforts from their own levels of authorities and within the limits of legal reach.[42]

The Future: Factors to Launch New Advancements in Defense

Policy Reform. Deeper levels of cooperation are required for success in defensive cyberspace operations. This requires policy and procedure changes to meet long-term strategic defensive goals involving the whole of government, coalition/international partners, industry, and academia. Three policy areas need attention in the future. First, DOD and policy makers must reconcile the conflicts between the Goldwater-Nichols Act and the Clinger-Cohen Act regarding cyberspace operations. Second, the DOD policy and acquisition communities and the operations community must enhance and expand collaboration to achieve the effective operational outcomes commanders and directors need in carrying out their mission areas while pursuing efficiency goals of the CIO and resource management communities. Third, DOD must enhance policies and processes to allow for increased information and intelligence sharing with other federal partners, allies, academia, and industry.

Codifying the Operational Command Framework. Organizing and optimizing the battlespace are imperative for substantive and effective operational outcomes in the future. Refining authority and aligning forces to provide, secure, and defend cyberspace as DOD organizations evolve—such as with the standing up of U.S. Space Command in 2019—will reinforce unified action and USCYBERCOM's command-centric, threat-informed approach to defensive priorities and decisions. Optimizing for effectiveness will involve continually reassessing the DODIN architecture and examining the span of control at points within the layered construct. These efforts underpin the focus on managing operational risks across all four DOD core functions: combatant command warfighting; the services' "organize/man/train/equip" responsibilities; intelligence activities; and business operations.

Contested Environment and Technology. The DODIN will continue to be a contested environment in an extraordinarily complex and complicated battlespace. This situation requires continuously defining cyber threats and examining the overwhelming amount of daily operational information and intelligence available. JFHQ-DODIN, together with the components, must continue the active defense of the DODIN to prevent adversaries from gaining hold and shaping the space, thus setting the norms on which all would operate.

Future advancements in defensive cyber will require "baked in" security, increased speed to allow operators to be more proactive in defense activities, and a visual depiction of friendly and adversarial cyberspace activity to integrate with the other

warfighting domains of land, air, sea, and space. DOD must further develop capabilities to be predictive in securing, operating, and defending the DODIN. Critical aspects include tighter security for unclassified and classified systems, integrated fusion of operations and intelligence, and analysis to sort irrelevant from relevant data rapidly and allow for specialized analysis.

Priorities and Advocacy. The JFHQ-DODIN Cyber Tasking Cycle is an effective way to strengthen and hasten the prioritization process for DODIN operations and cyber defense. For the future, this process will involve commanders, directors, and policy makers managing risk rather than avoiding risk. This requires experimentation, innovation, and willingness to learn and develop new operational concepts with a proactive approach. USCYBERCOM, as the voice for the cyberspace operational warfighting domain, will need to press for enterprise efforts and tailored capabilities to ensure effectiveness of operations.

Conclusion

Advances in the cyberspace warfighting domain defensive operations align with the overarching purposes outlined in the *National Defense Strategy* and *DOD Cyber Strategy*. The priority is to protect national interests and preserve vital partnerships that enable the American military's long-term competitive advantage. The key has been to stay ahead of adversaries in the incredibly dynamic cyberspace environment. Unity of command and control, together with a warfighter ethos, has strengthened efforts and increased the pace of proactive defensive actions on and off DOD networks in USCYBERCOM's persistent-engagement strategy.

This persistent-engagement strategy leverages operational information and intelligence from diverse areas to reinforce assertive defensive action as close to the source of malicious activity as practicable. For JFHQ-DODIN, its defensive cyberspace operations mission arises from a global responsibility to protect the entirety of the DODIN, a critical aspect of the persistent-engagement approach. Having reached full operational capability in 2018, JFHQ-DODIN continues to mature to address the full scope of its mission, covering all classified and unclassified networks, cloud endeavors, information-technology equipment, tools and applications, weapon system technologies, and data.

Challenges for defensive cyberspace operations continue to exist, but at the same time these challenges open doors to new opportunities for innovative solutions. Quantum computing threatens the veracity of encryption and increases the velocity and volume potentially available to an adversary. In addition, such new technologies as the Internet of Things, Internet Protocol version 6, and 5G telecommunications increase the scope

and complexity for defense and full-spectrum cyberspace operations overall. While they bring their own challenges, these and other emergent technologies allow for the creation and deployment of enterprise-wide approaches to support operational effectiveness for DOD component commanders and directors, to achieve management efficiencies, and overall, to give DOD competitive advantage against adversaries across multiple domains.

Future advancements in defensive cyberspace operations will depend on policy and modernization reforms, identification of cyber-related priorities and requirements, and operationalization of technologies and capabilities. JFHQ-DODIN is involved in or leading efforts in each of these areas to help bridge the capabilities requirements for operational effectiveness with the institutional administrative-efficiency efforts. This role is important to defensive cyberspace operations, given the organization's command-and-control responsibility, which includes examining the interoperability of various tools for enterprise-wide opportunities, as well as technology and process capabilities that represent a comprehensive suite of current or possible future solutions.

Notes

Epigraphs: DOD, *Summary DOD Cyber Strategy 2018,* p. 1; "Former NSA Deputy Director Talks Snowden, Pardons and Privacy," *SC Media,* 26 October 2016, video, https://www.scmagazine.com/.

1. Damian Paletta, "NSA Chief Says Cyberattack at Pentagon Was Sophisticated, Persistent," *Wall Street Journal,* 8 September 2015; Craig Whitlock and Missy Ryan, "U.S. Suspects Russia in Hack of Pentagon Computer Network," *Washington Post,* 6 August 2015.
2. Paletta, "NSA Chief Says Cyberattack at Pentagon Was Sophisticated, Persistent."
3. Ibid.; Whitlock and Ryan, "U.S. Suspects Russia in Hack of Pentagon Computer Network."
4. U.S. Senate, *Statement of Admiral Michael S. Rogers, Commander, United States Cyber Command, before the Senate Committee on Armed Services,* 115th Cong., Washington, DC, 2018, pp. 5–8, https://www.armed-services.senate.gov/; Jared Serbu, "WannaCry, Petya Ransomware Attacks Were 'Non-events' for DoD Systems," *Federal News Network,* 24 July 2017.
5. Brian J. Donahue [Brig. Gen., USA (Ret.)], President, By Light Professional IT Services LLC, in discussion with author, 21 December 2018.
6. For more on cyber conflict and competition, see chapters 1 and 9. Also see Paul M. Nakasone, "Countering Threats Old and New" (remarks, Aspen Security Forum, Aspen Institute, Aspen, CO, 21 July 2018), streamed live on 21 July 2018 and available as The Aspen Institute, "Countering Threats Old and New," Youtube, 21 July 2018, video, 57:54, https://www.youtube.com/; and U.S. Cyber Command [hereafter USCYBERCOM], *Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. Cyber Command* (Fort Meade, MD, March 2018), pp. 2–5, https://www.cybercom.mil/.
7. U.S. Department of Defense [hereafter DOD], *Summary [of the] Department of Defense Cyber Strategy 2018* (Washington, DC, 2018), pp. 4–5; USCYBERCOM, *Achieve and Maintain Cyberspace Superiority,* pp. 2–5.
8. DOD, *Summary DOD Cyber Strategy 2018,* p. 1.
9. Donahue, discussion with author.

10. *Quadrennial Defense Review Report* (Washington, DC: U.S. Defense Dept., February 2010), pp. 37–39.
11. U.S. Joint Chiefs of Staff [hereafter JCS], *Cyberspace Operations,* Joint Publication 3-12 (Washington, DC, 8 June 2018), p. viii; JCS, *Joint Communications System,* Joint Publication 6-0 (Washington, DC, 10 June 2015), p. I-1; DOD, *Cybersecurity Activities Support to DoD Information Network Operations,* DOD Instruction 8530.01 (Washington, DC, 25 July 2017, incorporating change 1), p. 2.
12. DOD, *Department of Defense Information Network (DODIN) Transport,* DOD Instruction 8010.01 (Washington, DC, 10 September 2018), pp. 3–4.
13. Joint Force Headquarters–Department of Defense Information Network [hereafter JFHQ-DODIN], "Protecting DOD Networks for Mission Success," fact sheet, October 2018; JFHQ-DODIN, "Fight the DODIN: Cyberspace Superiority through Unified Action & Assertive Defense," fact sheet, October 2018; JFHQ-DODIN, "24/7 Joint Global Cyberspace Operations," fact sheet, October 2018; "U.S. Cyber Command History," *U.S. Cyber Command,* https://www.cybercom.mil/.
14. Memorandum on Elevation of the United States Cyber Command to a Unified Combatant Command, 2017 Daily Comp. Pres. Doc. (18 August 2017); JCS, *Modification (MOD) to Execute Order to Implement Cyberspace Operations Command and Control (C2) Framework* (Washington, DC, 14 November 2014); JCS, *Cyberspace Operations.*
15. JCS, *MOD to Execute Order;* JCS, *Cyberspace Operations.*
16. JCS, *Cyberspace Operations;* USCYBERCOM, *Achieve and Maintain Cyberspace Superiority.*
17. "Combined Action Group," in U.S. Cyber Command Public Affairs Office, *Cyber Cyphers* (December 2018); Paul M. Nakasone, "AUSA 2018 CMF #2: Future Disruptive Threats," ILW Contemporary Military Forum, Association of the United States Army, Washington, DC, 8 October 2018, *Defense Visual Information Distribution Service,* video, 1:54:25, https://www.dvidshub.net/; Nakasone, "Countering Threats Old and New."
18. "Combined Action Group."
19. *Quadrennial Defense Review Report,* pp. 37–39.
20. William J. Lynn III, "Defending a New Domain," *U.S. Department of Defense,* 10 April 2010, archive.defense.gov/; DOD, *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC, July 2011), pp. 1–4; DOD, *Summary DOD Cyber Strategy 2018,* p. 2; USCYBERCOM, *Achieve and Maintain Cyberspace Superiority.*
21. Lynn, "Defending a New Domain"; DOD, *Strategy for Operating in Cyberspace,* pp. 1–4; DOD, *Summary DOD Cyber Strategy 2018,* p. 2; USCYBERCOM, *Achieve and Maintain Cyberspace Superiority.*
22. Lynn, "Defending a New Domain"; Donahue, discussion with author; DOD, *Strategy for Operating in Cyberspace,* pp. 1–4.
23. JCS, *The National Military Strategy of the United States of America: A Strategy for Today—A Vision for Tomorrow 2004* (Washington, DC, 2004); Gerry Gilmore, "Official Cites Value of Cyberspace to Warfighting Operations," *U.S. Strategic Command,* 8 April 2009, www.stratcom.mil/; Jordan Reimer, "U.S. Cyber Command Preparations under Way, General Says," *U.S. Strategic Command,* 17 March 2010, www.stratcom.mil/; Lynn, "Defending a New Domain"; *Cyberspace as a Warfighting Domain: Policy, Management and Technical Challenges to Mission Assurance:* Hearing before the Terrorism, Unconventional Threats and Capabilities Subcommittee of the Committee on Armed Services House of Representatives, 111th Cong., Washington, DC, 2009; *U.S. Cyber Command: Organizing for Cyberspace Operations: Committee on Armed Services House of Representatives,* 111th Cong., Washington, DC, 2010.
24. JCS, *MOD to Execute Order.*
25. Goldwater-Nichols Department of Defense Reorganization Act of 1986, Pub. L. No. 99-433, 100 Stat. 992; Clinger-Cohen Act of 1996, comprising Federal Acquisition Reform Act of 1996 (National Defense Authorization Act for Fiscal Year 1996, Pub. L. No. 104-106, div. D, 110 Stat. 186, 642) and Information Technology Management Reform Act of 1996 (National Defense Authorization Act for Fiscal Year 1996, Pub. L. No. 104-106, div. E, 110 Stat. 186, 679); Donahue, discussion with author.
26. JCS, *MOD to Execute Order.*
27. JFHQ-DODIN, "Operation Gladiator Shield 2017: Organizing for Sustained Conflict," base

order, Fort Meade, MD, 3 August 2017, pp. 2–4 (Unclassified/FOUO).

28. 2016 Public-Private Analytic Exchange Program Team, *Cyber Attribution Using Unclassified Data* (Washington, DC: Office of the Director of National Intelligence, 2016).
29. Casimir C. Carey III [Col., USA], "JFHQ-DODIN Brief: Predictive Intelligence" (AFCEA Defensive Cyber Operational Symposium, Baltimore, MD, 17 May 2018), downloaded from https://www.youtube.com/; Col. Paul Craft, "Artificial Intelligence Use in Command and Control," AFCEA Defensive Cyber Operational Symposium, May 2018, downloaded from https://www.afcea.org/.
30. Software Engineering Institute, "Insider Threat," *Carnegie Mellon University,* December 2017, https://www.sei.cmu.edu/. Also see Danny Palmer, "Former NSA Exec: We Misjudged Potential of Insider Threats like Snowden," *ZDNet,* 27 October 2016, downloaded from https://www.zdnet.com/.
31. Michael D. Maloney, "Pentagon's DC3I Memo Acknowledges Thousands of Cyber Breaches That Compromised DOD Systems and Commits to New Cyber Culture," *National Law Review,* 27 October 2015, https://www.natlawreview.com/.
32. Ibid.; DOD, "Department of Defense Cybersecurity Culture and Compliance Initiative (DC3I)," official memorandum, Washington, DC, 30 September 2015.
33. JCS, *Joint Concept for Integrated Campaigning* (Washington, DC, 16 March 2018).
34. *JFHQ-DODIN Subordinate Campaign Plan for Defensive Cyberspace Operations and Internal Defensive Measures* (Fort Meade, MD: JFHQ-DODIN, 11 December 2017). Classified: Information extracted is unclassified.
35. Paul G. Craft [Col., USA], "Fight the DODIN: Treating the Network as a Weapons Platform" (presentation, TechNet Cyber 2019, Baltimore, MD, 15 May 2019), PowerPoint slides available at https://cloud.afcea.org/owncloud/s/DLU97yGMezbi957?path=%2FDefending%20in%20Cyber%20Theater#pdfviewer.
36. JFHQ-DODIN, "Protecting DOD Networks for Mission Success," and "24/7 Joint Global Cyberspace Operations."
37. JFHQ-DODIN, "Protecting DOD Networks for Mission Success," "Fight the DODIN," and "24/7 Joint Global Cyberspace Operations."
38. John K. Porter III, "A New Perspective Aids Cyber Inspections amid Mission Risk," *Signal,* 8 April 2019, https://www.afcea.org/.
39. JFHQ-DODIN, "Fight the DODIN."
40. "U.S. Cyber Command History."
41. *Draft JFHQ-DODIN Concept of Operations;* Mark Pomerleau, "Cyber Command Stands Up Planning Cells at Combatant Commands," *C4ISRNET,* 11 October 2017, https://www.c4isrnet.com/; "Why DOD Is Starting a New Cyber Cell on the Korean Peninsula," *Fifth Domain,* 20 April 2018, https://www.fifthdomain.com/.
42. Paul M. Nakasone's remarks in White House, "Press Briefing by Press Secretary Sarah Sanders and National Security Officials," transcript, 2 August 2018, https://www.whitehouse.gov/; DOD, "Press Gaggle at the Pentagon by Secretary of Defense James N. Mattis," transcript, 7 August 2018, https://www.defense.gov/.

CHAPTER FIVE

Cyberspace and Warfighting

JOSHUA ROVNER

Offensive cyberspace operations hold out the promise of quick decisive victories by acting as powerful force multipliers for conventional forces. Significant technical and institutional obstacles, however, stand in the way of this vision. Evolving cyberspace capabilities also raise a series of fundamental strategic questions for political and military leaders. This paper describes the promise of cyberspace operations in wars against cyber-savvy states, the practical barriers to success, and the strategic questions that will remain unresolved even as cyberspace technology and doctrine mature.

Cyberspace operations are seductive and bewildering. They appeal to policy makers as low-cost and low-risk alternatives to conventional warfighting. They suggest a method of undermining an enemy's ability to fight by turning off its communications and blinding it by attacking the information-technology systems it needs for battlefield intelligence. Adversaries of the United States have spent decades trying to close the military gap, reorganizing their forces and fielding new weapon systems that challenge American dominance. Well-executed cyberspace operations at the outset of a conflict might render all these adversarial efforts irrelevant, restoring U.S. advantages. It is not surprising that policy makers are intrigued by the opportunity to use these tools in the event of conflict. They hold out the prospect of extending the lead of the United States in peacetime and of bloodless victory in war.

At the same time, cyberspace operations rely on technologies that nonspecialist policy makers find exotic and incomprehensible. This might lead them to overestimate the operational effects of cyberspace operations. Alternatively, it might inspire an overabundance of caution if they worry about using an alien technology to achieve policy ends. Policy makers can see and touch traditional tools of warfare. They understand what rifles and missiles accomplish and intuit how adversaries respond to threats of kinetic violence. But they might not have an intuitive understanding of what a "cyber threat" means, how it is delivered, or what it seeks to achieve. The nature of the cyberspace

domain may seem all-encompassing and totally intangible. It is easy to understand why policy makers might not be confident about making strategy in a radically different space.

We are thus left with opposing problems. One is false optimism about cyberspace operations. The other is a kind of stifling pessimism about the ability of senior leadership to think like strategists, given the complexity and weirdness of cyberspace technology. This chapter addresses both issues. It acknowledges the enthusiasm for wartime operations but describes the inherent limits of offensive cyberspace activities against military targets. It then provides a framework for policy makers who are forced to grapple with the strategic consequences in the event of a great-power war. We have a great deal of experience with cyberspace operations in violent conflict with nonstate actors, and we compete below the line of armed conflict against states continuously. We have not experienced cyberspace operations in a high-intensity interstate war, however, so we lack an empirical base for thinking about what could be the most consequential of all cyber conflicts. Some theory is needed.

I proceed as follows. The first section describes how doctrine in the United States and elsewhere reflects the emerging consensus that cyberspace is integral to conventional warfighting. The second section offers a more general discussion of how cyberspace operations might support, complement, or substitute for kinetic force. The third section describes the technical and institutional challenges of integrating cyberspace operations into warfighting operations and doctrine. The final section asks what strategic questions still remain even if militaries overcome these challenges.

Doctrine for Cyberspace Operations

U.S. doctrine assumes that cyberspace operations will feature prominently in future conventional war. Modern militaries rely on cyberspace for sharing data over distances. Those forces also rely on information technologies for their normal operations; their battle rhythm depends on dependable network communications. Offensive cyberspace operations are potentially appealing for the same reason, because an adversary's dependence on cyberspace makes it vulnerable to crippling attack.[1] It is no surprise, then, that U.S. Cyber Command emphasizes "fully integrating cyberspace operations into combatant commander plans as well as existing boards, bureaus, cells, and workgroups used to plan and execute warfare."[2]

U.S. military publications echo this call, at least on paper. They direct planners to integrate cyberspace operations in routine campaign planning and to add them to flexible-response options in the event of a crisis. Planners should also consider both offensive and defensive operations. While U.S. Cyber Command is responsible for

synchronizing efforts, regional combatant commands "must identify their requirements for cyberspace operations both as supported and supporting commands in support of this campaign planning effort."[3] The assumption throughout is that the cyberspace and physical domains are inextricably linked. It makes no sense to segregate planning for cyberspace operations from land or naval operations if the latter cannot operate without the former. Further, cyberspace operations work through physical assets—cables, power stations, server farms, and so on. Popular references to the "cloud" obscure the fact that digital information ultimately transits and resides in physical infrastructure. Effective cyberspace operations require more than clever code; they require securing the attack vector. Joint publications note that cyberspace operations can extend operational reach, but without careful planning in advance, cyber and kinetic attacks may work at cross-purposes.[4]

American commanders have enjoyed conventional military dominance for decades, but advances in cyberspace capabilities may put that to the test. Standing doctrine reminds U.S. forces, long accustomed to communicating without fear of jamming or interception, that adversaries "are likely to use technological advances in cyberspace and vulnerabilities in the [electromagnetic spectrum] to conduct cyberspace or EMS attacks."[5] This warning applies to headquarters elements but especially to lower echelons. Losing operational capability in cyberspace reduces freedom of action and makes it difficult to sustain complex campaigns requiring tight integration. Such a scenario would put a premium on the ability of decentralized units to operate independently and effectively. The fact that doctrinal statements are making this point suggests serious concern about overdependence on cyberspace.[6]

The Department of Defense and Joint Staff anticipate that cyberspace operations will play roles in all stages of a future conflict.[7] This includes efforts to gain access to areas where forces are likely to operate, maintaining command and control in the early days, preventing enemies from taking actions likely to bring dangerous escalation, and synchronizing cross-domain efforts in high-intensity combat.[8] But the complexity of operations at each stage and the need for tight integration create openings for motivated and technologically sophisticated opponents. Also, continuous operations against irregular adversaries have taxed readiness for conventional war against great powers with sophisticated cyberspace capabilities. The *National Defense Strategy* released in 2018 puts the matter bluntly: "This increasingly complex security environment is defined by rapid technological change, challenges from adversaries in every operating domain, and the impact on current readiness from the longest continuous stretch of armed conflict in our Nation's history. . . . America's military has no preordained right to victory on the battlefield."[9]

The desire to use cyberspace to enhance conventional battlefield effectiveness, along with the fear that adversaries could use cyberspace to erode U.S. dominance in areas where the United States has enjoyed it, has led to organizational changes. Integration is the watchword. All the regional combatant commands (CCMDs) have been directed to establish cyberspace operations–integrated planning elements (CO-IPEs). While U.S. Cyber Command has authority over cyberspace operations, "all actions with the affected CCMDs are coordinated through their CO-IPEs to facilitate unity of effort and mission accomplishment. . . . The CCMD coordinates and integrates cyberspace capabilities in the [area of responsibility] and has primary responsibility for joint [cyber operations] planning, to include determining cyberspace requirements within the joint force."[10] Cyberspace planners must consider kinetic operations, and vice versa.

The United States is not alone in assuming that cyberspace operations will play increasingly important roles in conventional campaigns. Chinese doctrine, discussed in more detail below, emphasizes the importance of controlling information in the early stages of any conflict. Russia has also moved toward integrating offensive cyberspace operations (OCO) into conventional offensives, albeit with mixed results. For Russian strategists, cyberspace operations disorient and demoralize adversaries before conflict begins and help to neutralize enemy command-and-control systems afterward.[11] U.S. allies are also developing their own ideas about how to combine OCO with traditional warfighting, viewing cyberspace as both a threat and an opportunity. British army doctrine, for instance, notes that threats are increasing "as we and other actors become more and more reliant on sophisticated information services."[12] At the same time, efforts to merge cyberspace and kinetic operations create new opportunities to debilitate adversary systems, achieve tactical surprise, and control the scope and pace of conflict.

The Promise of Cyberspace Operations in Conventional Warfighting

In the abstract, cyberspace operations ought to improve the quality of warfighting across the spectrum of conflict. Defensive efforts preserve reliable communications against enemy attacks, ensuring that warfighters maintain a good understanding of the battlefield and making it possible to share data across many units operating simultaneously. Defending communications has always been fundamental to battlefield effectiveness, and the same applies in cyberspace.[13]

Offensive cyberspace operations hold out promise as force multipliers in conventional conflict. OCO might channel enemy personnel away from civilians; drawing them out in the open would reduce the harm to innocents while leaving enemies vulnerable to kinetic attack. Particularly sophisticated levels of tactical integration might allow commanders to communicate with certain enemy individuals via cyberspace, subsequently affecting enemy organization and performance. A sequence of integrated OCO and

conventional missions might make it possible to achieve campaign goals sooner than would be possible otherwise. For example, we can imagine OCO against enemy air defenses enabling air strikes that would in turn provide cover for land forces. Alternatively, planners could integrate OCO in broader campaigns to erode the enemy's overall capability. Such operations would not support kinetic missions directly, but they could open possibilities for conventional forces. OCO would also impose cumulative costs that make it increasingly hard for enemy forces to organize a coherent defense. The more adversaries must scramble to keep networks running, the less effectively they can fight.[14]

Indirect attacks against enemy networks may serve battlefield ends, even if the attacks cause no damage. A hypothetical cyberspace operation might target unclassified communications or cross-domain solutions (i.e., the ability to move data across different security domains). Such an operation could inject confusion or delay into a campaign requiring synchronization of thousands of personnel working in many locations. Disrupting the timing of air tasking orders, for instance, might subsequently upset the quality of combined operations.

Some cyber attacks might have more-immediate effects. At a minimum, OCO may impact communications by forcing the enemy onto backup networks or into time-consuming work-arounds. In these cases, the enemy might reasonably suspect that its communications were being targeted to facilitate intelligence collection. It can protect itself by reducing the amount and quality of its communications, but it does so at the cost of reducing tactical efficiency. In other cases, OCO might have a direct impact by rendering target systems inoperable.

Cyberspace operations may serve as vehicles for psychological operations against enemy leaders and military personnel. Such operations potentially affect morale and trust, reducing battlefield effectiveness and the will to persist. Broader propaganda efforts in cyberspace may serve to undermine public support for the war and encourage settlement talks. Alternatively, cyberspace operations might aim at the enemy's defense industrial base in ways that reduce productivity or at the transportation infrastructure that enables coordination between firms and government. As with the discussion above, OCO may target information systems or the psychology of those who use them.

The point in all of these cases is to weaponize friction. Friction describes the normal bureaucratic hiccups that affect all organizations. Flat tires, sluggish e-mail, colleagues out sick—all of these routine occurrences slow down organizational productivity. If friction is normal in peacetime, however, it is much more problematic in war, which is after all a contest among large armed bureaucracies.[15] To the extent that modern war includes competitive cyber operations among sophisticated adversaries, it is in a sense a contest about who is better able to cope with friction. Defensive cyberspace operations mitigate

enemy efforts; offensive cyberspace operations inject bureaucratic confusion, doubt, and frustration.

Such efforts run the risk of provoking escalation if enemies fear the collapse of their regimes or simply lash out in frustration. Carefully targeted OCO may help to control the risk of escalation by signaling to specific political and military leaders that they will be held personally responsible for their actions. Tailored e-mail or text messages might also include promises that they stand to benefit from restraint.[16] In the ideal, then, OCO would help manage strategic interaction and frustrate enemy actions while controlling the scope of violence.

Finally, cyberspace operations can play a role in isolating wartime enemies. This may involve efforts to counter enemy propaganda and expose fabrications or target the individuals responsible for generating content. Particularly ambitious efforts might target not the enemy but its allies, using cyberspace operations to deter them from providing material support. Strategies of coercive isolation have been the subject of recent attention from scholars of international relations but to my knowledge have not been explored in the context of cyberspace.[17]

Technical and Institutional Roadblocks

It would be surprising if military leaders did not try to utilize OCO in future conventional campaigns, given the opportunities described above. Cyberspace operations promise nearly immediate impacts on enemy battlefield effectiveness, in addition to cumulative costs that erode enemy strength and morale. These operations can be conducted at little or no risk to the individual attacker.[18]

But several technical and institutional factors are likely to limit the effectiveness of cyberspace operations. Terrestrial command-and-control networks, for example, are extremely hard targets, requiring extensive and detailed intelligence to gain access and develop tools that can exploit specific vulnerabilities and do real harm. This task is harder in wartime, because combatants will be on guard against intrusions. They are also likely to employ redundant communications in the event of an attack, meaning that even successful OCO may have limited impact.

Operations against closely guarded facilities require elaborate preparations. In these cases, the widely held belief that the offense has the advantage in cyberspace is usually false.[19] Gaining access to hard targets and delivering payloads with significant effect is extremely difficult without time, expertise, and substantial organizational resources. A good deal of luck is required. Target characteristics must stay the same long enough for cyberspace developers to work on "exploits." Success also depends on key personnel staying in place. Among other problems, personnel changes mean new passwords

and security procedures that make it difficult to retain access into adversary networks. Success ultimately depends on cooperative adversaries, whose poor operational security leaves them at risk of attack. It is much easier to go on the offensive against adversaries who practice poor cyber hygiene, who are sloppy about vetting personnel, who do not encrypt communications, and who fail to update software routinely. Even in these cases, success is fleeting, because access is fragile. Minor network changes can spell doom for once-promising cyberspace operations; even mediocre defenders of hard targets can make life difficult for attackers seeking to degrade them.[20]

Access to adversary networks is a prerequisite to any cyberspace operation. Access is hard to gain and easy to lose. Capable defenders practice routine updates, educate their workforce about the importance of cybersecurity, and test their systems against real and imagined intruders. Mediocre defenders are easier to target, but even they can do things to frustrate OCO. These include at least occasional software updates and changes to configuration settings; such changes may not be intended to ward off attacks, but the outcome is the same from the perspective of the attacker. Firewall modifications, computer resets, and equipment transfers have similar effects. There are many other ways to lose access, some of which are beyond anyone's control. A flood at a target state's server facility, for instance, may require a temporary shutdown and replacement of hardware.[21]

Developing intelligence and capabilities for offensive cyberspace operations takes time. That luxury may not be available in a crisis. In theory, the attacker could use tools developed in peacetime, but defenders will take prophylactic measures as the chance of conflict increases. Changing security protocols will make it difficult for attackers to get through. In addition, defenders will work hard to ensure that communications systems are resilient if they suspect they will soon be under attack. They will be on the lookout for signs of malware and motivated to remove it. Commanders who expect on-call OCO in support of kinetic strikes are likely to be disappointed. There is no such thing as OCO on demand.

Wartime OCO probably means attacking redundant systems. Militaries have obvious reasons to prepare to operate under degraded conditions and to prepare to recover quickly by patching or reconfiguring compromised systems. As a result, even successful wartime OCO may have only temporary and limited effects.[22]

Cyberspace operations require that adversaries cooperate in a different sense, because any connection to the internet is voluntary. Adversaries fearful of being targeted can choose to disconnect or otherwise reduce their exposure. Military organizations that are "cyber dependent" are most at risk. Instead of investing more in complex information systems, they may choose to become merely "cyber enabled," sacrificing a bit of efficiency in the name of security. In extreme cases they may choose to become "cyber

independent" and revert to traditional communications requiring no connectivity whatsoever.[23]

The fact that adversaries can deliberately sequester themselves suggests the limits of OCO for warfighting. This is especially the case in wars of attrition, where the goal is to impose cumulative costs rather than choreograph sophisticated sequential battles in pursuit of a culminating victory. In these cases, combatants have less need for tightly linked operations requiring precise maneuver and timing. They just need to survive, maintaining the ability to skirmish and harass their opponents. From their perspective "dumbing down" the fight makes a great deal of sense. In other cases, however, the attacker may see value in forcing the enemy to abandon efficiency. The attacker may believe that the enemy will be more willing to settle if denied the ability to execute its preferred concept of operations. Forcing the enemy to disconnect creates an incentive for it to surrender rather than having to fight a costly conflict on one's own terms. Much depends on the quality of prewar intelligence and strategic assumptions about the enemy's reliance on cyberspace, ability to adapt, and will to persist.

Cyberspace operations pose a special risk for intelligence collection, because stealing digital information is difficult or impossible after attacking the source. The intelligence gain/loss trade-off, familiar in peacetime, is also present in a conventional war. Degrading an enemy's communications and information systems means less ability to collect from them. This may be worthwhile if commanders expect the outcome to be decided quickly. In a brief, high-intensity fight they will put a premium on anything that disrupts the enemy's ability to receive accurate intelligence and coordinate forces effectively at the critical place and time. But these operations are hard to hide, especially against hard targets such as military command networks. As Erik Gartzke and Jon Lindsay point out, "More complicated attacks are at greater risk of leaving behind clues for forensic investigations in technical artifacts or other behavior exposed to intelligence collection."[24]

If the fact that cyberspace operations may be easy to spot is unimportant in a war expected to end soon, sustaining intelligence sources becomes more important in a protracted conflict, where the outcome rests not on achieving clear battlefield victories but on imposing sufficient pressure over time to force the enemy to recalculate the value of continuing the fight. Intelligence collection via cyberspace can shed light on how military and political leaders view the evolving conflict, whether civil-military tension is manageable or rising, whether morale is stable or weakening, and so on. Meanwhile it can help determine where to strike next and provide tactical warning of enemy attacks.

Carefully designed cyberspace weapons may not produce the intended effects if the defender has made software or configuration changes in the interim. Effective offensive cyberspace operations can soon become ineffective. Because sophisticated weapons

require specific accesses with payloads designed to exploit specific vulnerabilities, they often have short shelf lives.[25] Deterrent threats may be hollow if it is hard to hold targets at risk. The same is true for warfighting. Carefully designed plans integrating cyberspace and kinetic operations may flounder if defenders have taken steps, wittingly or not, to protect their networks. These changes may be completely hidden from the attackers.

On the other hand, operations may unintentionally propagate to third-party systems and devices. The risk of contagion has raised concerns that OCO may cause widespread and uncontrollable collateral damage to civilians and firms. The 2017 NotPetya incident, in which an attack on a Ukrainian tax-preparation service eventually rippled throughout the global shipping industry, is a case in point.[26] Contagion is unlikely if payloads are customized for specific targets. Other methods, like target-identification checks, also help reduce the risk. But states may not take these cautionary steps if they seek immediate effects with the greatest chance of success.

The result is a wide range of possible outcomes, from disappointing fizzles to cyber operations that do much more than anyone expected. Good strategy requires calibrating operational effects with political objectives. Whether commanders can actually achieve this level of calibration, given the range of possible operational effects, is an open question.[27]

As with all warfighting options, OCO require intelligence, planning, and execution. These three functions sometimes work at cross-purposes. In some cases, intelligence personnel clash with operators. The intelligence gain/loss dilemma, as noted, illustrates the trade-off between collecting information and exploiting it. Operators may want to act quickly against adversaries, especially if they view targets as fleeting, but intelligence officers may not want to relinquish their hard-won accesses. This problem is not unique to cyberspace, of course. Leaders have always struggled with whether to act on intelligence at the risk of losing a valuable source of information. But the dilemma is particularly intense with regard to OCO, because there may be a very short time to act on intelligence before a given cyberspace option becomes obsolete. Brief windows of opportunity impel action.[28]

Intelligence personnel may also clash with military planners. The latter may expect intelligence on what they view as targets critical to the success of war plans, such as enemy communications networks. Intelligence personnel will probably struggle to meet these expectations, however, because these are the same targets most likely to be well defended. Even gaining access to hard targets is not enough, because wealthy adversaries have obvious incentives to build separate and redundant networks.

Finally, efforts to collect on hard targets might take intelligence personnel away from supporting other ongoing operations against lower-profile targets. In this case, planners and operators may find themselves in competition for scarce intelligence resources. This competition may produce internal frustration, even finger-pointing, as starry-eyed prewar hopes for cyberspace attacks are outstripped by operational realities.

Strategic Trade-Offs

Overcoming these technical and institutional problems would be a terrific accomplishment, especially in a conflict against a technologically sophisticated adversary. Conquering the operational difficulties inherent in cyberspace and aligning OCO with conventional campaigns are enough to tax the most talented planner. But even operational brilliance does not guarantee strategic success; even wartime leaders who are able to solve the problems described above will still confront a series of strategic trade-offs.

Escalation versus Protraction

The allure of cyberspace is the hope that it can facilitate quick and bloodless victories. Injecting fog into enemy information systems will make it difficult for enemies to keep track of events and prepare defenses. Injecting friction into enemy organizations will make it difficult for them to organize effective responses. High-intensity warfare demands access to information and reliable communications across deployed forces. States that cannot maintain control of information cannot keep up the fight. The problem, however, is that confused and cornered adversaries might use sudden and extreme violence to break out of their predicament. Those with nuclear weapons may choose to take the ultimate risk rather than concede defeat.

Scholars have been particularly concerned about nuclear escalation in a U.S.-China war. China's growing suite of antiaccess weapons have caused concern among defense analysts, spurring planners to draw up new concepts that will allow U.S. forces to operate in contested areas. Such concepts may include rapid, blinding strikes against Chinese land-based radar facilities and other systems needed to keep U.S. forces at bay. Critics warn that these strikes, delivered in conjunction with OCO against military forces, may cause Chinese Communist Party (CCP) leaders to fear a sudden end of their rule. To prevent that they may take extraordinary risks, including nuclear escalation. They may also consider cyberspace operations against civilian infrastructure, given the difficulties described above in targeting military networks.[29]

The simplest way to avoid escalation in a hypothetical U.S.-China conflict is to fight conservatively. This means eschewing mainland strikes and OCO against critical targets and generally erring on the side of caution rather than taking the risk that the CCP would fear rapid demise. Doing so, however, would increase the likelihood of protracted

war. In this scenario China could retreat to its vast and durable sanctuary on land, and the party leadership could solidify its position.

An alternative but related scenario is one in which the United States and China both try to use new technologies to score a quick, lopsided victory—and both fail. As we have seen, OCO may not live up to expectations against well-resourced adversaries who have invested heavily in network defense. In addition, new forms of coordination—or extra training for degraded communications—may allow deployed forces to continue fighting.[30] If plan A fails for Washington and Beijing, both might find themselves in a stalemate. Presumably they perceive enormous political stakes—or they would not have taken the risk in the first place. So neither side would be enthusiastic about settling the conflict, even though the prospects for decisive victory were low.[31]

Disrupting Communications versus Negotiating with a Unified Adversary

Disrupting enemy communications makes good tactical sense. Units who are unable to communicate will find it difficult to coordinate their efforts. Unreliable command and control undermines battlefield effectiveness, leaving deployed forces vulnerable to defeat in detail. New technologies offer the possibility of using OCO and electronic warfare to induce this kind of operational sclerosis.

Tactical success might interfere with strategy, however, if the goal is to force the enemy to negotiate favorable terms. Ideally, dividing the enemy's hierarchy would make it easier to insulate willing peacemakers while focusing military pressure on diehards. Dividing the enemy, however, risks making it hard to locate a reliable negotiating partner with the authority to speak for the nation and the ability to compel the armed forces to stand down. Multiple and rival power centers may emerge from atomized national institutions. Peace deals with any of them may prove temporary at best and geographically limited to the areas in which specific commanders hold sway.[32]

The U.S.-China strategic competition is instructive here as well. Both the United States and China are investing heavily in cyber capabilities. The United States recently elevated U.S. Cyber Command to the status of a unified combatant command, giving it the authority to synchronize global cyberspace operations and support regional combatant commands.[33] China appears to have done something similar, creating its Strategic Support Force in part to support the various services in space, cyber, and electronic warfare.[34]

More importantly, both have stressed the importance of information superiority. Chinese doctrine focuses on what it takes to win under "informatized conditions." The 2001 edition of *Science of Military Strategy (SMS),* for instance, states that precision strikes at the outset of war could "paralyze the enemy in one stroke."[35] A recent update to the *SMS*

focuses on the "effective suppression and destruction" of enemy information systems alongside an "information protection capability."[36] China seems to believe that it cannot win if it does not "seize and control the battlefield initiative, paralyze and destroy the enemy's operational system of systems, and shock the enemy's will for war."[37] This is not so different from the American approach, which relies on prompt attacks on enemy communications and intelligence to create a sense of shock and buy time for follow-on forces to surge into the theater.[38]

Reducing Costs versus Credible Assurances

Emerging technologies are alluring because they promise rapid victories, either by themselves or as force multipliers. The ability to win at low cost suggests the ability to secure important national interests with minimal risk. Offensive cyber operations, coupled with kinetic blinding strikes, are meant to stun the target in the opening stage of conflict, allowing the attacker to deploy reinforcements safely. The attacker controls the tempo of the war and can set the terms for ending it. The target, on the other hand, will struggle to muster any meaningful response and may face the terrible choice of accepting bad terms or fighting on at a severe disadvantage.

But in this scenario the victor may find it impossible to provide credible assurances that it will not cheat on the terms of the peace settlement and go for a more comprehensive victory later. Why should it settle for a limited victory when it appears to face little risk in seeking more-ambitious goals? It will be particularly hard to assuage the loser under these conditions. Recent scholarship suggests that this is an important reason why great powers have so much trouble coercing smaller rivals in peacetime. This problem also works against war-termination efforts.[39]

Cyberspace may also be an attractive venue for deception operations, given the speed of online communications and the increasing number of "attack surfaces." Military leaders may plant carefully constructed lies in enemy networks to divert the enemy's resources or sow confusion. In other cases they might simply flood the zone with noise. In either case, the tactical benefit of deception can work against efforts to convince an enemy that the deceiver will honor the terms of any peace deal. In this case, as in others, short-term military necessity works against long-term strategy. The enemy has good reasons to disbelieve the deceiver.[40]

Strategic Success versus Grand-Strategic Stability

Strategy is a theory of victory. It describes how military violence helps the state achieve its political goals. Strategy deals with questions about how to use force to compel the enemy to settle. Grand strategy, in contrast, is a theory of security. It describes how various foreign policy instruments help the state achieve durable national security. Grand

strategy deals with questions about the nature of world politics, the underlying sources of national power, and the utility of both military and nonmilitary tools.

Success in war is not the same as success in grand strategy. In some cases, necessary wartime decisions actually undermine long-term grand strategy. Draining the state coffers in pursuit of victory may leave the victor in a precarious state, especially if the war itself stimulates desires for revenge and third-party balancing. In other cases, strategic success may obscure the true sources of national strength. If a sea power scores a surprising victory on land, for example, it might overestimate its competence outside its primary domain and neglect its true comparative advantage.[41]

Finally, strategic decisions might cause other states to doubt that the postwar order is stable. The introduction of new military technology may have unexpected effects on the balance of power or on the postwar international economy. Suppose, for example, that the United States uses OCO energetically in a hypothetical U.S.-China conflict. Suppose further that it introduces new and powerful cyber weapons to overcome Chinese defense. Malware targeting PLA forces may infect civilian computers in China and beyond. This, in turn, may reduce postwar confidence in the regional and international economic order. Firms and consumers may retreat from online commerce and communication, with effects that are hard to predict.

I have previously argued that such fears are overstated, partly on the basis of an analysis of the reaction to the Stuxnet attack on Iran's nuclear complex. Users, firms, and states were mostly untroubled by that attack, despite significant malware contagion.[42] But the Stuxnet virus contained attributes that limited its ability to cause unintended harm: target-identification checks, limits on the numbers of computers it could affect, and automatic shutdown protocols. Tools used in a war with China, where the stakes would be much higher, might not be similarly constrained. So they might do as expected in the war but also do significant third-party damage. Offensive cyber operations and other novel attacks might contribute to strategic success in the war, but they might also undermine grand strategy after the shooting stops.

Notes

The author served as scholar in residence at the National Security Agency and U.S. Cyber Command in 2018 and 2019. The views here are his alone.

1. Jacquelyn G. Schneider, *Digitally-Enabled Warfare: The Capability-Vulnerability Paradox* (Washington, DC: Center for a New American Security, 29 August 2016), https://www.cnas.org/.
2. "USCYBERCOM 2018 Cyberspace Strategy Symposium Proceedings," *U.S. Cyber Command,* https://www.cybercom.mil/.

3. Joint Chiefs of Staff [hereafter JCS], *Joint Planning,* Joint Publication 5-0 (Washington, DC, 16 June 2017), www.jcs.mil/.
4. Ibid., pp. IV-35, V-23; JCS, *Cyberspace Operations,* Joint Publication 3-12 (Washington, DC, 8 June 2018), p. I-8, www.jcs.mil/.
5. JCS, *Joint Operations,* Joint Publication 3-0 (Washington, DC, 17 January 2017), pp. II-1, II-2, www.jcs.mil/. Section 1053 of the National Defense Authorization Act calls for an "assessment of the capability of joint forces to conduct joint electromagnetic spectrum operations against near-peer adversaries . . . [and] the capability to conduct integrated cyber and electronic warfare on the battlefield." John S. McCain National Defense Authorization Act for Fiscal Year 2019, H.R.5515, 115th Cong. (2018), https://www.congress.gov/.
6. JCS, *Joint Operations,* p. II-8.
7. "Adversary militaries are increasingly reliant on the same type of computer and network technologies that have become central to Joint Force warfighting. The Department will exploit this reliance to gain military advantage. The Joint Force will employ *offensive cyber capabilities* and *innovative concepts* that allow for the use of cyberspace *operations across the full spectrum of conflict*." U.S. Department of Defense [hereafter DOD], *Summary Department of Defense Cyber Strategy 2018* (Washington, DC, 2018), p. 1, https://media.defense.gov/ [emphasis original].
8. JCS, *Joint Operations,* pp. VIII-5, VIII-8, VIII-17, and VIII-20.
9. DOD, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Washington, DC, 2018), p. 1, https://dod.defense.gov/.
10. JCS, *Joint Operations,* p. III-9; JCS, *Cyberspace Operations,* pp. III-6, III-7.
11. Michael Connell and Sarah Vogler, *Russia's Approach to Cyber Warfare,* DOP-2016-U-014231-Final-2 (Arlington, VA: Center for Naval Analyses, September 2016), https://apps.dtic.mil/; Scott Boston and Dara Massicot, *The Russian Way of Warfare: A Primer,* PE-231-A (Santa Monica, CA: RAND, 2017), https://doi.org/10.7249/PE231; Sarah P. White, *Understanding Cyberwarfare: Lessons from the Russia-Georgia War* (West Point, NY: Modern War Institute, 20 March 2018).
12. Land Warfare Development Centre, *Land Operations,* British Army Doctrine Publication AC 71940 (Bristol, U.K.: British Ministry of Defence, last updated 31 March 2017), pp. 1–6, and chap. 7, https://assets.publishing.service.gov.uk/.
13. Max Smeets, "The Strategic Promise of Offensive Cyber Operations," *Strategic Studies Quarterly* 12, no. 3 (Fall 2018), pp. 90–113.
14. On sequential and cumulative operations, see J. C. Wylie, *Military Strategy: A General Theory of Power Control* (New Brunswick, NJ: Rutgers Univ. Press, 1967).
15. Carl von Clausewitz, *On War,* trans. and ed. Michael Howard and Peter Paret (Princeton, NJ: Princeton Univ. Press, 1976), bk. 1, chap. 7.
16. Direct messages can also inspire fear. Russia has reportedly engaged in efforts to frighten Ukrainian soldiers by means of text messages. "Sinister Text Messages Reveal High-Tech Front in Ukraine War," *Voice of America,* 11 May 2017, https://www.voanews.com/.
17. Timothy W. Crawford, "The Strategy of Coercive Isolation," in *Coercion: The Power to Hurt in International Politics,* ed. Kelly M. Greenhill and Peter Krause (Oxford, U.K.: Oxford Univ. Press, 2018).
18. This assumption may not always hold. Precise intelligence may allow military services to locate and target individual operators. The risk calculus for employing OCO might change if operators no longer believe they enjoy the benefits of anonymity.
19. Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22, no. 3 (2013), pp. 365–404; Thomas Rid and Peter McBurney, "Cyber-Weapons," *RUSI Journal* 157, no. 1 (2012), pp. 6–13.
20. This is akin to the fragility of gaining and maintaining access to enciphered adversary communications. Productive intelligence collection sources can dry up quickly.
21. On natural disasters and cyberspace operations, see JCS, *Cyberspace Operations,* pp. I-11, I-12.
22. Jon R. Lindsay and Erik Gartzke, "Coercion through Cyberspace: The Stability-Instability Paradox Revisited," in Greenhill and Krause, *Coercion,* p. 183.
23. Schneider, *Digitally-Enabled Warfare.*

24. Lindsay and Gartzke, "Coercion through Cyberspace."
25. Max Smeets, "A Matter of Time: On the Transitory Nature of Cyberweapons," *Journal of Strategic Studies* 41, nos. 1–2 (2018), pp. 6–32.
26. Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired,* 22 August 2018.
27. On the problem of uncertain effects, see Henry Farrell and Charles L. Glaser, "How Effects, Saliencies, and Norms Should Influence U.S. Cyberwar Doctrine," in *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations,* ed. Herbert Lin and Amy Zegart (Washington, DC: Brookings Institution, 2019).
28. Stephen Van Evera, *Causes of War: Power and the Roots of Conflict* (Ithaca, NY: Cornell Univ. Press, 1999), chap. 4.
29. Examples include Thomas J. Christensen, "The Meaning of the Nuclear Evolution: China's Strategic Modernization and US-China Security Relations," *Journal of Strategic Studies* 35, no. 4 (2012), pp. 447–87; Joshua Rovner, "AirSea Battle and Escalation Risks," SITC-NWC Policy Brief 12, *Institute on Global Conflict and Cooperation,* January 2012, igcc.ucsd.edu/; Caitlin Talmadge, "Would China Go Nuclear? Assessing the Risk of Chinese Nuclear Escalation in a Conventional War with the United States," *International Security* 41, no. 4 (Spring 2017), pp. 50–92; and Adam Segal, "U.S. Offensive Cyber Operations in a China-U.S. Military Confrontation," in Lin and Zegart, *Bytes, Bombs, and Spies*.
30. Paul Scharre, *Army of None: Autonomous Weapons and the Future of War* (New York: W. W. Norton, 2018), p. 21.
31. See Joshua Rovner, "Two Kinds of Catastrophe: Nuclear Escalation and Protracted War in Asia," *Journal of Strategic Studies* 40, no. 5 (2017), pp. 696–730.
32. Thomas J. Christensen, *Worse than a Monolith: Alliance Politics and Problems of Coercive Diplomacy in Asia* (Princeton, NJ: Princeton Univ. Press, 2011).
33. "Mission and Vision," *U.S. Cyber Command,* as of April 2018, https://www.cybercom.mil/.
34. Kevin L. Pollpeter, Michael S. Chase, and Eric Heginbotham, *The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations* (Santa Monica, CA: RAND, 2017).
35. Cristina L. Garafola, "The Evolution of PLAAF Mission, Roles, and Requirements," in *China's Evolving Military Strategy,* ed. Joe McReynolds (Washington, DC: Jamestown Foundation, 2016), p. 80.
36. People's Liberation Army Academy of Military Science, Military Strategy Studies Department, *Science of Military Strategy* (Beijing: Military Science, December 2013), quoted in Garafola, "Evolution of PLAAF," pp. 90–91.
37. Ibid., p. 116, quoted in John Costello and Peter Mattis, "Electronic Warfare and the Renaissance of Chinese Information Operations," in McReynolds, *China's Evolving Military Strategy,* p. 165. The 2013 edition of *Science of Military Strategy* argues that this approach is appropriate whatever the balance of capabilities: "In the future, no matter whether we will face an enemy with superior equipment or an enemy with inferior equipment, we will always need to focus on paralyzing enemy warfighting systems and emphasize 'striking at systems,' 'striking at vital sites,' and striking at [key] nodes." Ibid., p. 126, quoted in Kevin Pollpeter and Jonathan Ray, "The Conceptual Evolution of China's Military Space Operations and Strategy," in McReynolds, *China's Evolving Military Strategy,* pp. 257–58.
38. JCS, *Joint Operations,* p. xx.
39. Phil Haun, *Coercion, Survival, and War: Why Weak States Resist the United States* (Palo Alto, CA: Stanford Univ. Press, 2015).
40. Wartime learning reveals the true balance of power and resolve, and scholars have argued that such information can facilitate war termination. Others have focused on the importance of personal impressions in efforts to reach peace. Deception operations can slow down the process of wartime learning and undermine attempts to build trust. On the danger of military necessity, see Isabel V. Hull, *Absolute Destruction: Military Culture and the Practices of War in Imperial Germany* (Ithaca, NY: Cornell Univ. Press, 2005). On information, see Dan Reiter, *How Wars End* (Princeton, NJ: Princeton Univ. Press, 2009), and Branislav L. Slantchev, "The Principle of Convergence in Wartime Negotiations," *American Political Science Review* 97, no. 4 (November 2003), pp. 621–32. On trust, see Marcus Holmes, "The Force of Face-to-Face Diplomacy: Mirror Neurons and the Problem of Intentions," *International Organization* 67, no. 4 (October 2013), pp. 829–61, and Todd Hall and Keren Yarhi-Milo, "The Personal

Touch: Leaders' Impressions, Costly Signaling, and Assessments of Sincerity in International Affairs," *International Studies Quarterly* 56, no. 3 (September 2012), pp. 560–73.

41. The Seven Years' War (1756–63) left Great Britain with vast new possessions that it was not capable of holding. The strategic disaster of the American War of Independence (1775–83) served as a painful grand-strategic learning exercise. As one historian puts it, "Only in the atypical years of the mid-century did the British become obsessed with colonies for their own sake, and the debacle of the American War cured them of that." N. A. M. Rodger, *The Command of the Ocean: A Naval History of Britain, 1649–1815* (New York: W. W. Norton, 2005), p. 580.
42. See Joshua Rovner and Tyler Moore, "Does the Internet Need a Hegemon?," *Journal of Global Security Studies* 2, no. 3 (July 2017), pp. 184–203. For a critique, see Ben Buchanan, "Cyber-Operations and the Misunderstood Doomsday Machine: A Rebuttal," *War on the Rocks,* 24 August 2017, https://warontherocks.com/.

CHAPTER SIX

Agile Collaboration in Defense of the Nation

LT. GEN. TIMOTHY D. HAUGH, USAF; MAJ. WILLIAM R. GARVEY, USAF; CAPT. ERIKA E. VOLINO, USAF; AND MSGT. RYAN R. LEMMERMAN, USAF

The 2018 Department of Defense Cyber Strategy *energized the Department of Defense's approach to national cyber defense. Many of the measures highlighted in the* Cyber Strategy *fall within the capabilities of the Cyber National Mission Force (CNMF). The CNMF is tasked—in partnership with agencies such as the Department of Homeland Security and the Federal Bureau of Investigation—to defend the United States against malicious cyberspace actors. The states that sponsor these actors view cyberspace as a permissive environment where they can engage in malicious operations, steal intellectual property, and spread malign influence with few or no consequences. The CNMF is challenging this perception by defending forward and persistently engaging adversaries, assisted by new authorities and growing partnerships with interagency, international, and private-sector entities. This chapter highlights the CNMF's unique and indispensable role in fulfilling the Department of Defense's vision to adopt a wartime mind-set and defend American interests in cyberspace.*

U.S. Cyber Command's Cyber National Mission Force (CNMF) celebrated its fifth anniversary in January 2019. Reaching this milestone is cause for reflection on the progress the command has made, the lessons learned, and the challenges still to be overcome. Using the 2018 *Department of Defense Cyber Strategy* as a guide, this chapter highlights the CNMF's role in fulfilling the secretary of defense's vision for defending American interests in cyberspace. It lays out the history of the CNMF, explaining how the command has reorganized, its new authorities, key partners that the force has supported, and how the CNMF is persistently engaging malicious cyber actors.

A Brief History

A distributed denial-of-service (DDoS) campaign in 2012–13 targeted forty-six American institutions, primarily banks, whose websites crashed under the strain, preventing customers from accessing their accounts.[1] The attack cost American businesses tens of millions of dollars to remediate.[2] The federal government responded by releasing an indictment in 2016 against seven individuals working for ITSecTeam and Mersad, two

Iranian computer companies that performed work on behalf of the Islamic Revolutionary Guard Corps. Prominent cyber analysts assessed that the activity had been directed by the Iranian government.[3] The U.S. government relied on law enforcement as its primary means to combat this activity. The nascent U.S. Cyber Command (USCYBERCOM) played no significant role in the federal government's response. If asked to assist, USCYBERCOM would not have had the authorities, forces, or partnerships to respond in a meaningful way to a cyber attack against civilian infrastructure. Fortunately, the command has made significant progress in the intervening years and is now a key contributor to the nation's defense.

A combatant command is a headquarters that serves as a coordinator of activities and operations within a geographic region or across a common set of functions and services. In November 2008, Secretary of Defense Robert Gates directed the establishment of USCYBERCOM. It was initially instituted as a subunified command under the authority of U.S. Strategic Command. This relationship worked in USCYBERCOM's infancy, as the command established policies and directives to lay the groundwork for cyber operations. Every combatant command needs fielded forces to execute assigned missions, and in January 2014 USCYBERCOM activated the CNMF, a joint tactical command with a dedicated focus on cyberspace operations. The CNMF focuses on combating malicious cyber actors in defense of the nation and is the only force designed to engage in both internal defense measures and response actions.

President Trump authorized the elevation of USCYBERCOM from a subunified command to a combatant command in May 2018. That same month, the CNMF reached full operational capability, several months ahead of schedule. This was not an easy accomplishment. The CNMF's personnel had to meet a rigorous set of standards, to include training and maintaining fully qualified personnel on cyber teams while achieving a high operational tempo. Achieving full operational capability brings the expectation that the CNMF can and will contribute to deterring, disrupting, and defeating adversaries who endanger the nation's critical infrastructure. The timing is key. America's adversaries had hitherto enjoyed a period akin to "the Happy Time" during World War II, when German U-boats were able to operate unhindered in the Atlantic and inflict tremendous damage on American and Allied interests. The CNMF, in partnership with interagency, industry, and international partners, would challenge the early successes of America's adversaries who have operated below the level of armed conflict with impunity.[4]

The 2018 *Department of Defense Cyber Strategy* (hereafter the *Cyber Strategy*) lays out a framework to execute the *National Defense Strategy* and *National Military Strategy* in cyberspace. It asserts that the world order has shifted to long-term strategic competition with peer and near-peer adversaries. These adversaries compete in cyberspace, below

the threshold of armed conflict. In many cases they are challenged solely by the cybersecurity industry. The *Cyber Strategy* outlines how the Department of Defense (DOD) is taking action to defend forward and support partners with authorities and responsibilities for homeland defense. It directs the department to "*defend forward, shape the day-to-day competition, and prepare for war* by building a more lethal force, expanding alliances and partnerships, reforming the Department, and cultivating talent, while actively competing against and deterring our competitors."[5] Owing to its unique capabilities, the CNMF plays a critical role in accomplishing the secretary of defense's vision to compete, deter, and win in cyberspace.

Structuring the Force to Defend the Nation

> *The Department's workforce is a critical cyber asset. . . . We will create processes for maintaining visibility of the entire military and civilian cyber workforce and optimizing personnel rotations across military departments and commands, including maximizing the use of the Reserve Component.*
>
> DOD CYBER STRATEGY

USCYBERCOM has organized its forces to support agile defense. The armed services present 133 cyber teams to the commander of USCYBERCOM with which to execute combatant-command authority. The CNMF consists of thirty-nine of these teams, along with a modest staff. The CNMF recently reorganized its cyber teams into five joint cyber task forces—four aligned against regional malicious cyber actors and a fifth task force dedicated to addressing threats to national critical infrastructure. The latter, known as the "Emerging Threats" task force, is adversary-agnostic and staffed with experts in infrastructure vulnerabilities and threats. Attribution of malicious cyber activity is often difficult and having a force that addresses emerging threats in an adversary-agnostic manner allows the CNMF to pivot quickly to threats as they occur. Emerging Threats leads the CNMF's response to malicious activity until task force analysts (working closely with partner organizations) attribute the activity to a threat actor and hand off responsibility to the appropriate regionally focused task force. The Emerging Threats task force is the CNMF's focal point for interagency partnership and the point for intake of data from and collaboration with the private sector. The task force's worldwide scope and subject-matter expertise make it an agile organization well suited to address emerging threats.

The "Total Force" is an integral part of the CNMF's ability to defend the nation's key cyber terrain. The CNMF is taking advantage of Total Force inclusivity to bring skilled cyber professionals into the fight. The Active component that provides the bulk of

personnel for the CNMF's thirty-nine cyber teams is augmented by Guard and Reserve Component forces. The presence of Guard and Reserve personnel in the CNMF is a force multiplier, as they bring familiarity and continuity to the mission. Additionally, many Guard and Reserve personnel have civilian careers that keep them on the cutting edge of cybersecurity and technology (working for companies such as Microsoft, Google, and Symantec) and they bring the benefit of their experience to their cyber teams.

New Authorities Enable Agile Defense

> *The United States cannot afford inaction: our values, economic competitiveness, and military edge are exposed to threats that grow more dangerous every day. We must assertively defend our interests in cyberspace below the level of armed conflict and ensure the readiness of our cyberspace operators to support the Joint Force in crisis and conflict.*
>
> *DOD CYBER STRATEGY*

The United States is committed to the rule of law and to the promotion of an international rules-based order in cyberspace. Although adversary nations may view cyber as an unconstrained environment with no consequences for malicious actions, America's cyber warriors meticulously adhere to law, DOD policy, and commander's guidance, and they are in close consultation with our interagency partners when conducting operations. This is foundational to implementing new authorities that have expanded the capability of USCYBERCOM to defend the nation.

The National Defense Authorization Act (NDAA) for fiscal year 2019 expanded USCYBERCOM's freedom to maneuver in cyberspace. Section 1632, "Affirming the Authority of the Secretary of Defense to Conduct Military Activities and Operations in Cyberspace," is particularly noteworthy. It declares activities or operations in cyberspace to be "traditional military activities," in line with DOD activities in other domains. Section 1632 affirms that the secretary of defense may conduct activities in cyberspace to defend the United States and its allies in circumstances short of war and outside named "areas of hostility." These actions are to be "for the purposes of preparation of the environment, information operations, force protection, deterrence of hostilities and counter-terrorism operations."[6] Cyberspace requires situational awareness of a rapidly moving series of adversaries, given the ability of the adversary to co-opt internet-connected devices anywhere in the world for malicious purposes. Allowing the nation's cyber warriors to prepare the battlespace before a crisis is a significant improvement over the very difficult challenge of performing preparation in the midst of a crisis. It is important to understand that this legislative language should be treated as

an authorization not for the use of military force but rather for posturing to use military force effectively when called on to defend the nation. The recent *Cyber Strategy* provides an impetus to conduct maneuver as far forward as possible, while section 1632 of the NDAA establishes congressional oversight of mechanisms and gives the CNMF's elements room to maneuver within assigned missions.

Interagency Partnership

> *In coordination with other Federal departments and agencies, the Department will build trusted relationships with private sector entities that are critical enablers of military operations and carry out deliberate planning and collaborative training that enables mutually supporting cybersecurity activities.*
>
> DOD CYBER STRATEGY

The 2018 *Cyber Strategy* highlights "persistent engagement" as key to the department's approach to cyberspace operations.[7] Gen. Paul Nakasone, commander of USCYBERCOM, defines persistent engagement as the concept that states are in constant contact with adversaries in cyberspace, with success determined by how cyber forces *enable* partners and how they *act* while in contact with cyber adversaries.[8] In persistent engagement, the CNMF must enable interagency partners such as the Federal Bureau of Investigation and the Department of Homeland Security (DHS) by providing information that can be shared with critical infrastructure elements or appropriate entities in the cybersecurity industry. General Nakasone considers enabling partners to be two-thirds of persistent engagement and the other third to be the ability to act against cyber adversaries when called on.[9]

Partnerships are key to defending the nation's sixteen "critical infrastructure sectors." USCYBERCOM's close relationship with the National Security Agency enables the CNMF's personnel who are working in a cyber capacity to collaborate with their counterparts in the signals-intelligence and information-assurance fields. A strong relationship between cyber and signals-intelligence functions is key to cyber situational awareness. Additionally, the relationship between DOD and DHS is crucial for the ability of the CNMF to accomplish its mission, given DHS's mandate to protect the nation's critical infrastructure. The NDAA introduced new avenues for DOD to partner with DHS. Section 1650, "Pilot Program Authority to Enhance Cybersecurity and Resiliency of Critical Infrastructure," authorizes the secretary of defense (in coordination with the secretary of homeland security) to provide up to fifty DOD technical cyber personnel to DHS every fiscal year.[10] These personnel will increase communication and collaboration with interagency partners and provide support to enhance the protection role and

better defend forward. Alongside the new authorizations from the NDAA, an agreement signed by the secretaries of defense and homeland security in late 2018 solidified the agencies' partnership and outlined areas for increased cooperation.[11] The objectives of the interagency partnership include use of a threat-informed and risk-based approach to maintain critical functions and services, a close working relationship with the intelligence community to build a common understanding of cyber threats, and continual coordination between the agencies to support the planning and operations of both departments.

Collaboration between DOD and DHS is already under way. In support of efforts to combat foreign influence in the 2018 midterm elections, the CNMF embedded cyber operators in DHS. These personnel provided assistance at DHS's cybersecurity watch floor (the Integrated Operations and Communications Center), which maintains situational awareness of cyber threats to the United States.[12] In addition to resource sharing, information sharing between the agencies will play a key role in protecting critical infrastructures from cyber aggression. The information gathered by DOD and shared with DHS is not intended to remain solely within federal channels. Once shared with DHS, information can then be passed to those who need to know in industry, as well as to state and local governments—providing an enhanced form of "defense in depth."[13]

Private-Sector Partnership

> *The Department must be prepared to defend non-DoD-owned Defense Critical Infrastructure (DCI) and Defense Industrial Base (DIB) networks and systems. Our chief goal in maintaining an ability to defend DCI is to ensure the infrastructure's* continued functionality and ability to support DoD objectives *in a contested cyber environment.*
>
> *DOD CYBER STRATEGY*

Most of the nation's critical infrastructure is owned and maintained by the private sector. In addition, federal dollars no longer drive American innovation. In 2018 the federally sponsored share of $533 billion spent in U.S. research and development was 26 percent, while the private sector's share was 66 percent.[14] This underscores both the importance of defending the private sector and the potential value of the private sector's partnering with the U.S. government to defend the nation's key infrastructure. The CNMF certainly cannot do it alone. CNMF's deputy commander, Maj. Gen. Stephen Hager, summarized the need for strong private-sector partnership succinctly: "If I'm going to defend forward to help our nation's critical infrastructure, I need to know what's most important to those critical infrastructures—to the financial sector, to the energy sector, so if I am doing reconnaissance in gray [contested] and red [adversary] space, I

know what to look for. So I know what to look for as a military person, but I don't necessarily know what the financial institutions think [is] important."[15]

Section 1642 of the NDAA allows the president to authorize the secretary of defense to take appropriate and proportional action in foreign cyberspace to disrupt, defeat, and deter attacks.[16] The section also allows the secretary to "make arrangements with private sector entities, on a voluntary basis, to share threat information related to malicious cyber actors, and any associated false online personas or compromised infrastructure."[17] Project INDIGO is a prime example of such collaboration; it is a pilot initiative between the CNMF and the Financial Systemic Analysis & Resilience Center (FSARC).[18] FSARC is an industry-funded, nonprofit entity that focuses on threats to the most critical American financial firms. The project was coordinated with and operates in support of DHS, the Department of the Treasury, and the Office of the Secretary of Defense. INDIGO commenced in October 2017, when CNMF personnel received FSARC training on risks associated with key financial systems. The training concluded with the CNMF analysts observing a financial-sector exercise in which nine major financial institutions subjected a key financial system to a risk-mitigation-measure stress test, validating the FSARC's "playbook" for such an incident.[19]

The project also included information sharing. USCYBERCOM received FSARC consolidated and anonymized network-defense data from American financial institutions. This information included malware samples, threat products, and technical artifacts related to state-actor activity. The shared data informed the CNMF analysts' understanding of the threat actors. The CNMF personnel analyzed the FSARC data and produced several intelligence reports for Treasury, which then distributed them to industry partners. The INDIGO pilot has matured into the DOD/DHS PATHFINDER initiative—a wider effort to facilitate cyber collaboration between the U.S. government and private-sector entities. The financial sector was the first instantiation of PATHFINDER; the program will expand to the energy sector (in partnership with DHS and the Department of Energy).

International Partnership

> *Many of the United States' allies and partners possess advanced cyber capabilities that complement our own. The Department will work to strengthen the capacity of these allies and partners and increase DoD's ability to leverage its partners' unique skills, resources, capabilities, and perspectives.*
>
> *DOD CYBER STRATEGY*

USCYBERCOM has also evolved to address today's challenges through international partnerships. The cyber domain is not bound by geographic borders, and cyber threats to America's allies can and likely will become threats to the United States. The CNMF, in coordination with U.S. European Command, has sent American service members to work side by side with NATO and non-NATO European allies. In 2018, CNMF personnel engaged in defensive cooperation efforts in Belgium, Estonia, France, Germany, Lithuania, Macedonia (today North Macedonia), Montenegro, Ukraine, and the United Kingdom. By embedding with host-nation military and civilian cyber experts, CNMF defenders were able to share expertise, identify and remediate malicious activity, and expose malicious cyber actors and their malware.[20] The success of these initial efforts laid the foundation for future "hunt" missions with international partners. The CNMF is prepared to send personnel to any theater to expose malicious cyber actors, thereby strengthening both American and partner-nation defenses, and to pursue foreign threats relentlessly in and through cyberspace.

As the CNMF generates insights into malicious cyber threats, it shares actionable information outside of U.S. government channels, including with international partners and the private sector. USCYBERCOM took a step forward in November 2018 when the CNMF publicly disclosed malware its analysts had uncovered by publishing the malware's "fingerprint" to a popular malware-aggregation website. (Major antivirus companies use these sites to update their threat definitions.) The CNMF also created a Twitter account to disseminate threats quickly to cybersecurity practitioners and members of the public.[21] The USCYBERCOM Malware Alert account was not meant to provide attribution; however, the cybersecurity industry is quite capable of contributing its own analysis—and did so in this case. The initial batch of signatures the CNMF posted in November 2018 were matched by the aggregation site to LoJack malware, which several cybersecurity companies have tied to Advanced Persistent Threat 28, a designator for malicious cyber activity publicly attributed to Russian-state actors.[22] State actors typically invest a substantial amount of time developing malware, and the CNMF can help the cybersecurity industry rapidly detect and mitigate it. The CNMF's efforts to expose malware achieve several goals—benefiting global cybersecurity, signaling American intent to partner with private-sector and international entities, changing the conditions of security in our favor, and constraining adversaries.

Defending the Nation by Defending Forward

> *The Department will counter cyber campaigns threatening U.S. military advantage by defending forward to intercept and halt cyber threats.*
>
> *DOD CYBER STRATEGY*

The recent *Cyber Strategy* promoted a new perspective when it stated, "We will *defend forward* to disrupt or halt malicious cyber activity at its source."[23] Defending forward is a shift in DOD's approach to cybersecurity, from waiting to engage adversaries inside DOD networks to proactively engaging them as close to the source as possible.[24] As stated by Lt. Gen. Vincent Stewart, the former deputy commander of USCYBERCOM, at the 2018 CYCON conference in Washington, DC, "defending forward is nothing more than being active in your defense. Just like we've always done—fight forward, disrupt forward, deny forward, make his servers less effective and have a minimal number of clean-up issues in blue [friendly] space."[25]

Defending forward can take many forms. One is deploying the CNMF to partner nations to find and expose adversary presence on devices that could be used to target the United States. Publicly disclosing malware that the CNMF discovers is another example of defending forward. More examples might be:

- Partnering with interagency, international, and private-sector entities to defeat malicious cyber activity
- Conducting preparation of the environment (to include in areas outside named areas of hostility)
- Taking appropriate and proportional action in foreign cyberspace to disrupt, defeat, and deter adversary attacks

The bottom line of "defend forward" is that USCYBERCOM will persistently engage malicious cyber actors to defend the nation. In coordination with our interagency partners, the CNMF will set the conditions in which the United States competes in cyberspace and defends the nation's key infrastructure from cyber aggression.

To measure the progress that USCYBERCOM has made in its ability to defend the nation, let us revisit the 2012–13 Iranian DDoS of the American financial sector and examine how the CNMF could help defeat such an attack today. Through intelligence analysis and information-sharing partnerships, the CNMF could provide indications and warnings of malicious cyber activity and ensure that its forces and partners are postured to respond. During the attack, the victim institutions would provide network-defense data to USCYBERCOM through processes initially defined by Pathfinder. Working in support of DHS and the Departments of Justice and the Treasury, CNMF would analyze the data and issue reports back to Treasury and through it to the financial sector—enabling the financial institutions' cybersecurity teams to defend themselves better. The CNMF (with network-owner permission and—if needed—requested support from DHS) could deploy forces to federal, state, local, or partner-nation networks containing devices that had been hacked and added to the attacker's "botnet." If

the CNMF operators uncover the malware the attacker used to do so, they can publicly disclose its signature. The botnet would shrink in size and effectiveness as antivirus programs updated their threat definitions and quarantined the attacker's malware. Lastly, the CNMF could engage in cyberspace "traditional military activities" authorized in the fiscal year 2019 NDAA. If the attacker was one of the four nations mentioned in the NDAA's section 1642, USCYBERCOM could "take appropriate and proportional action in foreign cyberspace to disrupt, defeat, and deter" the DDoS campaign.[26] In short, USCYBERCOM has increased the partnerships, processes, and authorities needed to provide agile defense of the nation's key infrastructure. Although much remains to be done, we should recognize the progress that has been made.

Conclusion

> *The* 2018 DoD Cyber Strategy *directs the Department to* defend forward, shape the day-to-day competition, and prepare for war *by building a more lethal force, expanding alliances and partnerships, reforming the Department, and cultivating talent, while actively competing against and deterring our competitors. Taken together, these mutually reinforcing activities will enable the Department to compete, deter, and win in the cyberspace domain.*
>
> *DOD CYBER STRATEGY*

The men and women of the CNMF are embracing their role in fulfilling the *Cyber Strategy*. CNMF operators, planners, and intelligence analysts daily demonstrate innovative approaches to complex cyber problems—all with the goal of defending the nation. Previous policies bound the hands of America's cyber defenders and allowed the nation's adversaries to set the conditions of the cyberspace security environment. While authoritarian states invest heavily in limiting their populations' access to information and attempt to control or cut off the flow of information between people, the United States values an open, interoperable, reliable, and secure internet.[27] This end state can only be realized with a whole-of-government (and beyond, including private-sector partners) approach to cybersecurity, including military capabilities.

The CNMF provides capabilities that span the spectrum of cyberspace operations. These include defensive "hunt" operations on DOD, domestic, and foreign networks. They also include military activities authorized in the 2019 NDAA, such as information operations and operations in foreign cyberspace to disrupt, defeat, or deter attacks. The CNMF enables and is enabled by partnerships with interagency, industry, and international entities. The CNMF has also demonstrated that it can discover and publicly expose malicious cyber actors. The sum of these capabilities is an ability to set the

conditions of the cyberspace security environment in our favor and to counter malign influence activities conducted in and through cyberspace. In short, the CNMF—in partnership with interagency, private-sector, and international entities—plays a unique and indispensable role in fulfilling the secretary of defense's vision for defending American interests in cyberspace.

Notes

Epigraphs: DOD, *Summary DOD Cyber Strategy 2018,* respectively in order: pp. 6, 7, 5, 3, 5, 4, 7.

1. U.S. Justice Dept., "Seven Iranians Working for Islamic Revolutionary Guard Corps–Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks against U.S. Financial Sector," press release, 24 March 2016, https://www.justice.gov/.
2. Ibid.
3. Nicole Perlroth and Quentin Hardy, "Bank Hacking Was the Work of Iranians, Officials Say," *New York Times,* 8 January 2013.
4. U.S. Cyber Command [hereafter USCYBERCOM], *Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. Cyber Command* (Fort Meade, MD, March 2018), p. 3, https://www.cybercom.mil/.
5. U.S. Department of Defense [hereafter DOD], *Summary Department of Defense Cyber Strategy 2018* (Washington, DC, 2018), https://media.defense.gov/ [emphasis original].
6. John S. McCain National Defense Authorization Act for Fiscal Year 2019 [hereafter NDAA FY19], H.R.5515, 115th Cong. (2018), https://www.congress.gov/.
7. DOD, *Summary DOD Cyber Strategy,* p. 4.
8. "An Interview with Paul M. Nakasone," *Joint Force Quarterly* 92 (1st Quarter 2019).
9. Ibid.
10. NDAA FY19.
11. John Rood, "Joint Secretary of Defense–Secretary of Homeland Security Memorandum on Defending the Homeland from Strategic Cyber Threats," 28 September 2018.
12. Lauren Williams, "DOD, DHS Report Advancing Cyber Cooperation," *Federal Computer Weekly,* 15 November 2018.
13. Rood, "Joint Security Memorandum."
14. "2018 Global R&D Funding Forecast," supplement, *R&D Magazine* (Winter 2018).
15. Stephen Hager, "CyCON US 2018—Cyber Conflict during an Era of Strategic Competition," YouTube, 7 January 2019, video, 30:20, https://www.youtube.com/.
16. Section 1642 is titled "Active Defense against the Russian Federation, People's Republic of China, Democratic People's Republic of Korea, and Islamic Republic of Iran Attacks in Cyberspace." NDAA FY19.
17. Ibid.
18. Chris Bing, "Inside 'Project Indigo,' the Quiet Info-Sharing Program between Banks and U.S. Cyber Command," *Cyber Scoop,* 21 May 2018, https://www.cyberscoop.com/.
19. "Identifying Cyber Threats with FSARC," *JPMorgan Chase,* 9 October 2018, https://www.jpmorgan.com/.
20. USCYBERCOM, "U.S., Montenegro Conduct Groundbreaking Cyber Defense Cooperation," press release, 2 October 2018, https://www.cybercom.mil/.
21. USCYBERCOM Malware Alert (@CNMF_VirusAlert), https://twitter.com/cnmf_virusalert?lang=en.
22. Lee Matthews, "U.S. Cyber Command Shares Malware Samples to Help Thwart Bad Actors," *Forbes,* 8 November 2018, https://www.forbes.com/.
23. DOD, *Summary DOD Cyber Strategy,* p. 1 [emphasis original].
24. Vincent Stewart, "Lt Gen Vincent Stewart, Deputy Commander, US Cyber Command," *Army Cyber Institute,* 18 December 2018, video, 25:57, https://cyber.army.mil/.

25. Ibid., 26:25.
26. NDAA FY19.
27. *National Cyber Strategy* (Washington, DC: White House, September 2018), https://www.whitehouse.gov/.

CHAPTER SEVEN

Public-Private Partnerships in Cyberspace in an Era of Great-Power Competition

ERICA D. BORGHARD AND SHAWN W. LONERGAN

Effective public-private collaboration is vital to cultivating a U.S. advantage in the context of emerging great-power challenges in cyberspace. Two areas that are of particular concern are the civilian assets that contribute to the overall military advantage of the United States—defense critical infrastructure and the defense industrial base—and the critical infrastructure that undergirds the U.S. economy and provides the essential functions and services on which the American public relies for daily life. In this chapter, we advance a comprehensive proposal organized around public-private partnerships to address the challenge of defending critical infrastructure in cyberspace. The core logic of our proposal rests on shifting the conceptual orientation in both the U.S. government and the private sector toward systemic "resilience" rather than a singular focus on defense or deterrence.

Introduction: Resilience in the Context of Great-Power Competition

There is a growing recognition among senior leaders in the American foreign policy community that over the course of the past decade the distribution of power in the international system has shifted in a way that disadvantages the United States. There is an imperative for the United States to assess the implications of these changes and position itself to secure a favorable international environment, one that reflects its interests and values.[1] This shift in the balance of power is manifest in the very public efforts of U.S. strategic competitors to challenge the United States in arenas where the latter had, in recent history, been dominant. Examples include the persistently growing Chinese defense budget (which grew 110 percent between 2008 and 2017 to U.S.$228 billion), Russian and Chinese efforts to project regional military power in perceived historical spheres of influence, Chinese leadership in international institutions (such as the Asian Infrastructure Investment Bank), and Russian nuclear modernization.[2] Much of the contemporary academic writing on this topic focuses on the *potential* for a decisive shift in the global balance of power—that is, one that has not yet occurred. For instance,

the United States still outspends China on defense by more than double, and Russian nuclear modernization has been met with a reinvigorated program in the United States, driven by the *Nuclear Posture Review 2018*.[3] However, the reality is that great-power competition is already occurring—and has been for a number of years—in and through global cyberspace.

The idea of the United States engaged in an international great-power competition permeates recent strategy documents, including the 2017 *National Security Strategy,* the *2018 National Defense Strategy,* and the 2018 *Department of Defense* [*DOD*] *Cyber Strategy.* The 2017 *National Security Strategy* depicts an international environment in which great-power competition has resurfaced after having lain dormant in the decades following the fall of the Soviet Union. What distinguishes the current challenge from previous ones is that U.S. adversaries actively seek to contest American advantages and interests below the level of war—this is why the environment is characterized as "competition" rather than "conflict."[4] Similarly, the *2018 National Defense Strategy* portrays the current strategic environment as defined by the "*reemergence of long-term, strategic competition* by . . . revisionist powers."[5] In cyberspace, great-power competition takes the form of persistent and corrosive adversary campaigns that, when considered as individual cyber incidents or attacks, may appear to be relatively inconsequential but, when assessed in the aggregate over the long term, reveal adversary efforts of strategic importance. In particular, there are three key threats to the United States posed by great-power competition in cyberspace: first, cyber-enabled influence campaigns that undermine public trust in and legitimacy of U.S. institutions; second, the erosion of the U.S. innovation base, particularly national security technologies, through widespread cyber-enabled theft of intellectual property (IP) at scale; and third, disruptive or destructive campaigns targeting critical infrastructure and key resources (CIKR).[6] Taken together, as described in the 2018 *DOD Cyber Strategy,* these "pose long-term strategic risk to the Nation as well as to our allies and partners."[7]

The private sector plays an essential role in this competition, especially in cyberspace. Therefore, effective public-private collaboration is vital to cultivating a U.S. advantage in the context of emerging great-power challenges. As the 2018 *DOD Cyber Strategy* observes, "the private sector owns and operates the majority of U.S. infrastructure and is on the frontlines of nation-state competition in cyberspace."[8] Two areas that are of particular concern and where the private sector is a key stakeholder are the civilian assets that contribute to the overall military advantage of the United States—defense critical infrastructure and the defense industrial base (DIB)—and the critical infrastructure that undergirds the U.S. economy and provides the essential functions and services on which the American public relies for daily life.[9] The DIB, comprising over 100,000 entities, is the "worldwide industrial complex that enables research and development, as well as design, production, delivery, and maintenance of weapons systems, subsystems,

and components or parts, to meet US military requirements."[10] Defense critical infrastructure includes both DOD and non-DOD-owned assets that are "essential to project, support, and sustain military forces and operations worldwide."[11]

Specifically, there are two concerns regarding adversary cyber threats to essential private-sector stakeholders. First, the immense scale of cyber-enabled IP theft across the U.S. economy and military affects great-power competition, because it enables U.S. adversaries and competitors to reap technological, economic, and military gains faster than the rate of American innovation and negates U.S. first-mover advantages. Put simply, the contest in cyberspace is shaping the distribution of conventional military power between the United States and its strategic competitors, and this will only accelerate, absent a dedicated, significant U.S. effort to arrest and roll back these dynamics.[12] Second, the U.S. private sector, specifically privately owned and operated CIKR, is an important target of coercion for political/strategic objectives by U.S. adversaries. Historical, legal, and cultural factors limit the extent to which the U.S. government and private entities can—or are willing to—collaborate to promote U.S. national and economic security. However, in an era of great-power competition, the U.S. government can no longer afford for cyberspace to be mostly a self-help environment for the private sector.

In this chapter, we advance a comprehensive proposal that builds on prior work on public-private collaboration to defend the U.S. financial services sector in cyberspace, specifically Project Indigo, which became the Pathfinder initiative.[13] We address the broader context and challenge of defending CIKR across all sectors as well as of thwarting cyber-enabled IP theft.[14] The core element of our proposal is shifting the conceptual orientation in both the U.S. government and the private sector toward systemic "resilience" rather than a singular focus on defense or deterrence. Specifically, there is a nontrivial set of malicious adversary behavior that does not rise to a threshold that would trigger U.S. employment of the full spectrum of credible retaliatory response options, making deterrence difficult. Moreover, effective defense against these threats is difficult. Reorienting around resilience, therefore, means being realistic about the probability of adverse events and making appropriate investments in readiness, response, and rapid recovery efforts. We argue that resilience can be cultivated through shared programs that promote intelligence sharing and early warning and the development of joint playbooks and response options.

A key goal of our proposed approach is building and continuously cultivating the resilience of the U.S. innovation base and critical infrastructure to ensure they can withstand and rapidly recover from cyber events or adversary campaigns of strategic significance. Resilience rests on restoring essential functions and services. With respect to critical infrastructure, this requires identifying core business functions in an individual firm or even sector and understanding cross-sector interdependencies that

could trigger cascading effects during a crisis. Within the national security innovation base, resilience rests on an improved assessment of the supply chain and third-party risk stemming from more-vulnerable contractors and firms that provide easier points of entry for the theft of valuable IP.

A resilience-based approach requires a wholesale reassessment of the conceptual frameworks that we currently employ (to our detriment) to define and understand the nature of the threat environment, our vulnerabilities, and risks.[15] While defensive measures—whether taken by network defenders in the private sector or government, either separately or in collaboration—are important, they are insufficient in isolation and should not be seen as collectively a panacea. This is because a well-resourced, dedicated, patient, and skilled adversary can almost always surmount network and endpoint defenses to gain access to critical networks and systems and deliver disruptive (and potentially destructive) effects against them. Investing in the continuous maturing of defensive postures is important for addressing routine, day-to-day cyber incidents. However, there is a threshold at which it is more efficient and effective to reduce risk through resilience, given the (relatively low) probability of a single catastrophic event and the reality of persistent adversary campaigns that are already occurring and pose a strategic threat.

Furthermore, while deterrence remains an important strategic concept for the U.S. government in cyberspace, we should acknowledge that thus far a deterrence-based approach to cyber threats has only been successful to prevent cyber attacks above the level of armed attack.[16] The fundamental objective of deterrence is to preserve the status quo—to prevent adversaries from taking undesirable actions that they have not yet taken. As defined by Robert Art in his seminal piece on the use of military force, deterrence is "the deployment of military power so as to be able to prevent an adversary from doing something that one does not want him to do and that he might otherwise be tempted to do by threatening him with unacceptable punishment if he does it. Deterrence is thus the threat of retaliation. Its purpose is to prevent something undesirable from happening."[17]

Leveraging deterrence for U.S. cyber strategy is not sufficient to address the full range of threats and challenges posed by adversary behavior in the domain.[18] The United States seeks to maintain the status quo where deterrence has been successful—against cyber attacks targeting the United States that would amount to an armed attack. However, the United States demonstrably endeavors to *change* the status quo where deterrence has not been successful—against cyber attacks on the United States that do not rise to that threshold. It finds the latter unacceptable, specifically the using of cyber means to steal U.S. intellectual property (and at astounding rates), adversary efforts to hold critical infrastructure at risk, and cyber-enabled influence operations that undermine confidence in U.S. democracy and institutions.

The United States should develop concepts for great-power competition in cyberspace that incorporate the notion of resilience, which is built on assumptions that have more fidelity with the reality of the current environment.[19] The concepts of "defend forward" and "persistent engagement" are consistent with this idea.[20] Defend forward, as these authors understand it, posits that to disrupt and defeat malicious adversary cyber campaigns, the United States should proactively observe, pursue, and counter adversary operations in day-to-day competition. The concept follows from the recognition that organizing U.S. cyber forces around a reactive posture has been ineffective in preventing a number of important adversary cyber campaigns and that initiatives that leverage solely nonmilitary instruments of power, such as naming and shaming, sanctions, and indictments, have insufficiently altered the adversary's cost/risk calculus. The cyberspace environment is dynamic, opportunities are fleeting, and U.S. adversaries are agile and adaptive. Therefore, keeping pace with them and anticipating their behavior rather than reacting and responding to them requires gaining and maintaining access against defined targets and pursuing adversaries as they maneuver. However, defend forward represents only one element of what should be a more systemic and holistic resilience initiative. As we demonstrate below, the resilience of the nation as a whole will ultimately depend on the extent to which the United States implements more-robust measures for public-private collaboration.

Protecting U.S. National Security Intellectual Property

Technological and military innovation have served as historical drivers of the U.S. conventional advantage over its adversaries. Cyber-enabled theft of U.S. intellectual property, particularly national security innovation information, coupled with adversary investment in technologies with military applications (e.g., artificial intelligence, machine learning, or 5G telecommunications infrastructure) threatens to erode that advantage.

However, it is important to note that the general category of cyber-enabled intellectual property theft belies an important distinction between economic espionage conducted using cyber means—which the U.S. government considers to be an unacceptable state practice—and certain types of IP theft that support national security objectives—which is permissible under most interpretations of customary international law because it is considered a necessary state practice.[21] The waters are further muddied by the fact that the same threat-actor groups often conduct cyber-enabled economic espionage for commercial gain and also IP theft for national-security reasons. Our analysis and policy recommendations focus on the latter challenge, because while this behavior is not necessarily illegal, it represents a significant national security threat in its potential to

erode the long-term competitive military advantage that the United States enjoys. This is separate and distinct from global economic competition.

Despite decades of systematic, large-scale cyber-enabled theft of U.S. intellectual property, it was not until 2016 that, speaking before Congress, the former director of the National Security Agency and commander of U.S. Cyber Command, Gen. Keith Alexander, described how cyberspace had facilitated the largest transfer of wealth in history (yet this was a reference to economic rather than national-security theft).[22] Until recently, the U.S. government was reticent to address IP theft by China publicly. Indeed, while China has been associated with cyber espionage since at least the early 1990s, the first time the United States publicly named the Chinese government as being behind cyber-enabled IP theft was in a 2011 National Counterintelligence Executive report.[23] This ambivalence was definitively rejected in favor of more-aggressive public posturing following a February 2013 *New York Times* article based on a seminal investigative report issued by Mandiant earlier that year that directly named the Chinese People's Liberation Army as one of the sources of a series of cyber intrusions targeting private corporations in the United States.[24] The next month Tom Donilon, the U.S. national security advisor at the time, addressed the Asia Society in New York City and issued the first public admonishment by a senior U.S. official of Chinese cyber activities against U.S. corporations and national interests.[25] It was subsequently reported that, three months prior to Donilon's speech, the United States had issued a secret démarche order to the Chinese government in protest of cyber espionage on the heels of over six months of unproductive closed-door dialogues between the two governments.[26]

This public rebuke set the stage for how the U.S. government would subsequently treat the challenge posed by adversary IP theft, which has thus far leveraged diplomatic, economic, and legal instruments of power. Specifically, the United States adopted a "naming and shaming" strategy in an attempt to foster international norms against cyber-enabled economic espionage and IP theft, coupled with indictments and sanctions, such as the May 2014 indictment of five People's Liberation Army officers for the activities identified in the 2013 Mandiant report.[27] Arguably the most successful example of this approach is the 2015 diplomatic agreement signed between Presidents Obama and Xi to refrain from cyber-enabled IP theft conducted to secure an economic competitive advantage.[28] More recently, the United States and China initiated another round of bilateral talks in October 2017 that reaffirmed the 2015 agreement.[29] However, Chinese compliance with the 2015 agreement has been varied. While the March 2018 *Worldwide Threat Assessment* noted that Chinese cyber economic espionage did decrease following the 2015 agreement, IP theft for national-security purposes continued apace: "Most Chinese cyber operations against U.S. private industry are focused on cleared defense contractors or [information technology] and communications firms whose products

and services support government and private sector networks worldwide."[30] The January 2019 *Worldwide Threat Assessment* reaffirmed the central role of cyber-enabled IP theft in adversary efforts to reduce U.S. military/technological advantages and specifically calls out Russian and Chinese leadership.[31] More recently, in March 2019 the *Wall Street Journal* reported that the U.S. Navy is "under cyber siege" by Chinese-affiliated threat groups seeking to steal national security innovation information.[32]

While legal and diplomatic efforts have generated some positive outcomes, it is apparent that they are inadequate, because they have failed to stem the tide of IP theft. It is certainly the case that an actor such as China values its international reputation, and naming and shaming might generate some behavior modifications. However, it is clearly not sufficiently costly when balanced against the enormous gains of widespread pilfering of the U.S. strategic innovation base. Therefore, the challenge is to discern how to implement policies that create meaningful costs for adversaries that conduct cyber-enabled IP theft in a way that is not self-defeating in their effects on the U.S. economy (for instance, through trade wars).[33] Moreover, some U.S. efforts to increase adversary costs could be misperceived as precursors to war if broader relations were very strained. Public and private diplomacy, therefore, should continue to fulfill a key signaling function, particularly as diplomatic measures are coupled with cyber actions. Over time, this could contribute to stabilizing effects between cyber rivals through building a shared diplomatic language that would help clarify how parties understand and interpret thresholds.[34]

A program to impose costs on U.S. adversaries that use cyber means to steal intellectual property in support of their national security objectives should be organized around deeper public-private collaboration among the DIB, DOD as the Sector-Specific Agency, and the interagency. In many ways, the hurdles to collaboration across stakeholders in the DIB are minimal in comparison to those confronting the shared defense of CIKR. For instance, classification impediments are not particularly salient across the DIB. Most companies in the DIB are familiar with operating in classified environments to produce products for classified consumers, employ personnel with security clearances, and even have DOD-sponsored sensitive compartmented information facilities and other collateral spaces that enable routine classified communication. Beyond standards to handle classified information, DOD enforces cybersecurity requirements on the DIB, including the newly established Cybersecurity Maturity Model Certification, which promulgates a framework for cybersecurity standards and risk organized around a firm's level of maturity.[35] Furthermore, the DIB and DOD operate from common cultural frameworks, values, ideas, and, for the most part, a shared view of the threat environment, with personnel transitioning between employment in both areas.

The institutional tools are also largely in place to support deeper collaboration between private-sector firms in the DIB and the interagency. Within DOD, the DIB Cybersecurity Program was established as a voluntary information-sharing initiative to share unclassified and classified cyber-threat information. It also supports an analyst-to-analyst exchange program and provides analysis and forensics support. All defense firms that participate in the DIB Cybersecurity Program are cleared defense contractors, including affiliated universities and federally funded research and development centers, and are required to possess the physical and network infrastructure to receive classified information. The DOD Cyber Crime Center is the implementation arm of the DIB Cybersecurity Program. More recently, the Cybersecurity Directorate (CSD) was established within the National Security Agency with the mission, among other things, to protect the DIB against cyber-enabled IP theft.[36] On the private-sector side, an information-sharing program within the defense sector exists through the National Defense Information Sharing and Analysis Center (NDISAC), formerly known as the Defense Industrial Base Information Sharing and Analysis Organization. The NDISAC provides mechanisms for a wide scope of cyber-threat intelligence sharing across the sector.

However, while the organizational structures exist on both the DOD and DIB sides, public-private partnerships for national defense should be reenergized. With the standing up of NSA's CSD, the government needs to clarify which organization is the coordinating entity to take the lead engaging and partnering with the defense sector in support of mitigating IP theft risks. Then, this entity and the NDISAC should serve as the anchoring organizations to support a more robust, better-resourced collaborative effort to cultivate the resilience of the DIB. This effort should contain three elements: first, an intelligence-sharing program across classification lines; second, development and routine exercising of playbooks; and third, predefined responses.

First, stakeholders across the DIB and the interagency, including the intelligence community (IC), should build on and expand existing classified and unclassified intelligence-sharing efforts to support getting ahead of a breach, rather than responding to and sharing information after the fact. This is particularly salient in the context of intellectual property theft because there is little that can be done to repair the damage from or mitigate the consequences associated with the loss of proprietary national security–related information, which likely took significant time and resources to develop, unless stolen data can be rapidly recovered and corrupted. Therefore, proactive and anticipatory intelligence as part of an early warning program is critical to ensure the long-term integrity of the U.S. national security innovation that resides within the DIB. This should entail developing systematic, holistic assessments of threat actors as strategic, learning organizations with tactics, techniques, and procedures (TTPs) that may evolve over time with clearly defined strategic objectives. Identifying the strategic objectives,

in particular, enables firms in the DIB to be proactive about network and infrastructure defense in expectation of future adversary behavior. Stakeholder development of objective, measurable, and observable indications and warning (I&W), some of which will stem from playbook development and exercises discussed below, can help confirm the strategic motivations of threat actors and trigger proactive defense postures. An ideal objective that would complement these proactive efforts would be to improve U.S. understanding of adversary intelligence collection requirements so that the United States can anticipate the areas they are likely to target within the DIB.

Second, stakeholders should develop and routinely exercise playbooks that stipulate roles and responsibilities in times of crisis and that are built around scenarios about likely adversary information/intelligence requirements. Playbooks should sync response efforts across the interagency to coordinate potential policy options taken by various departments and agencies, such as the Departments of Justice, State, Homeland Security, and Defense. The outcomes of playbooks and exercises should drive decision making about the emplacement of defensive and early warning assets and refine collaborative intelligence collection and analysis. Playbooks should also explicitly recommend policy options for appropriate measures that consider the compressed time frame associated with responding before the adversary can capitalize on stolen property. Playbook development and exercising creates shared expectations about and credibility for different responses at various thresholds.

Finally, for cost generation to be an effective instrument for rewriting the status quo, offensive cyber responses taken by the IC or DOD should not necessarily be limited to adversary behavior that inflicts destructive or disruptive effects on network and system functioning but, rather, should also include, when appropriate, offensive cyber responses to the theft of the national-security IP. Cyber operations in adversary or non-U.S. cyberspace to corrupt or degrade stolen national security information and the infrastructure and capabilities employed to acquire it could be conducted by the Cyber National Mission Force using Title 10 authorities or by intelligence agencies using Title 50 authorities.[37] These operations serve a dual function of covert or overt signaling and degrading adversary capabilities.[38] Therefore, DOD in conjunction with select agencies within the IC should establish countermeasure deployment criteria and corresponding rules of engagement to address adversary theft of DIB IP.

One unique aspect of this problem set is that proactive deception efforts based on the principles of military deception can be effective to force adversaries to reveal themselves, expend valuable resources pursuing false targets, and sow confusion and uncertainty about the integrity or authenticity of any purloined property. There are unique authorities across the interagency that could support the equivalent of military deception in "blue space" (U.S. cyberspace), where, while there are strict limits to

DOD's ability to operate, the Department of Homeland Security (DHS), the intelligence community, and law enforcement agencies (to include the Air Force Office of Special Investigations) have greater purview.[39] Examples of these include but are not limited to emulating networks, planting false or harmful information, beaconing capabilities, and using logic bombs and honeypots.

Defending U.S. Critical Infrastructure and Key Resources

In addition to protecting the defense sector, another vital challenge for the United States in a context of great-power competition in cyberspace is establishing public-private collaboration to defend CIKR from cyber attacks or adversary campaigns that could cause catastrophic economic or national security effects. Below, we propose a program to better enable U.S. critical infrastructure to be resilient to a cyber campaign of strategic consequence. A significant impediment to public-private collaboration is the reified silos that separate critical infrastructure sectors from the federal government and one another. This is in contrast to the inherently shared environment in which DOD and DIB are already cooperating. Overcoming these barriers is imperative to promoting critical infrastructure cyber resilience, because all stakeholders operate in a shared threat environment.

While the notion of distinguishing between civilian and military targets has a long-standing history in international humanitarian law and the law of armed conflict, this distinction has not held in practice in cyberspace.[40] State actors engage in offensive, espionage, and influence operations to target adversarial governments, military organizations, economies, and societies alike. In many cases, the same threat actor groups will conduct operations across a diverse range of targets—even as they may employ the same TTPs. For instance, APT 28 (a.k.a. Fancy Bear), to whom CrowdStrike first publicly attributed responsibility for hacking the Democratic National Committee e-mails in the lead-up to the 2016 U.S. presidential election as part of Russia's influence campaign, is also reportedly conducting traditional cyber-enabled espionage operations against a range of Western governments.[41] Similarly, in 2016 the U.S. Department of Justice indicted seven individuals associated with the Islamic Revolutionary Guard Corps who participated in both the sustained distributed denial-of-service attacks against the U.S. financial services sector from 2011 to 2013 and the cyber intrusion of a dam in Westchester County, New York.[42] The reality is that governmental and private actors routinely confront shared adversaries and threats in cyberspace. However, both of these entities lack a common picture of the threat environment because information is siloed in several respects: across classification lines; across agencies; between the government and the private sector; and across different sectors of the economy.

There have been important efforts to enhance information sharing to surmount these barriers. For example, the Cyber and Infrastructure Security Agency (CISA) within DHS promotes information sharing across the interagency and the private sector through distributing unclassified and classified information to enable network defense, including indicators of compromise, malware signatures, emerging TTPs, and some analytic products. The U.S. Computer Emergency Readiness Team (CERT) operates under the auspices of DHS and serves an information-sharing function, but there are several other U.S.-operated CERTs that are maintained outside the official auspices of the federal government even as they partner with it.[43] DHS has also initiated an expedited process for granting security clearances to specific private citizens who serve in key roles within U.S. critical infrastructure, but the implementation of this program has been slow. The private sector has also organized itself around several information-sharing and public-private partnership entities, such as Information Sharing and Analysis Centers, Sector Coordinating Councils, and Information Sharing and Analysis Organizations. Finally, the U.S. government has pioneered Pathfinder initiatives to move beyond information sharing to collaborate more actively with critical infrastructure asset owners and operators.[44] This program, which began as a pilot program, Project Indigo, in 2017 initially focused on the financial services sector, has since expanded to other sectors, including energy and communications (collectively known as "tri-sector" or "lifeline sectors").[45]

However, while these initiatives serve an important function, they remain limited to focusing on aiding reactive, defensive postures to respond to and block recognized activity after it has already occurred. The origins of this approach may derive in part from the language used in section 9 of the Obama administration's February 2013 Executive Order 13636, which directs the secretary of DHS to "identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security."[46] The July 2016 Presidential Policy Directive 41, which defines coordination across the interagency for significant cyber events, similarly uses "cyber incident" as the unit of analysis.[47] The key criterion for federal government efforts to address cyber threats to the private sector, therefore, is whether a given event constitutes a cyber incident that crosses some threshold of severity. However, this approach is problematic for two reasons. First, it is nearly impossible to anticipate the severity of a single cyber incident before it has occurred, which by default forces the government into responding to events only after they have reached a particular level of harm. Second, a single cyber incident considered in isolation may not cross any significant threshold, but may become enormously significant when considered as part of a long-term adversary

campaign. Focusing on addressing individual cyber incidents, therefore, risks missing strategically important adversary behavior.

Indeed, similarly to existing information-sharing efforts between the DIB and DOD, information-sharing programs between the government and critical infrastructure sectors are not focused on assessing adversaries as strategic threat actors with organized campaign plans and dynamic capabilities that may encompass a range of targets. The extant focus on reactive information sharing fails to address the challenge of anticipating the adversary, both in the immediate time horizon and over the long term, to better position asset owners and operators to defend their networks and critical systems. Rather than taking the long view, U.S. CIKR defenders are confined to a constant churn of reacting.

As a first step toward remedying these deficits, the U.S. government should support and resource a more systematic and proactive collaborative program with U.S. critical infrastructure entities that support critical economic and national security missions and functions, currently designated section 9 firms, as outlined in Executive Order 13636.[48] Implementation would require establishing systematic and transparent criteria, which are currently opaque, for designating firms as section 9. Moreover, section 9 criteria should enable the expansion of the current list of section 9 firms if necessary as well as procedures for dynamically reassessing the list of section 9 firms, as well as criteria, over time. Additionally, it would be better supported by reorganizing some offices and units in the CISA and U.S. Cyber Command around critical infrastructure sectors rather than adversaries to foster the cultivation of sector-specific knowledge across the interagency. However, there are also limits to the section 9 concept. Defining individual firms and sectors as the discrete entities that warrant additional federal assistance may be an inadequate lens through which to view threats to U.S. critical infrastructure. Ultimately, what is of strategic significance is not a particular threat to a given firm or even sector but, rather, the critical functions and services that support the U.S. economic and daily life that may be put at risk. This does not mean that the federal government should scrap the entire section 9 framework, but there should be a parallel effort to identify core functions and the cross-sector interdependencies.

A program of public-private collaboration across U.S. critical infrastructure, similar to that for the DIB, should meet two core objectives to be successful: first, effective collaborative intelligence sharing to promote early warning; and second, routine sector and cross-sector playbook development, exercises, and collective defense efforts. First, similarly to protecting U.S. national security IP, early warning is crucial to a proactive approach to anticipating, thwarting, and mitigating the consequences of adversary offensive cyber actions. Some of the measures to support an early warning capability

within and across CIKR are comparable to those previously suggested: developing sector-specific I&W criteria in cooperation with all stakeholders that, if triggered, would signify a probable or imminent attack; aligning U.S. intelligence collection priorities around developed I&W frameworks; side-by-side and routine analytic collaboration on all data sets across multiple classification levels and sectors; and tracking threat actors as strategic, learning organizations that conduct organized campaigns across multiple sectors. However, unlike with the DIB, the infrastructure to support these efforts would have to be built from scratch for much of critical infrastructure, particularly with respect to shared work spaces and sensitive compartmented information facilities. Additional measures to enable early warning and the development of a shared picture of the threat environment could include voluntary placement of network sensors on externally facing network infrastructure in information and operational technology environments of identified critical infrastructure. The collected data would be shared in real time and anonymized through aggregation into a data lake. Moreover, investments in automated analysis tools, including artificial intelligence, that can be applied against collected data, as well as additional feeds from public and private sources for enrichment, would make processing such large amounts of data more efficient and effective.

Second, developing and exercising sector-specific and multisector playbooks involving all stakeholders should inform and augment collective defense of U.S. critical infrastructure in cyberspace. Collaborative intelligence-sharing efforts should inform and iteratively refine playbook scenario development, and exercising playbooks should feed back into enhancing intelligence collection within the IC against I&W. These playbooks should designate defined thresholds that, if breached, would indicate a catastrophic event, as well as drive efforts to measure and assess persistent and corrosive adversary campaigns that may unfold over time without a single, decisive event of significance. Furthermore, playbooks should guide the development of standing roles, responsibilities, and authorities that enable U.S. responsive actions at various thresholds using all levers of national power, including permitted private-sector responses. In particular, playbooks can inform scenarios in which U.S. Cyber Command would authorize the Cyber National Mission Force to conduct anticipatory offensive cyber operations in non-U.S. cyberspace to thwart impending attacks, on the basis of improved early warning, as part of defend forward. Playbooks should be routinely tested through tabletop exercises and war gaming involving all stakeholders, and lessons learned should be incorporated into a continuous process for playbook development.

International Efforts

The focus of our argument has been on improving collaborative efforts between the U.S. government and the private sector across the DIB and critical infrastructure. However,

given the interdependence of the global economic system and supply chain, adversary campaigns aimed at critical infrastructure or IP theft have important international dimensions. Measures intended to promote the resilience of U.S. CIKR, for instance, will inevitably be limited if they fail to consider the international dimension of threats, vulnerabilities, and interdependencies. The same is also true with respect to the global supply chain that feeds certain elements of the DIB. Therefore, in tandem with domestic efforts, the U.S. government should leverage international relationships to foster resilience further. These should include utilizing international information-sharing organizations and intelligence-sharing alliances (Five Eyes, SIGINT Seniors Europe, and bilateral intelligence agreements) to foster a common understanding of the threat environment to include intelligence estimates of threat actor campaigns, strategic objectives, and trends over time. The U.S. government should also enhance alliance-based initiatives for coordination to pursue and admonish malicious behavior in cyberspace through international diplomatic, legal, and economic means. An example of this is the coordinated efforts by the United States and its allies in 2018 to attribute the NotPetya cyber attacks to Russia.[49] Finally, despite challenges associated with developing international norms of behavior for cyberspace and recent rifts in international organizations on these issue areas, the United States should work with its transatlantic alliance partners to continue to play leadership roles in international forums, such as the United Nations Group of Governmental Experts and Organization for Security and Co-operation in Europe, and not cede leadership within these venues to actors with whom the United States and like-minded nations do not share common values.[50]

Potential Impediments

There are several potential impediments to implementing this proposal, but all can be remedied through various measures. First, critical infrastructure and DIB firms lack market incentives to prioritize resilience over investments in immediate, day-to-day network defense and threat intelligence. Devoting limited cybersecurity resources to resilience requires trade-offs and may decrease efficiency. However, this could be addressed through creating market incentives for resilience investments, such as subsidies or tax incentives for sharing threat information and routine collaboration. Additionally, the Cybersecurity Information Sharing Act's liability protections, which protect entities that share indicators and defensive information with one another or the U.S. government, could be expanded to apply more broadly to information sharing between the private sector and the interagency.[51] Second, as already noted above, unlike the case with the DIB, there are substantial impediments to information sharing between the government and critical infrastructure owners and operators across classification lines. While a DHS-led Private Sector Clearance Program exists, it operates at a glacial pace and is not perceived

within the private sector to be a viable avenue for processing security clearances for appropriate individuals within section 9 firms. The president should direct the DHS secretary to prioritize and appropriately resource this effort. At the same time, reassessing classification protocols so that meaningful and useful information, particularly associated with providing context rather than more exquisite information about sources and methods, is a priori pushed down to lower classification levels would address this gap. Finally, public-private collaboration will likely be hampered by interagency infighting over roles and responsibilities and slow government responses during times of crisis. The playbook development process for the DIB and critical infrastructure should alleviate some of these issues through eliciting buy-in *ex ante* about roles and responsibilities. Furthermore, it should also drive the development of standing rules of engagement and preapproved campaign plans to support planning for, developing capabilities against, and responding to exigent threats, which will improve government response time.

Conclusion

By definition, any effort by a great power to change the status quo will be costly and incur greater risks of adversary retaliation, potential escalation, and miscalculations and misperceptions. The United States does not typically consider itself to be a revisionist state actor, but the reality is that the status quo in cyberspace is unacceptable to the United States and, left unchecked, will lead to the continued erosion of the relative U.S. power advantage across all instruments of power. Therefore, the United States must accept that to develop a global cyber system that reflects its interests and values it must be willing to incur some risks and absorb some costs. However, implementing the recommendations in our proposal to enhance the United States as a ready, resilient platform across critical infrastructure and the defense industrial base will enable the United States writ large to better absorb and recover from adversary behavior and help reshape the status quo to protect its interests and values in cyberspace.

Notes

The views of the authors are personal and do not reflect the policy or position of any U.S. government agency or organization or of PricewaterhouseCoopers.

1. Debates about emerging multipolarity or the durability of the U.S. position in the international system trace their roots to the end of the Cold War. See, for example, Robert O. Keohane, *After Hegemony: Cooperation and Discord in the World Political Economy* (Princeton, NJ: Princeton Univ. Press, 2005), or Charles Krauthammer, "The Unipolar Moment," *Foreign Affairs* 70, no. 1 (1990).
2. "SIPRI Military Expenditure Database," *Stockholm International Peace Research Institute,* https://www.sipri.org/databases/milex, accessed 7 April 2020; U.S. Department of Defense [hereafter DOD], *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2018*

(Washington, DC: Office of the Secretary of Defense, 16 May 2018); Joshua R. Itzkowitz Shifrinson, *Rising Titans, Falling Giants: How Great Powers Exploit Power Shifts* (Ithaca, NY: Cornell Univ. Press, 2018); David M. Edelstein, *Over the Horizon: Time, Uncertainty, and the Rise of Great Powers* (Ithaca, NY: Cornell Univ. Press, 2017); Matthew Kroenig, *The Logic of American Nuclear Strategy: Why Strategic Superiority Matters* (Oxford, U.K.: Oxford Univ. Press, 2018); U.S. House, *Russian Nuclear Forces and Prospects for Arms Control,* testimony of Austin Long, RAND Corporation, before the House of Representatives Committee on Foreign Affairs, Subcommittee on Terrorism, Nonproliferation, and Trade, 115th Cong., Washington, DC, 2018, https://www.rand.org/.

3. DOD, *Nuclear Posture Review 2018* (Washington, DC, February 2018).
4. *National Security Strategy of the United States of America* (Washington, DC: White House, December 2017), pp. 27–28, www.whitehouse.gov/.
5. DOD, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Washington, DC, 2018), p. 2, https://dod.defense.gov/.
6. In this chapter, we focus on the latter two challenges. Countering adversary cyber-enabled influence campaigns is also a vital element of succeeding in great-power competition, but for the purposes of this discussion we address IP theft and threats to U.S. CIKR.
7. DOD, *Summary Department of Defense Cyber Strategy 2018* (Washington, DC, 2018), p. 1.
8. Ibid., p. 5.
9. Ibid., pp. 2–3. Of course, the DIB does not comprise the full scope of the entities that support national security innovation but is an important and large component of it.
10. "Defense Industrial Base Sector," *Department of Homeland Security,* https://www.dhs.gov/.
11. DOD, *Strategy for Defense Critical Infrastructure* (Washington, DC, March 2008), p. 4.
12. See Andrea Gilli and Mauro Gilli for a critique of this argument. Andrea Gilli and Mauro Gilli, "Why China Has Not Caught Up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage," *International Security* 43, no. 3 (Winter 2018/19), pp. 141–89. However, the immense efforts competitors such as China have devoted to widespread IP theft suggest that U.S. adversaries do indeed perceive these endeavors to offer immense value.
13. Chris Bing, "Inside 'Project Indigo,' the Quiet Info-Sharing Program between Banks and U.S. Cyber Command," *CyberScoop,* 21 May 2018, https://www.cyberscoop.com/; U.S. Senate, *Statement of General Paul M. Nakasone, Commander, United States Cyber Command before the Senate Committee on Armed Services,* 116th Cong., Washington, DC, 2019, p. 10, https://www.armed-services.senate.gov/.
14. See Erica D. Borghard, "Protecting Financial Institutions against Cyber Threats: A National Security Issue," *Carnegie Endowment for International Peace,* 24 September 2018, https://carnegieendowment.org/.
15. For a more extended discussion of resilience, see Chris C. Demchak, *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security* (Athens: Univ. of Georgia Press, 2011).
16. DOD, *Summary DOD Cyber Strategy 2018*.
17. Robert J. Art, "To What Ends Military Power?," *International Security* 4, no. 4 (Spring 1980), p. 6.
18. There are debates in the literature regarding the extent to which deterrence is possible in cyberspace and at what threshold. In this piece, we do not claim that cyber deterrence is not feasible; rather, we simply point out that it has not succeeded in the way the U.S. government has operationalized it for threats below the use-of-force threshold. For a further discussion of these issues, see, for example, Joseph S. Nye, "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (2017), pp. 44–71; Michael Fischerkeller and Richard Harknett, "Deterrence Is Not a Credible Strategy for Cyberspace," *Orbis* 61, no. 3 (2017), pp. 381–93; Robert Jervis, "Some Thoughts on Deterrence in the Cyber Era," *Journal of Information Warfare* 15, no. 2 (2016), pp. 66–73; Martin Libicki, *Cyberspace in Peace and War* (Annapolis, MD: Naval Institute Press, 2016); Aaron Brantly, "The Cyber Deterrence Problem," in *2018 10th International Conference on Cyber Conflict, CyCon X: Maximising Effects,* ed. T. Minárik, R. Jakschis, and L. Lindström (Tallinn, Est.: NATO CCD COE, 2018); Thomas Rid, *Cyber War Will Not Take Place* (Oxford, U.K.: Oxford Univ. Press, 2013); Jon R. Lindsay, "Tipping the Scales: The Attribution Problem and the

Feasibility of Deterrence against Cyberattack," *Journal of Cybersecurity* 1, no. 1 (2015), pp. 53–67; and Jacquelyn G. Schneider, "Cyber and Cross-Domain Deterrence: Deterring in and through Cyberspace," in *Cross-Domain Deterrence: Strategy in an Era of Complexity,* ed. Erik Gartzke and Jon R. Lindsay (Oxford, U.K.: Oxford Univ. Press, 2019).

19. U.S. Cyber Command's *Command Vision* prominently features the term "resiliency." However, missing from the vision is a full articulation of the concept of resilience and of its operationalization across different stakeholders. U.S. Cyber Command, *Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. Cyber Command* (Fort Meade, MD, June 2018).
20. "Persistent engagement" is how Cyber Command implements the DOD strategy of "defend forward."
21. Gary Brown and Keira Poellet, "The Customary International Law of Cyberspace," *Strategic Studies Quarterly* 6, no. 3 (Fall 2012), p. 133.
22. U.S. House, *Evolving the Cybersecurity Conversation before the Subcommittees on Information Technology and National Security of the House Committee on Oversight and Government Reform,* prepared statement of Gen. (Ret.) Keith B. Alexander, former Director, National Security Agency, and former Commander, USCYBERCOM, 114th Cong., Washington, DC, 2016.
23. Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009–2011* (Washington, DC: Office of the Director of National Intelligence, October 2011); Thom Shanker, "U.S. Report Accuses China and Russia of Internet Spying," *New York Times,* 3 November 2011.
24. David E. Sanger, David Barboza, and Nicole Perlroth, "China's Army Is Seen as Tied to Hacking against U.S.," *New York Times,* 18 February 2013; *APT1: Exposing One of China's Cyber Espionage Units* (Alexandria, VA: Mandiant, February 2013). China denied its involvement in these attacks, but the denial was less than credible given Chinese government control over its internet infrastructure; David Barboza, "China Says Army Is Not behind Attacks in Report," *New York Times,* 20 February 2013.
25. Thomas Donilon, "Complete Transcript: Thomas Donilon at Asia Society New York," *Asia Society,* 11 March 2013, https://asiasociety.org/.
26. Siobhan Gorman, "U.S. Eyes Pushback on China Hacking," *Wall Street Journal,* 22 April 2013.
27. United States of America v. Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, and Gu Chunhui, U.S. District Court, Western District of Pennsylvania, Docket Number: Criminal Number 14-118, filed: May 2014. Also see the official press release, U.S. Department of Justice, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage against U.S. Corporations and a Labor Organization for Commercial Advantage," press release, 19 May 2014.
28. White House, "Fact Sheet: President Xi Jinping's State Visit to the United States," fact sheet, 25 September 2015.
29. Department of Homeland Security, "First U.S.-China Law Enforcement and Cybersecurity Dialogue," press release, 6 October 2017.
30. Daniel R. Coats, *Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community* (Washington, DC: Director of National Intelligence, 6 March 2018), p. 6, https://www.dni.gov/; U.S. Trade Representative, *Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation under Section 301 of the Trade Act of 1974* (Washington, DC: White House, 22 March 2018).
31. Daniel R. Coats, *Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community* (Washington, DC: Office of the Director of National Intelligence, 29 January 2019), p. 15.
32. Gordon Lubold and Dustin Volz, "Navy, Industry Partners Are 'under Cyber Siege' by Chinese Hackers, Review Asserts," *Wall Street Journal,* 12 March 2019.
33. David J. Lynch and Anna Fifield, "Trump Says He Expects to Sign a Trade Deal with China 'Very Soon,'" *Washington Post,* 25 February 2019.
34. See Erica D. Borghard and Shawn W. Lonergan, "The Logic of Coercion in Cyberspace," *Security Studies* 26, no. 3 (May 2017), pp. 452–81, and Erica D. Borghard and Shawn W. Lonergan, "Confidence Building Measures for

the Cyber Domain," *Strategic Studies Quarterly* 12, no. 3 (Fall 2018), pp. 10–49.

35. The Office of the Under Secretary of Defense for Acquisition & Sustainment Cybersecurity Maturity Model Certification; see its website, https://www.acq.osd.mil/cmmc/.
36. "Strengthening the Front Line: NSA Launches New Cybersecurity Directorate," *NSA/CSS,* 1 October 2019, https://www.nsa.gov/; Mark Pomerleau, "New NSA Directorate to Focus on Industrial Base," *Fifth Domain,* 9 October 2019, https://www.fifthdomain.com/.
37. "Title 10 authorities" refers to military authorities, while "Title 50 authorities" refers to intelligence and covert-action authorities; see Andru E. Wall, "Demystifying the Title 10–Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action," *Harvard National Security Law Journal* 3, no. 1 (2011), pp. 85–142. Notably, the 2019 National Defense Authorization Act defined unattributed military cyber operations as a traditional military activity under Title 10, not requiring them to be defined as covert action under Title 50; see Robert Chesney, "The Law of Military Cyber Operations and the New NDAA," *Lawfare* (blog), 26 July 2018, https://www.lawfareblog.com/. Offensive cyber actions rightly remain within the scope of governmental, rather than private, authorities, because these are inherently military or intelligence capabilities that necessitate appropriate command and control and should be nested within U.S. strategic aims.
38. Signaling is typically thought of as occurring at the strategic level through formal (and often public) channels. However, covert signaling at the operational and tactical levels can be a useful way for actors to convey credibility, intent, and other such "messages" to adversaries; see, for example, Austin Carson and Keren Yarhi-Milo, "Covert Communication: The Intelligibility and Credibility of Signaling in Secret," *Security Studies* 26, no. 1 (2017), pp. 124–56. Because cyber operations in themselves are imperfect and costly tools of signaling, coupling cyber operations with other forms of signaling is particularly important for influencing the adversary's decision calculus.
39. U.S. Joint Chiefs of Staff, *Cyberspace Operations,* Joint Publication 3-12 (Washington, DC, 8 June 2018), p. I-4.
40. Indeed, international efforts to establish shared norms surrounding how and the extent to which international law applies in cyberspace have been manifestly unsuccessful. See Borghard and Lonergan, "Confidence Building Measures for the Cyber Domain," pp. 16–18, and Alex Grigsby, "The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased," *Net Politics,* 15 November 2018, https://www.cfr.org/.
41. "Who Is Fancy Bear?," *CrowdStrike,* 12 September 2016; "APT 28: New Espionage Operations Target Military and Government Organizations," *Symantec,* 4 October 2018.
42. U.S. Justice Dept., "Seven Iranians Working for Islamic Revolutionary Guard Corps–Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks against U.S. Financial Sector," press release, 24 March 2016.
43. CERT teams carry out responses to cybersecurity incidents. US-CERT operates under the auspices of the Department of Homeland Security, https://www.us-cert.gov/. There are other government-affiliated CERTs within the United States, supported typically through federally funded research and development centers; an example is the CERT Division at Carnegie Mellon University, https://www.sei.cmu.edu/about/divisions/cert.
44. *Statement of General Paul M. Nakasone,* 2019.
45. Bing, "Inside 'Project Indigo.'"
46. Exec. Order No. 13,636, 3 C.F.R. 217 (2013), https://www.govinfo.gov/content/pkg/CFR-2014-title3-vol1/pdf/CFR-2014-title3-vol1-eo13636.pdf.
47. *Presidential Policy Directive: United States Cyber Incident Coordination,* PPD-41 (Washington, DC: White House, 26 July 2016), https://obamawhitehouse.archives.gov/.
48. Executive Order 13636, section 9, identifies firms that play essential roles in the economy and against which significant cyber attacks would cause catastrophic economic or national security consequences. However, the implications of a section 9 designation, as well as the criteria that determine inclusion within section 9, need to be fleshed out more fully.
49. The State Department's Cyber Deterrence Initiative is engaged in some of these efforts, but couching these in the context of a more proactive "defend forward" effort rather than solely in support of deterrence outcomes

would be an important improvement. Derek Hawkins, "The Cybersecurity 202: U.S. and Allies Make Coordinated Push to 'Name and Shame' Russian Hackers," *Washington Post,* 5 October 2018.

50. For further discussion of confidence-building measures for cyberspace, see Borghard and Lonergan, "Confidence Building Measures for the Cyber Domain."

51. Cybersecurity Information Sharing Act of 2015 (Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, div. N, tit. I [2015], https://www.congress.gov/).

CHAPTER EIGHT

Joint Operations in Cyberspace
From Operational Unity to Shared Strategic Culture

VICE ADM. TIMOTHY J. WHITE, USN (RET.)

Jointness in conventional operations entails coordinating disparate and distinct entities toward a shared purpose. Jointness in cyberspace is an existential fact of operating in a domain defined by a shared technological ecosystem. The joint cyber force, composed of the individual services with their distinct organizational proclivities, needs to evolve to a truly shared cyber strategic culture where there is a fusion of purpose, capabilities, vulnerabilities, talent, terrain, and threats.

How the United States organizes itself around and conducts joint operations in cyberspace is fundamentally distinct from joint operations in the conventional sense. From a conventional perspective, "jointness" is an attribute that has to be externally imposed—indeed, it was done so via legislation in 1986 with the Goldwater-Nichols Act—rather than organically built or derived out of some shared attributes or common ecosystem. Conventional jointness entails coordinating disparate and distinct entities toward a shared purpose or assigned mission. Jointness in cyberspace, in contrast, is an existential fact of operating in the domain. In this sense, cyber jointness is an a priori condition that is defined by a shared technological ecosystem. It *precedes* any effort to construct a joint cyber environment—the organizations, decision-making processes, and capabilities required to comprehensively conduct operations anywhere, independent of spectrum and protocol, to include organizations across the interagency and the private sector.

In cyberspace, U.S. military organizations start from a position of inherent jointness. An implication of this is that anytime we attempt to impose or force external organizational controls or legacy constructs onto an ecosystem and environment that, together, already produce their own unique characteristics and dynamics, we are likely to diminish efficacy. An example of this is the attempt to conceptualize military cyberspace organizations via a wholesale appropriation of lexicon and doctrine developed for

kinetic or physical conflict. Such dynamics are poorly matched to the cyber domain and the reality of cyber operations. We should accommodate and account for the emergent behaviors of the cyber environment and ecosystem rather than inhibit them.

The convergence of cyber with information operations as well as kinetic operations in the multidomain battlespace is driving the U.S. military to meet and overcome this challenge through promoting jointness and interoperability across the entire force (broadly construed beyond cyber operators). The evolution of the joint force in cyberspace—the operational arm of which is the Cyber National Mission Force (CNMF)—has reflected this essential reality. Put simply, there are no Army bits, naval bytes, or Air Force protocols within the CNMF; there is no distinction between services in cyberspace in terms of operational capability, training, and utilization. This inherent jointness of the operational force is something that we should deliberately cultivate and strengthen because disintegration or segmentation in the current strategic environment of great-power competition is a sure path to failure.

Despite operating in an inherently shared technological ecosystem with common threats and challenges, the CNMF—the joint cyber force as composed of the individual services, each with its distinct organizational proclivities and perspectives—is still evolving toward a truly shared cyber strategic culture. Strategic culture involves the attitudes, beliefs, and norms regarding the use of force that are shared within a defined group. A cyber strategic culture, therefore, would encompass a common conception of the nature of strategic competition in cyberspace and the use of cyber capabilities to achieve political, informational, and military effects both below and above the use-of-force threshold. Moreover, as a nation—moving beyond the military realm—we have yet to develop a shared conception of the broader national mission in cyberspace or to envision how the collective "we" should orient ourselves around it when our civilian and economic assets and systems are persistently compromised and targeted outside of conflict. The blurred distinction between the civilian and military worlds in cyberspace means that any joint conception of cyber requires a shared vision that widens the military aperture to incorporate the nation itself as a ready, resilient *platform* from which the United States can project and sustain power.

The Cyber Ecosystem and the Joint Environment

Cyberspace by its nature imposes—even causes—jointness. As a global, man-made ecosystem of interconnected and interdependent networks of computers and supporting infrastructure, cyberspace is fundamentally distinct from the other domains of warfare. While the individual services are independent bodies, they nevertheless share the same dynamic cyber terrain, confront the same cyber threats, and face the

same cyber vulnerabilities. This shapes how the United States organizes the joint cyber force and how that joint force interacts. This interface in turn becomes the operational environment.

The individual services are organized around self-contained domains of warfare (land, sea, and aerospace), each with its distinguishable terrain. While the U.S. military may define cyberspace as a separate "domain" of warfare, in reality cyberspace links together and permeates all the other domains. In this sense, the definition of cyberspace in Joint Publication 3-12 as "dependent on the physical domains of air, land, maritime, and space" inverts the burden of dependence in the relationship between the cyber and physical domains.[1] In any contemporary contest between modern powers, conventional operations in the physical domains of warfare fundamentally depend on and are shaped by operations in cyberspace. In no other historical or contemporary instance of joint operations has this been the reality of the terrain ecosystem and operating environment. Cyberspace is a contested space in which actors continuously engage because of the condition of constant contact that derives from the interconnectedness of the cyberspace strategic environment. As such, cyberspace has become a key part of great-power competition. Any engagement with an adversary in any one domain of conflict will almost certainly be preceded by engagements in cyberspace or will be shortly followed by them. Cyber operations will be—and likely already are—an intrinsic component of conflict.

While cyberspace creates a *shared* playing field for the individual services, it also provides a more *level* playing field for our adversaries—but not for the reasons that are typically identified. We may be tempted to proclaim cyberspace to be a great disrupter or leveler when we enumerate the range of possible enemies in this domain and recognize that virtually any unsophisticated threat actor can conduct offensive operations at little to no cost. Cyberspace does indeed enable a proliferation of cheap and easy operations, but these are likely to be less impactful against a target and do not represent the strategically significant threats toward which the joint force should be oriented. Put simply, the distribution of offensive capabilities across relatively unskilled actors is important but is not what levels the playing field in cyberspace. Rather, cyberspace has already become a key arena for great-power competition where the United States confronts near-peer or even peer competitors who exploit the asymmetric nature of cyber operations, hold us at risk owing to our military and civilian dependence on information technology, and engage in widespread theft of intellectual and national security information to use against us in strategic competition across all elements of national power.

Great-power competition in cyberspace finds the United States saddled with norms and frameworks of conventional or nuclear great-power competition in its approach to this new type of contest. During the Cold War, the United States and Soviet Union competed below the use-of-force threshold but were never in direct conflict in large part owing

to the looming fear of a devastating nuclear confrontation. Today, the United States contests its adversaries in cyberspace below the use of force, but our cyber forces are nevertheless *directly* engaging the adversary (and vice versa) on a persistent basis. We are only beginning, however, to develop strategic and operational frameworks to guide our approach to this type of conflict. One fear is that failure to craft such frameworks will allow further erosion of U.S. advantages in the other domains, thus accelerating a shift in the systemic balance of power away from the United States.[2]

Employing offensive cyber capability to generate strategic effects against an adversary and sustaining protection, defense, and maneuver effects over time is complicated, challenging, and unpredictable. This is why only state actors and their proxies have thus far mounted strategic cyber campaigns of significant consequence.[3] Put simply, states can make time their ally.

On the one hand, time moves slowly in offensive cyber operations. Intelligence and operational preparation of the environment for the purposes of delivering effects against strategic targets, such as critical infrastructure or hardened military targets, takes time. This includes time required to gain access to customized target sets, to develop precise capabilities tailored to those targets, and to retain continuous access to be ready to employ one's capability at the desired time. Many capabilities and accesses are not modular; developed for one target set, they often cannot be applied to a different one during a fast-moving campaign or crisis.

On the other hand, time moves quickly. At the tactical level, effects can be delivered rapidly with minimal warning if an attacker's presence on a network remains obfuscated until the moment of attack. Cyber terrain may change rapidly and unpredictably as a target (perhaps even unwittingly) patches a vulnerability or makes some other modification that negates an access or capability. Furthermore, some types of offensive operations are access independent and do not require the same time or resources to prepare the environment. Examples of these include cyber-enabled information operations and large-scale distributed denial-of-service attacks that, employed as part of a broader adversary strategy, could achieve significant effects.

Finally, the strategic and geopolitical operating environments may demand rapid responsiveness that requires the joint cyber force to go to battle with solely the accesses and capabilities on hand—which may be mismatched to those that would better support one's desired objectives. Thus, time moves at once slowly and extremely quickly in the context of the pace of full-spectrum cyber operations. Hence, there is an enormous potential for things not to take root, or for capabilities that were resource- and time-intensive to be effectively impotent or incompatible with strategic objectives and campaign maneuver at the time of employment.

Therefore, the challenges facing the joint cyber force are conceptualizing, organizing, resourcing, training, and equipping execution of strategically significant cyber campaigns. These should include countering sophisticated cyber campaigns that target critical American infrastructure and key resources across the public and private sectors, as well as the persistent and large-scale theft of intellectual property via cyber means that is eroding America's strategic advantage. We must also restore confidence in the information technology on which our military capabilities depend, and neutralize adversary campaigns that sow popular distrust of American institutions and thus diminish our democracy from within.

Implications for the CNMF

CNMF forces are both distinctly and purposefully joint. "Joint" in cyberspace is something more nuanced and altogether complete. This departs from the concept of jointness as a product of Goldwater-Nichols, which for conventional forces has come to mean something doable by a combination of services in functionally aligned groups to operate in common areas toward agreed—or stated—common outcomes. In conventional space, you have to work to get joint, to be joint, and to do joint. In cyberspace, you are already joint; you have to work to be better—to be *unified*. "Joint" in conventional terms means that we coordinate disparate and separate entities to achieve a shared objective. In the cyber realm, we are moving beyond "joint" to "singular," where there is a fusion of purpose, capabilities, vulnerabilities, talent, terrain, and threats, ideally leading to a shared epistemology.

During our time leading the CNMF this was both accommodating and liberating. Once we, the CNMF, accepted we were joint, we began to expect of ourselves joint outcomes. We, in effect, unleashed joint. In all our collective time in previous assignments, both joint and command, this was the first time that we moved beyond joint and approached singular. We truly moved from many to one. We were unchained, unencumbered, and empowered to think, learn, and do. For our military personnel, the best part was that we did not know one another by our formally designated operational specialties. Instead, we knew one another by functions, roles, and purposes. We assessed one another not according to rank or seniority, but by apprentice, journeyman, senior, and master levels of proficiency—you were assessed on your merits, not your tenure. Moreover, within the CNMF, we cultivated jointness across civilian and military lines such that the distinction between civilian and uniform began to blur. At the same time, perhaps counterintuitively, the distinction between "government" (in terms of inherently governmental responsibilities and functions) and "not government" (or private sector) roles grew stark. We grew into a clearer understanding of the roles and responsibilities of government and the private sector within our shared mission space as we pursued

joint, collaborative efforts to defend U.S. critical infrastructure. When called on to support a broader government operation in 2017, the purely functional and blended teams the CNMF mustered included officers and enlisted personnel from across the services as well as civilians. Because we were organized into joint task forces already, these teams came together rapidly and effortlessly and were organized by function, role, and purpose.

This inherently joint ecosystem gives rise to several implications. First, we in the CNMF built common organizational structures on top of and in alignment with core missions, functions, and tasks. Our organizational environment and technological ecosystem, therefore, are becoming phase matched (in terms of aligning inputs and outputs and reducing transaction costs to promote efficiency and accelerate decision-making speed) to common causes such as policy, authority, TTPs (tactics, techniques, and procedures), and targeting processes. This work continues—as the CNMF works to reset how we define mission elements on the basis of our requirements and improve the process through which we send demand signals back to the services for personnel, training, and equipment to support the CNMF's defend-the-nation mission.

Second, the shared fact of our terrain and our vulnerabilities means that the adversary could theoretically contest us anywhere or everywhere. We must accept that we share exposed and protected flanks. In cyberspace, offense and defense converge at the tactical and operational levels. Therefore, the joint force must think in terms of scope and scale, and approach our vulnerabilities—our wide front and the potentially deep reach of adversary capabilities—from a unified perspective. The coexisting simultaneity of persistent and transient offense and defense means that our orientation toward the adversary and the domestic assets, systems, and networks we are tasked with defending cannot be siloed by service. Rather, we must jointly position our forces to detect and counter our adversaries through area reconnaissance, focused surveillance, and precise targeting as a unified response that occurs seamlessly across all organizations (environment) and event horizons (ecosystem). A critical deficiency in matching existing authorities to our shared terrain is that we lack common authorizations across services to operate on the Department of Defense's information network; the network is artificially service partitioned and access granted is service sanctioned. *There is only one network.*

Third, the services must be able to provide a common functionality when operating together as part of the joint cyber force. Part of that must come from a dedicated, joint effort to manufacture, assemble, and design our features (and to do so domestically to the greatest extent possible to reduce exposure to risk through supply chain vulnerabilities). An additional, essential component of common functionality is mobilizing and aligning to avoid talent fratricide in recruitment and retention while, at the same time,

ensuring optimization in both missioning and positioning. This also necessitates some commonality across service-based training and education.

Fourth, we are rarely ever a garrison force. There is no sanctuary or secure bastion. The adversary is contesting us below the use-of-force threshold. Thus, whether defending forward or supporting other agencies or state and local authorities, the joint force will always be engaged in the cyber fight. This means that we must be capable of persistently holding adversary strategic targets at risk while concurrently defending against a relentless and intrusive set of adversaries. This is the fundamental nature of great-power competition in cyberspace. Of course, competition does not always escalate to outright conflict, and the empirical record to date suggests that cyber is not inherently escalatory. Nonetheless, the joint force is continuously engaged in a multidomain contest and must be prepared to prevail in battles that loom on the horizon. In Thomas Schelling's sense, we have already "waded into the water"; the very nature of the combined ecosystem and environment means that we are already committed to action and are actively contesting our adversaries for an advantageous position in the domain.[4]

Fifth, there is no "readiness" or "rest and recuperate" cycle—there is only doing. Given this reality, we need to be more thoughtful and systematic about how we organize, resource, and enable a constantly engaged, joint fighting force to achieve decisive results, while also ensuring the freedom to regroup and continually learn in an environment where the technology is rapidly changing. In the conventional domains, learning typically occurs in the wake of conflict, in the pauses between wars that give breathing space to reassess, reflect, and innovate. But in cyberspace, we need to learn, adapt, and proliferate that knowledge to the force while being constantly engaged. Equally important, we must address attrition and mental health issues of the force that are products of the current operational tempo.

Sixth, in our space we exist with and must adapt to an unparalleled dynamism. While the adversaries themselves remain constant, the threat-actor groups, subgroups, or proxies that the former employ vary, shift, and mutate over time. These manifold actors are also characterized by a diversity of organizational structures, TTPs, personnel, and force employment strategies. The technology changes even faster with the unremitting introduction of new strains of malware and attack vectors and the discovery of new vulnerabilities. That is a real synergy of churn that is not experienced in conventional contexts. The distinctions between yesterday, here and now, and tomorrow are oblique. They move too fluidly and too rapidly to be binned and bound. That is why joint matters—herein lies the potential to meet, pace, and win the competition. The joint force can marshal mass and rapidly align against emerging threats. But this requires promoting a culture within the joint force that emphasizes operators and developers working in

tandem to build capabilities that take into account operational needs, rapid production within an intelligence-operations-development cycle, and deployability.

Finally, this dynamism engenders a greater urgency to sustain our alliances. In the context of what can sometimes feel akin to constant revolution, we must ensure there are some constants on which we can rely. As the threat actors and technologies change, our international allies and partners with whom we share common values and have forged deep historical and institutional ties are integral to the success of the joint force in cyberspace. In fact, it is the joint force—rather than any individual service—that is best positioned to build and sustain capabilities across our international allies and partners. Our alliances have always been a key source of our comparative advantage in great-power competition, and we cannot afford to imperil these relationships for the contemporary competition. For instance, we have treated offensive cyber operations as we do nuclear weapons—as exquisite and overwhelming sensitive capabilities. But we cannot be so secretive that it hinders our ability to operate with our alliance partners. Because cyberspace is not contained by any one area of operations defined by geography or political sovereignty, operational contingency planning and intelligence sharing around common adversaries must become multinational. This would contribute to a more holistic view of the adversary and allow us to find new ways to counter threats through not only gaining new accesses but also coordinating responses. Great-power competition is international in scope and therefore must be confronted through coalitions.

The Challenges Ahead

Despite the inherent jointness that characterizes the CNMF, there is a range of challenges posed by cyberspace operations and security that remain misunderstood or insufficiently prioritized but that require decisive efforts to address.

In the CNMF, as in any joint unit, there is a tension between the "administrative control" (ADCON) and "operational control" commands. An individual service member is charged with executing a mission for the National Security Agency / Cyber Command but may report to a service commander who has neither an operational responsibility nor insight but is nonetheless responsible for the former's rating. Inevitably, those ADCON commanders want to "command," and this can come at the expense of the mission as we are forced to pull service members away from operational tasks to instead conduct service-related activities (e.g., unit training, bake sales, potlucks, unit runs, etc.). Put simply, because ADCON commanders do not have any operational responsibility other than being a force provider, they often create requirements at the expense of the mission. This is a systemic problem that can undermine morale and, over the long term, negatively impact retention.

Further, services provide to the CNMF "trained" personnel by work role. From the services mind-set, such personnel are indeed provided "trained." However, given changes in the ecosystem, adversary TTPs, and the unique capabilities we employ, we must spend an average of one year for additional training for what is only a two- or three-year assignment. The services' view is that the CNMF must update work roles, but that process is neither sufficiently agile nor responsive to the changing nature of capabilities and our unique requirements versus those of the services. Compounding this issue, the services maintain their own training pipelines and do not have common schoolhouses. Though there has been an increasingly common-core curriculum, its contents are determined by that which can be agreed to by all of the relevant veto players. This means that any common curriculum may not meet the demands required to support a national mission versus a service-specific one, and the pace of curricular development and approval often comes at the expense of agility.

Moreover, even if the CNMF is equal to the combination of Fleet Cyber Command / Tenth Fleet, Army Cyber Command, Sixteenth Air Force (Air Forces Cyber), Marine Corps Forces Cyber Command, and Coast Guard Cyber Command, there is still a critical interoperability problem. Friction is introduced because the CNMF currently relies on certain types of capabilities and service-developed tools that do not interoperate with joint mission task elements in the CNMF comprising members from across the services. For instance, an Army-fielded cyber protection team capability cannot be integrated with a Navy-developed cyber protection team capability, and each requires its own training to operate. This means that a commander cannot assemble the most skilled and efficient mission task element without taking into consideration organizational (environment) and technological (ecosystem) constraints.

In addition, there is no common recognition across the joint force regarding appropriate staffing. The services are oriented toward domain-centric competencies and conflict. For instance, Army Cyber Command and Fleet Cyber Command / Tenth Fleet are both three-star commands. These outrank the two-star CNMF commander, who nevertheless possesses the preponderance of Cyber Mission Force teams and the national-level mission. Unity of command is imperative to achieve a national strategy for cyberspace, and the joint force led by the CNMF commander can and should play a larger role in this effort. This is especially critical to ensure that the use of cyber power is in sync with national-level objectives such that the United States can defend forward in defining a favorable status quo in the global system.

Toward a Cyber Strategic Culture

The CNMF is a joint force, but it not yet a singular one; it must become one. The culture is not a shared cyber strategic culture that transcends those of the individual services

and that inheres institutionally in the CNMF. However, there is an emergent shared culture and thoughtfully cultivating it remains a key opportunity for the future. All the designers and practitioners (the operators and maintainers; the planners and developers; the analysts and builders) already inhabit the same headspace. This is a step beyond William Gibson's conception of cyberspace in *Burning Chrome,* which he proposed as something shared, common, and pervasive.[5] Rather, it is more akin to Robert Heinlein's term, "grok," in *Stranger in a Strange Land,* which is something that is intuitively understood.[6] Intuited is more intrinsic, more comprehensive, and more complete. That is how we bridge sprawling, diverse, and yet interconnected technologies with commonly understood organization and aligned missions, functions, and tasks. That is the promise of cyberspace: a joint warrior operating in a joint environment in a joint force to achieve a joint force commander's objective within and across a joint ecosystem.

Nevertheless, we do need actively to support a common identity and culture. Each service has its own strategic culture that it brings to the joint cyber fight. Out of this patchwork of different service cultures, we need to create a new cyber strategic culture that exists both within the joint cyber community and across the leaders within the services. Of what should that shared culture or identity be composed?

- First, it must be skills and purpose based, rather than rank- or unit-centric. The convolution and difficulty of the problem set in cyberspace mean that we cannot unthinkingly default to always prioritizing rank, hierarchy, and authority over demonstrated ability and innovation. We have to accept some risk in flattening our organizational mentality so that we can harness our creative potential to stay ahead of the adversary. This will pose a challenge, because when the CNMF, as part of a combatant command, interacts with higher headquarters or partners the latter will expect a rank-based, unit-centric, traditional structure.
- Second, our identity should be both externally (adversary) and internally (defend the nation) oriented. These two facts of the cyber challenge are inseparable in a way that is simply not true of other domains. We cannot orient toward the adversary without also orienting toward the homeland. This is because we cannot defend what we do not know or understand. The domestic environment and ecosystem, therefore, fundamentally shape counteradversary actions in gray and red spaces.
- Third, our culture must be outcomes driven; we cannot venerate process over deliverables. To achieve this, we need a workforce that is empowered to deliver directed outcomes. We also need standing rules of engagement (ROE) that define and delineate how capabilities can be employed to support the mission in an area of operations, and that support civilian oversight and aligning Cyber Command with national-level objectives. Standing ROE would not only support capability

development and rapid response but also enable long-term planning and better military decision making.

- Finally, we must have a shared language and conceptualization of operating in the domain. Integral to achieving the promise of a more intuited sense of cyberspace, a shared cyber strategic culture, is a common framework to describe this shared space and mission and drive planning and decision making around it. This absence exacerbates the tensions that already exist across the different services, and between the joint commander and service commanders, regarding potentially competing strategic frameworks and priorities and mechanisms for reconciling them.

A Call to (a) Separate Service

Why not a separate Cyber Service? In many respects, an independent service would indeed address the challenges and concerns raised in this paper. For instance, it would institutionalize a cyber strategic culture that would be reinforced and inculcated through common education and training. It would also enable recruitment and talent management of individuals based on skills and experience directly pertinent to the cyber challenge, who may not necessarily conform to requirements and expectations of the other services. This would enable the United States to grow the force while pursuing talent management initiatives, to include a broadened role for civilians.

However, we are not (yet) at a point where the benefits of *another* service would compensate for the costs. At this juncture, the move toward a separate service would be apt to undermine jointness, rather than enhance it. A separate Cyber Service would likely be less responsive to the priorities of the other services. At the same time, even after the hypothetical creation of a Cyber Service, the other services would nevertheless continue to require their own indigenous cyber force structures. When the Air Force separated from the Army, for instance, the Army retained air defense capabilities and some airlift and close air support that it perceived to be integral to achieving land warfare outcomes at the tactical level, leaving the Air Force to prioritize investment in strategic capabilities initially. A separate Cyber Service would necessitate a determination about what capabilities should remain organic to each service and what the specialization of the independent Cyber Service would be.

Further, we can study history and observe that change is hard, acceptance is harder, and effectiveness is hardest. We have plenty of work to do now in ensuring that DOD's service culture and constituency take seamlessly integrated, full-spectrum cyberspace operations as seriously as they do ground maneuver, driving ships, strike, sustainment, and so on. DOD is more "joint" now than yesterday or yesteryear. However, we can still do more and better to integrate cyber with and into maneuver warfare doctrine, "fires" disciplines, and operational design.

We may need a separate Cyber Service if we find ourselves unable to overcome institutional and cultural impediments to addressing the implications and challenges outlined in this paper and, more significantly, if there is a pivotal moment or event that reveals our current force is unable sufficiently to defend the nation in, through, and from cyberspace against strategic threats. If this moment of reckoning does occur, it will hopefully be in the wake of victory and not defeat.

Posturing to Defend the Nation

The core mission of the CNMF is to defend the nation against strategic threats in cyberspace by defending forward to disrupt, degrade, or defeat adversary capabilities before they damage the United States and its interests. The scope of what must be defended in cyberspace distinguishes neither between services, nor between civilian and governmental assets. Therefore, how we approach the joint fight must extend beyond the military sphere to reflect the national scope and scale of the mission. A singularly joint force, therefore, must include all stakeholders from across the intelligence community and the federal government and, crucially, the critical infrastructure asset owners in the private sector who are essential for the successful defense of the nation. This does not imply that the latter should be "militarized" from an organizational or cultural perspective. Rather, we—all the stakeholders—must together accept that we are fighting jointly to defend the nation from strategic actors who seek to undermine our economic power, political legitimacy, and national security.

Notes

1. U.S. Joint Chiefs of Staff, *Cyberspace Operations,* Joint Publication 3-12 (Washington, DC, 8 June 2018), p. vii.
2. This is compounded by market trends shifting manufacturing and fabrication of information technology and operational technology to low-cost locations, including such competitors as China.
3. However, there is a risk that over time the barriers to entry could lower (particularly given the relatively low transaction costs of offensive cyber operations and free-market dynamics that characterize the environment in which capabilities are procured, as well as technological developments such as artificial intelligence). This may create the conditions that enable nonstate actors to pursue more-sophisticated cyber campaigns, thus injecting a new dynamic into great-power competition in cyberspace that may further confound the U.S. strategic position.
4. Thomas C. Schelling, *Arms and Influence* (New Haven, CT: Yale Univ. Press, 1966), pp. 66–67.
5. William Gibson, "Burning Chrome," *Omni,* July 1982.
6. Robert Heinlein, *Stranger in a Strange Land* (New York: G. P. Putnam, 1961).

CHAPTER NINE

Cyber Strategy, Talent, and Great-Power Competition

JACQUELYN G. SCHNEIDER

Central to the success of both the 2018 National Cyber Strategy *and the 2018* Department of Defense Cyber Strategy *is the need to recruit, retain, and utilize a talented workforce. This chapter tackles the cyber talent problem identified in the two 2018 strategies. It provides historical context to the importance of human capital in warfare, discusses why cyber talent is particularly important to modern conflict, identifies challenges in recruiting, retaining, and using talent in cyberspace for DOD, provides a rough overlay of many existing talent initiatives, and concludes with recommendations for tackling the talent challenge identified in both cyber strategies.*

Central to the success of both the 2018 *National Cyber Strategy* and the 2018 *Department of Defense Cyber Strategy* is the need to recruit, retain, and utilize a talented workforce. The *National Cyber Strategy* calls on the U.S. government to "develop a superior cybersecurity workforce," while the *Department of Defense Cyber Strategy* further expounds on this vision, identifying the cyber workforce as a "critical cyber asset."[1] The commander of U.S. Cyber Command, Gen. Paul M. Nakasone, U.S. Army, reaffirmed the importance of cyber manpower to U.S. cyber competition in his February 2019 testimony before the Senate Armed Services Committee, arguing that "the retention of top talent—particularly in some critical, high-skill jobs—is a significant concern because it will be crucial to our continued success."[2]

In a discipline that often seems to privilege technology, both of these cyber strategies identify human capital as a core requirement for success. What is clear from these strategies is that the cyber competition of today is not about technology. It is about technologists. Therefore, the successful implementation of strategy requires not just the right investment in technical capabilities or the appropriate authorities to conduct operations. None of the other tenets of cyber strategy can be accomplished without the right manpower and talent.

Human Capital, War, and Cyber Talent

The central role of human capital in a state's security is not new. In fact, the challenge of mobilizing, training, and retaining personnel for defense and conflict dates back to some of the first known examples of organized conflict. For example, the introduction of the longbow made recruitment of physically capable and technically competent archers central to England's ability to dominate new tactics of warfare. While the longbow itself was not an expensive weapon, its effective employment required extensive instruction and then practice to maintain proficiency; states struggled to recruit and train enough longbow archers to create the mass required for decisive battlefield advantage. A state hoping to capitalize on the revolutionary technology had to invest significant organizational and cultural effort into developing resident longbow talent for the king's army. As Douglas Allen and Peter Leeson note about its adoption, "the longbow required large numbers of archers to be effective, and the number of individuals privately willing to develop longbow skills was never sufficient to meet this demand. Second, as a result, a ruler who wanted to adopt the longbow had to create and enforce a culture of archery through tournaments, financial incentives, and laws supporting longbow use to ensure sufficient numbers of archers."[3] The difficulty obtaining competent archers helped usher in the new era of firearms—a weapon that required much less physical strength or technical competence.[4]

Especially after the earliest firearms, which were inaccurate and difficult to reload, were replaced with muskets and sabers, states no longer had to rely on specialized skill to create battlefield advantage. As John Landers writes, the gunpowder revolution "required no quality of the common soldier beyond endurance and a habit of machine-like obedience. . . . [T]he development of drill also laid the foundations for an enhanced degree of tactical co-ordination that underpinned substantial increases in both the scale and duration of battlefield combat, with corresponding increases in numbers of casualties."[5] The gunpowder revolution created weapons that could be fired by personnel without unique prior skills, making it easier for states to recruit manpower. However, the massed, linear battlefield employment of these firearms required that significant numbers of unskilled personnel be given intensive training. The requirement from the state therefore transitioned from cultural or societal investments in talent (such as the archery competitions created by the English kings) to investments in training and discipline. Drill became the means by which masses of unskilled labor could be equipped with firearms to sustain power at scale. The onus was on the military organization to train the general population in baseline skills. They could recruit from the general population by offering shelter, food, and (peacetime) security for those otherwise dependent on capricious landlord-tenant relationships. Military service could provide a means for upward social mobility or, in some cases, a substitution for imprisonment.

This focus on mass pools of unskilled labor saw its zenith in the armies of *levée en masse* of the French Revolutionary Wars. The *levée en masse* capitalized on the revolutionary movement toward governance by the people to mobilize massive militaries in the largest engagements ever seen until then in Europe. This was total war: "The French were exhorted to rise up as one nation, to do more than render unto Paris their sons for the front, but for all and sundry to join in a collective war effort."[6] Winning war was not about recruiting the right skilled manpower but instead about exercising the power of the state and the patriotism of its populace to put the entire weight of a nation behind a military objective. This was accompanied by the spread of conscription, a process by which the state leaned on patriotic sentiment to recruit wide swaths of the population for military conquest. As Carl von Clausewitz describes the change, "The people became a participant in war; instead of governments and armies as heretofore, the full weight of the nation was thrown into the balance."[7] The *levée en masse* took the human-capital trends of the gunpowder revolution and multiplied them. The multitudes of civilian conscripts made training and drill even more important to military effectiveness. Further, good order and discipline (as well as the development of effective political systems) in the *levée en masse* military became more important for common soldiers than individual skill.

The focus on large conscripted armies continued into World War I and World War II. At the same time, major technological advancements were changing the battlefield—from the development of chemical weapons to that of tanks, aircraft, and radio. World War I, especially, was caught in the tumult of technological change, its manpower-heavy tactics engulfed by the onset of highly lethal and long-range weaponry. World War I saw the loss of almost eleven million military personnel in combat, primarily (at least on the western front) in high-casualty trench warfare. Nations were faced with a dual dilemma of filling the trenches with able but not necessarily skilled men and at the same time providing manpower with the increasingly technical skills required to use the new technologies that, it was hoped, could break the impasse to which trench warfare had devolved. For example, Great Britain late in the war was forced to make a strategic choice to prioritize emerging technical manpower over trench manpower. As Paul Kennedy writes, "By the last years of the war, few extra able-bodied men could be drafted into the army without affecting armaments production. . . . [T]he Manpower Committee of the War Cabinet gave priority first to the navy and air force, then to the merchant marine, shipbuilding, coalmining and timber industries, and then to armaments and food production: the army came at the bottom of the list."[8]

Technology and the resources to produce that technology became even more important in World War II, where the introduction of blitzkrieg by the German military placed central importance on the combined use of tanks, aircraft, and mobile artillery, all linked by radio. Further, submarines and aircraft carriers revolutionized naval warfare,

making both the undersea and surface-warfare domains active zones of technical experimentation. To counter these new technologies, states raced to develop radar, sonar, and encrypted communications. As in World War I, states had to learn to balance their needs for large swaths of the population to build armies large enough to absorb the attrition of highly lethal ground warfare and the need to recruit and train specialized manpower to operate the new technologies. Pilots and aircrew, for example, became constant concerns for all the major powers. Nations had to recruit and train at scale individuals who could pass stringent visual tests, demonstrate technical skills, and succeed in basic aeronautical tasks. Further, high casualties meant that combatants engaged in these sustained air campaigns had to build training pipelines to keep up with the thirsty demand for pilots and aircrew.

The need that developed in World War II for highly specialized weapons technicians has only become more pronounced in the last sixty years. The advent of nuclear weapons generated a need for very highly specialized talent—nuclear physicists, rocket scientists, and aeronautical engineers. Strategic deterrence was built on emerging radar capabilities and satellite technology. Under the seas, a highly technical cat-and-mouse game of sensor capabilities was also occurring, and in the air, states battled to win competitions in maneuverability, speed, and avionics. Further, the development of the microprocessor (a key advancement for nuclear targeting that would have implications across the warfare domains) made computers both cheap enough to build into ordnance and yet indispensable for all aspects of war. Scientists such as Alan Turing and Claude Shannon built the foundation of these technologies; airmen, soldiers, and sailors experimented with the technology to create operational doctrines and tactics to employ these new capabilities. Further, as the use of radio communications exploded, so also did signals intelligence and the creation of a new breed of top computer scientists within the civilian intelligence community. They became highly skilled cryptologists, who, moving in and out of government, built the National Security Agency into a hub for high-level talent in the Cold War.

But at the same time that states were developing high-tech weaponry for strategic engagements, certain states were also actively combating each other in limited wars: in Korea, Vietnam, Israel, Egypt, Iran, Afghanistan, and Iraq. Some of these wars were proxy conflicts within a more strategic Cold War. The American and Soviet governments had to balance the need for manpower to fight these wars with domestic pressures. In the United States in particular, decision makers had to deal with issues of public support for conscription while also attempting to attract and retain talent to operate high-tech weaponry. Meanwhile, for the many states caught in them, U.S.-Soviet proxy wars were existential conflicts, in which they had to race to create both pools of talented manpower and forces large enough to endure sometimes extended conflicts.

This brings us to today and the historical question of where cyber talent fits in the trajectory of human capital and war. We have seen that the relationship between technology and warfare has a large impact on the types of human capital in which a state must invest. Whereas the advances in lethality brought by gunpowder decreased the need for specific human capital and skill and vastly increased the need for quantity of personnel, the development of technology like the longbow or the airplane required unique efforts to attract and retain talent for the military. Further, as warfare became both more lethal and more technological, militaries saw the need for human capital in both large numbers and with specific critical skills. This required societal investments in governance, education, and institutions. Cyber talent is not unique in these respects. It is a specific type of human capital (like longbow archery) that requires societal investment in recruitment and retention, while the proliferation of digital capabilities throughout the modern military makes cyber skills an essential part of the training that goes into utilizing larger numbers of less-skilled human capital.

Cyber Talent and Great-Power Competition and Conflict

The 2017 *National Security Strategy* and *2018 National Defense Strategy* proclaim the resurgence of great-power politics and long-term competition with the rising peers China and Russia. From these documents both the *National Cyber Strategy* and the *Defense Cyber Strategy* derive their core tenets. Central to victory for both competition and conflict within these strategies is the ability to compete while deterring conflict and, if necessary, winning military engagements quickly and decisively. Technology plays a central role in these strategies—in ensuring economic prosperity, in protecting freedom of speech and democratic governance, in safeguarding a free and open internet, in ensuring situational awareness of adversary capabilities, in providing long-range and precise military strike capabilities, and in coordinating joint forces across the globe. The armed forces, in great-power competition and conflict, must be poised to defend the United States against day-to-day cyber and influence operations while honing conventional and nuclear military power to deter adversary aggression.

To do this, the United States needs a force that can innovate and experiment with technologies, integrate new technologies into operations, and, perhaps most importantly, maintain and sometimes function without technology. Whereas the mechanization revolution created a whole new class of military professionals trained to maintain and utilize technology like the tank or the airplane, today's warfare requires a class of military professionals that can safeguard, collect, store, process, transmit, use, and restore data. Instead of machinery technicians, future warfare calls for data scientists, network engineers, cloud-security specialists, satellite communications engineers,

machine-learning scientists, robotics engineers, computer programmers, user-experience engineers, development and operations engineers, and system-development engineers.

These emerging technological missions will happen in conjunction with many of the bread-and-butter mission sets of today's military—launching missiles, conducting air defense, patrolling zones, conducting ground maneuvers, transiting oceans, and providing nuclear deterrence. Consequently, the future force will include data scientists and infantry officers, programmers and fighter pilots, graphic designers and logisticians, webmasters and special operations units. Technologists in this force will be located at research and lab centers in the United States, embedded in combat units deployed and at home, and assigned to Reserve and Guard units focused on defending the nation against asymmetric threats. In addition, technological skills will become necessary capabilities for other core combat specialties as the force of today becomes trained and prepared for the conflicts of tomorrow.

Cyberspace is the medium through which almost all these digital technologists and technologies operate. Consequently, cyberspace personnel play a significant role in both competition and conflict. In competition, cyberspace serves as a zone of confrontation in which states vie both to gain economic advantage and to leverage their cyber accesses and exploitation to build military campaigns. In conflict, the space becomes even more contested as states transition from economic or influence campaigns to the exploitation of cyberspace vulnerabilities to create virtual and physical damage to both military resources and critical infrastructure. Cyber personnel in competition may reside far from deployed or forward projected areas, but as competition moves to conflict and difficult accesses and precarious networks require the physical presence of cyber talent, quite often cyberspace personnel will move geographically to areas closer to the battlefield.

Cyber talent for great-power competition and conflict, therefore, needs to be able to provide network defense and conventional and unconventional access and exploit development for offensive cyber operations. Individuals are required who understand information operations as well as the ways in which information is transmitted and secured. It will include both civilians and military armed forces, deployed and at home. These will be tailored-access operators, cloud security engineers, network security architects, hackers, information security engineers, and cybersecurity analysts.

The Problem: The Cyber Talent Shortage

Technologists and cyber talent, then, will be a huge element of success in the new era of competition and conflict. The problem that states have—as medieval kings did with the longbow—is in creating, recruiting, and retaining that technological talent in the armed forces. This is especially challenging in cybersecurity. A 2018 study conducted by the

International Information System Security Certification Consortium, or (ISC)^2, identified a cybersecurity labor gap of almost 500,000 professionals.[9] Estimates suggest that the gap will only continue to grow; a 2019 report from the Departments of Commerce and Homeland Security forecasts a total of 1.8 million unfilled cybersecurity positions by 2022.[10] Further, an annual survey conducted by the Enterprise Strategy Group found that 53 percent of the organizations it surveys "report a problematic shortage of cybersecurity skills."[11] The problem extends to the Department of Defense (DOD). According to its principal deputy chief information officer, "DoD has seen over 4,000 civilian cyber-related personnel losses across our enterprise each year."[12]

Why is there a talent shortage for cybersecurity professionals? Part of the problem is that cyber threats have proliferated so fast that the talent pipeline has been unable to keep up. For years, cybersecurity was a marginal niche of information technology. Companies went all-in on talent to develop IT (information technology) applications for themselves, often with little thought for the repercussions of that technology. Consequently, the private sector initially relied on small groups of IT personnel on staff and, increasingly, vendors to solve cybersecurity issues. This means that for a long time generating a cybersecurity workforce has been generally delegated away from the core practices of industry. As cybersecurity researcher Greg Falco explains, many think that "it's not going to be me—it's my vendor who is going to get attacked."[13] Similarly, colleges and universities at the beginning of the information revolution sought to create computer scientists and computer engineers but for many years offered no similar education opportunities in cybersecurity. Heather Ricciuto, an academic outreach leader for IBM Security, argues that "the lack of resources at an educational level is a significant contributor to the shortage. . . . [W]hile hands-on, technical skills are most sought-after by employers, many schools lack trained teachers or course materials in cybersecurity."[14]

Because of the lag between need and training, there is intense competition for cybersecurity professionals among civilian companies and between the private sector and government. As large as the challenge may be for these civilian industries, it is even greater for the U.S. Department of Defense. The military must pull from a smaller segment of talent than top civilian companies, for a series of reasons. First, while civilian companies draw from a global talent pool, the U.S. government (civilian and military) recruits American citizens predominantly—a requirement that is especially central to missions that are deemed sensitive. Further, qualified candidates must have only limited past drug use and be willing to report all foreign travel and connections (something that can be laborious and creates huge career impediments in fields dominated by foreign researchers and workers). The backlog of requests for security credentials is a significant problem for recruiting individuals into the defense cybersecurity workforce. As of spring 2019 it numbered almost 500,000 government security investigations; processing

for a top-secret clearance was taking an average of 468 days, the less restrictive secret clearance 234 days.[15] These processing times increase for candidates with more foreign contacts and travel, making many cybersecurity professionals with significant civilian expertise even more difficult to bring on board.

The IT interfaces that are used to recruit and hire these personnel also impede successful competition for cybersecurity talent. In a 2019 report, the National Commission for Military, National, and Public Service found that

> civil servants and others also told us that the federal hiring process is too slow, fails to accurately assess job applicants, contains a variety of inflexible hiring preferences, and many times fails to hire anyone for open positions. We heard from current and aspiring civil servants that USAJOBS, which is the federal government's central portal for job postings and applications, does not meet the needs of either applicants or hiring managers. Existing rules and regulations make leaving and returning to federal employment unnecessarily difficult and discourage employees who value flexibility and the ability to move from one organization to another. These problems seem especially severe when it comes to younger Americans. Americans under the age of 35 make up 35 percent of the nation's workforce but only 17 percent of federal civilian employees. Ready or not, generational change will come to federal agencies, because 30 percent of civil servants, including a majority of senior agency executives, will be eligible to retire in five years. Yet young adults are avoiding or being turned away from federal employment.[16]

Bringing these individuals into the armed forces is even more difficult than the already daunting challenge of recruiting the civilian workforce. Military personnel must meet physiological requirements—whether that be physical fitness tests or baseline health assessments. Recruiters often require candidates to go through military entrance processing stations and, often, complete basic military training. Top cybersecurity professionals with asthma, certain dental implants, irritable bowel syndrome, or problems with pronation may not be medically qualified to serve in the armed forces; nor would those who have suffered from depression within three years or have allergic reactions to fish, insects, or nuts.[17] The number of individuals medically disqualified is not inconsequential. Joe Schuman finds that "in 2012, according to the Department of Defense's Accession Medical Standards Analysis & Research Activity (AMSARA) Annual Report, 38,000 of 200,000 active-duty applicants (or 19 percent) across all military services were medically disqualified from service."[18] Further, the hierarchical and longevity-based promotion structures of military organizations mean that almost all individuals—regardless of talent or expertise—must start their military careers at the lowest ranks. This makes it hard to recruit midlevel or senior talent into military positions.

Recruiting and retaining this small pool of talent is an uphill battle for DOD. It's easy to blame differences in the pay of military and civilian cybersecurity professionals, but surveys suggest that many top technologists are willing to sacrifice compensation for work satisfaction. While DOD can offer meaningful missions and often opportunities to work on technologies not accessible in the civilian realm, it has a long way to go to

create a satisfying work environment. Service members often invest ten to twelve hours a day on their missions and are asked to perform extended temporary additional duty and remote deployments. On top of their mission requirements, service members are asked to deal with unwieldy administration, including an overly complicated Defense Travel System, human resources applications that are often inaccessible from standard internet browsers, defense websites incompatible with non-PCs, and time-consuming computer-based training that functions more as a risk mitigator than a skill enhancer.

Additionally, the accessions and promotion system struggles with nontraditional candidates and provides little flexibility for career progression—a major disincentive for younger candidates. The traditional military family life, which calls on members and their families to move to new stations every one to three years, poses significant challenges for dual-career couples, who represent a prominent constituency in the high-technology talent sample.[19] Also, unlike many of the major technology firms that have prioritized family services, DOD does not have high-quality child care at all military installations (and especially not covering the extended hours of many duty days).[20]

Talent, Cyber Strategy, and Current Initiatives

What is being done to win the talent competition? How does current strategy guide the development of the cyber workforce? Both the *National Cyber Strategy* and the *Defense Cyber Strategy* suggest that manning the cyber workforce is not about generating masses of unskilled workers but instead recruiting high-quality manpower. The *National Cyber Strategy* identifies four priority actions to generate quality cyber manpower: first, "build and sustain the talent pipeline"; second, "expand re-skilling and educational opportunities for America's workers"; third, "enhance the federal cybersecurity workforce"; and fourth, "use executive authority to highlight and reward talent."[21]

To that end, a May 2019 presidential executive order set forth a series of initiatives to attract and retain federal government cyber talent. These initiatives include establishing a "cybersecurity rotational assignment program," identifying "cybersecurity aptitude assessments," ensuring "existing awards and decorations for the uniformed services and civilian personnel recognize performance and achievements in the areas of cybersecurity and cyber-operations," developing "a plan for an annual cybersecurity competition (President's Cup Cybersecurity Competition) for Federal civilian and military employees," launching "a national Call to Action," transforming "the cybersecurity learning environment to grow a dynamic and diverse cybersecurity workforce," aligning "education and training with employers' cybersecurity workforce needs," and establishing and using "measures that demonstrate the effectiveness and impact of cybersecurity workforce investments."[22]

The *Department of Defense Cyber Strategy* summary outlines four action priorities to cultivate talent. The first, "Sustain a ready cyber workforce," focuses on the organizational requirements for professional development, career progression, and manning within DOD. The second, "Enhance the nation's cyber talent," calls for talent development within U.S. education partners and industry, starting from primary and secondary levels through higher education. The third, "Embed software and hardware expertise as a core DoD competency," broadens cybersecurity to other computer science disciplines and offers retention and employment opportunities beyond the Department of Defense. Fourth and finally, the summary (like similar initiatives at the federal level) aims to "establish a cyber top talent management program" that tracks talent acquisition and retention and offers incentive programs to meet talent management goals.[23]

These initiatives follow closely the recommendations of a Defense Science Board analysis of cyber as a strategic capability. Some of these recommendations include that "the Commander USCYBERCOM direct and ensure development of a portfolio of cyber military capabilities/effects, focused on adversary military targets," that "includes the development of infrastructure and tools to support the Cyber Mission Forces" and "ensures operational experience and an exquisitely skilled workforce"; that the heads of the services "direct their personnel staffs (i.e., the '1s') to treat the cyber mission career field as a national security priority," to ensure that "promotion boards understand the cyber mission as a priority and facilitate recruitment, retention, and career-long professional development in cyber expertise"; and that "the Commander USCYBERCOM establish and expand professional military education opportunities, at all levels, to allow military personnel to work in cyber-related private-sector positions."[24]

Together, these strategies identify cybersecurity and associated cyber skills as high-demand but low-density resources in which DOD must prioritize recruiting and retaining the best talent rather than recruiting large masses of unskilled populations and training them to create comparable advantages. Initiatives to fulfill this strategic direction have already begun within both DOD and the larger federal government.

Current initiatives include organizational fixes, near-term solutions for acquiring and hiring individuals, and programs to pair civilian talent with immediate DOD problems. This includes direct-commissioning programs into armed forces cyber components and the Cyber Excepted Service, which aims to expedite the process of federal hiring for civilians from an average of 111 days to forty-four.[25] Further, DOD has invested in programs that pair innovative civilians with core DOD cyber missions, such as the Defense Digital Service Tatooine Program and initiatives led by the Defense Innovation Unit (DIU).[26]

Other talent initiatives supporting the cyber strategies include programs to identify top talent within the current workforce and among individuals coming into DOD. The Air Force, for instance, is asking its airmen to identify their coding-language proficiencies—as the service now asks about spoken languages and rewards airmen for their ability to speak highly desirable languages.[27] The Army is testing different methods of identifying talent, including the cyber component of the Armed Services Vocational Aptitude Battery and civilian tests that identify potential cyber talent that does not come into the military with previous training or certifications.[28] Finally, DOD is investing in training (or retraining) its current force, including programs to send service members to civilian certifications, the Federal Cyber Reskilling Academy, and the National Science Foundation Career Compass Challenge, as well as service-specific initiatives.[29]

DOD, like the federal government, is already making concerted long-term investments in talent from the broader civilian community. In particular, the National Security Agency has instituted the National Centers of Academic Excellence program, which offers curriculum guidance for both cyber defense and cyber operations. The National Security Agency program has provided a baseline for use by higher education in developing cybersecurity teaching and research centers with the aim of creating a pipeline of cyber talent. Most importantly, the National Security Agency initiative solves a collective action problem for many university computer-science departments that had struggled to find institutional space or pedagogical precedent to create and administer accredited cybersecurity programs.[30] Looking at an early part of the talent-building pipeline, DOD has announced cybersecurity scholarship programs, apprenticeship programs, boot camps, and hackathons.[31]

Future Solutions

DOD has already made significant strides toward implementing its strategy to attract, train, and retain a talented cyber workforce. This is a promising start, but even more work will be required to ensure that the initial steps taken today translate into strategic success in the future. Cultural, organizational, and technological changes will be needed.[32]

Cultural Solutions. The vast majority of initiatives currently fielded for talent focus on institutional or organizational changes. However, one of the major barriers to recruiting and retaining cyber talent is cultural. As the military becomes smaller and represents a smaller percentage of the overall American population, the divide between civilians and military personnel becomes a significant impediment to attracting top talent. Raj Shah, former head of the Defense Innovation Unit and a reserve Air Force pilot, argued in testimony for the National Commission on Military, National, and Public Service that

> in 1980, 64% of Congress and 59% of Fortune 500 CEOs were military veterans. Today, those numbers have fallen to 19% and 6% respectively. Military service in the US is also becoming a hereditary trait. From the DoD's own reporting in 2013, 80% of new recruits have extended family that are veterans and 25% have a parent that has served. Coupled with the fact that less than 1% of the US population currently wears a uniform, we risk US military service being predominantly borne by a warrior caste—similar trends in history have not shown to be accretive to democratic stability.[33]

The civil-military divide has been especially obvious in Silicon Valley, where employees in companies such as Google have protested working with the military.[34]

DOD will need to build real relationships between technologists and armed service members, reducing the gap between civilians and military people by fostering daily relationships. This can be done by creating military units in high-tech areas like Silicon Valley, Boston, Austin, and the North Carolina "Research Triangle"; some of this is already under way, with the new Army Futures Command as well as DIU locations in both Boston and Silicon Valley. Other possibilities include engaging with academics at research universities and in graduate programs and building on initial moves to provide creative career progression opportunities, including fellowships in the civilian sector, normalized transitions between the Reserves or National Guard and active duty, or sabbatical periods. Some of the top talent will have high-risk relationships with foreign companies or technologists; this is an externality of their industry and should not be a deal breaker. Processes and criteria for security clearances, however, may need to be reevaluated.

Finally, the armed forces may need to reevaluate their standards for grooming and physical fitness, especially regarding what requirements are necessary for the warrior of the future. Technologists embedded in combat units may need to meet their physical standards, but others farther from the line of fire may be valuable contributors even with poor fitness scores.[35] Further, the ailments that disqualify individuals from military service need to be revisited, especially for cybersecurity direct accessions.

Organizational Solutions. The military has already launched a series of initiatives to streamline hiring for cybersecurity professionals, test for technological skill sets, identify programming capabilities, and invest in scholarships and reskilling academies. These are strong first steps but have yet to show significant progress in closing the technological talent gap. Without complementary changes in promotion structures, improvements on the recruitment side might not solve retention shortfalls in the long term. Additional focus on providing certifications, unique training on emerging technologies, and opportunities to employ or experiment with innovative technologies can help. Difficulties retaining talent could be further mitigated by distributing technological capability within forces that already have high retention rates. Retraining capable service members can decrease accession lags while also investing in people who have already assimilated

into military culture. Providing technological training to combat units and noncyber specialties may also provide an overall increase in technological capabilities with less investment in new personnel.

The Reserves and Guard provide a potential organizational solution in the search for technologists. Their personnel are often employed in the civilian sector, and some have cutting-edge training and experience. Further, the Reserves and Guard provide a nontraditional option for technologists looking to serve their country without active-duty obligations. There are significant caveats, however, about using the Reserve and National Guard as the primary solutions to a technological talent gap in the active-duty military.[36] Over the last fifteen years, the Reserve and Guard force has become more like the active-duty, deploying in place of active-duty units and prioritizing the growth of full-time Reserve and Guard personnel. While that has solved many of the difficulties of fighting multiple wars with an all-volunteer active-duty force, it has also made the Reserve and Guard less useful as an outlet to attract nontraditional talent.

Additionally, because the Reserve and National Guard have not heavily invested in innovative information technology, part-time reservists and guardsmen spend a disproportionate amount of their time trying to navigate unwieldy online training, human-resources applications, and travel and orders websites. Those who take significant pay cuts from their civilian jobs to participate in drills and annual training may find it frustrating to spend their time on such nonmission work. Finally, many reserve units struggle to employ their part-time technologists gainfully in short drill periods and instead promote multiple-month full-time orders for them. Highly successful (and highly paid) talent may not opt for these long-term commitments and therefore remain underemployed. Recent testimony from Raj Shah recommends the development of a strategic reserve that could allow the active-duty military to rely on the resident talent of a Reserve or Guard cybersecurity force without the difficulty of keeping a given reservist or guardsman deployable.[37] The Cyberspace Solarium Commission extended this recommendation, calling for Congress to investigate the potential for this cyber strategic reserve force.[38]

Technological Solutions. Many of the challenges faced by the active-duty, Reserve, and Guard communities can be solved with investment in better information technologies, especially IT that streamlines personnel actions, travel, and training. So far, DOD has not prioritized technological solutions for administration and instead has chosen to spend labor time—a fixed cost for active-duty forces—to manhandle cumbersome administrative tasks. If DOD wants to retain the best talent across capabilities and skill sets, it must give investment in administrative IT as high a priority as new missiles or radars. Further, investment in IT for human resources can create databases of special

skills, align those skills with appropriate jobs, and track successes and problems in recruitment, assignment, and retention.

Challenges, Evaluating Success, and Moving Forward

DOD has embraced talent as a key component of its larger strategy to compete successfully in cyberspace. Its strategic goals and initiatives fall under a larger need within the federal government to develop cyber talent and use that talent to win in great-power competition. The focus on recruiting specific human capital rather than masses of unskilled labor for training is not without historical precedent; similar efforts occurred in the "infantry revolution" and in more recent times starting with the surge of technology onto the battlefield in the "mechanization revolution." These historical analogies show the difficulty in strategies contingent on competition for specific human capital. More importantly, historical examples show that strategies contingent on highly specialized talent require significant monetary investment, as well as governance and societal structures that can compete for talent with civilian and national-security sectors and can measure both short-term and long-term success in developing a talented workforce.

As DOD implements its cyber strategy, it will need to tackle a series of important questions. First, how will it prioritize the resources required to recruit and retain cyber talent? Those implementing the strategy should attempt to track the costs of these initiatives, prioritizing solutions that are either low in cost or create large successes that outweigh their costs. This raises the second challenge, measuring short- and long-term success. How will we know whether the investments we make in talent are worthwhile, especially investments in long-term talent? Finally, this analysis has highlighted the increasingly complex relationship between civilian and uniformed cyber talent. While many of the solutions to the talent shortage involve leveraging civilian training and talent resources, the question remains: Which tasks must be performed by armed service members and which by civilians? As Raj Shah testified,

> While organisations like the Defense Digital Service and the Defense Innovation Unit have done a tremendous job attracting civilians for short tours of service, this human capability cannot be solely outsourced to contractors or even civilians. We need uniformed members, both officer and enlisted, to combine their tech-nativity with the credibility and authority inherent under Title 10.[39]

Notes

1. *National Cyber Strategy* (Washington, DC: White House, September 2018), https://www.whitehouse.gov/; U.S. Department of Defense [hereafter DOD], *Summary* [*of the*] *Department of Defense Cyber Strategy 2018* (Washington, DC, 2018), p. 17, https://media.defense.gov/.
2. U.S. Senate, *Statement of General Paul M. Nakasone, Commander, United States Cyber Command before the Senate Committee on Armed Services,* 116th Cong., Washington, DC, 2019, p. 9, https://www.armed-services.senate.gov/.

3. Douglas W. Allen and Peter T. Leeson, "Institutionally Constrained Technology Adoption: Resolving the Longbow Puzzle," *Journal of Law and Economics* 58, no. 3 (August 2015), pp. 683–715.
4. Gervase Phillips, "Longbow and Hackbutt: Weapons Technology and Technology Transfer in Early Modern England," *Technology and Culture* 40, no. 3 (July 1999), pp. 576–93.
5. John Landers, *The Field and the Forge: Population, Production, and Power in the Pre-industrial West* (Oxford, U.K.: Oxford Univ. Press, 2003), p. 195.
6. Michael Broers, "The Concept of 'Total War' in the Revolutionary-Napoleonic Period," *War in History* 15, no. 3 (July 2008), p. 247.
7. Carl von Clausewitz, *On War,* ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton Univ. Press, 1976), pp. 591–92.
8. Paul Kennedy, "Britain in the First World War," in *Military Effectiveness,* vol. 1, *The First World War,* ed. Allan R. Millett and Williamson Murray (Cambridge, U.K.: Cambridge Univ. Press, 1988), p. 37.
9. $(ISC)^2$, *Strategies for Building and Growing Strong Cybersecurity Teams: $(ISC)^2$ Cybersecurity Workforce Study, 2019* (Clearwater, FL, 17 October 2018), p. 8, https://www.isc2.org/. This chapter is agnostic as to divisions of talent within cybersecurity—for instance, the difference between information security, network defense, and offensive cyber capabilities. However, further iterations of talent strategies should think more concretely about differences between these cyber skills and their respective talent needs.
10. "U.S. Cyber Workforce Shortage Worsening, Agencies Tell President," *MeriTalk,* 31 May 2018, https://www.meritalk.com/; Secretary of Commerce and Secretary of Homeland Security, *A Report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future* (Washington, DC: U.S. Commerce Dept., 30 May 2018), p. 1, https://www.nist.gov/; Frost & Sullivan, Center for Cyber Safety and Education, and $(ISC)^2$, *2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk* (Clearwater, FL, 30 April 2019), p. 2, https://isc2-center.my.salesforce.com/.
11. Jon Oltsik, "The Cybersecurity Skills Shortage Is Getting Worse," *ESG Blogs* (blog), *Enterprise Strategy Group,* 10 January 2019, https://www.esg-global.com/.
12. *Cyber Operational Readiness of the Department of Defense,* statement by Essye B. Miller, Department of Defense Principal Deputy Chief Information Officer, before the Senate Armed Services Committee Subcommittees on Cybersecurity and Personnel, 115th Cong., Washington, DC, 2018, p. 2, https://www.armed-services.senate.gov/.
13. Quoted in Betsy Foresman, "On Cybersecurity, Educational Institutions Have a People Problem," *EdScoop,* 1 April 2019, https://edscoop.com/.
14. Shirley Tay, "A Serious Shortage of Cybersecurity Experts Could Cost Companies Hundreds of Millions of Dollars," *CNBC,* updated 6 March 2019, https://www.cnbc.com/.
15. Lindy Kyzer, "How Long Does It Take to Process a Security Clearance? Q1 2019 Update," *ClearanceJobs,* 12 March 2019, https://news.clearancejobs.com/; Caroline D'Agati, "Latest Update on the Security Clearance Backlog and Transfer to DoD," *ClearanceJobs,* 16 April 2019, https://news.clearancejobs.com/.
16. National Commission on Military, National, and Public Service, *Interim Report January 2019: A Report to the American People, the Congress, and the President* (Washington, DC, January 2019), p. 12, https://inspire2serve.gov/. See also Eric Katz, "The Federal Agencies Where the Most Employees Are Eligible to Retire," *Government Executive,* 18 June 2018, https://www.govexec.com/, and Partnership for Public Service and McKinsey & Company, *A Pivotal Moment for the Senior Executive Service: Measures, Aspirational Practices and Stories of Success* (Washington, DC: Partnership for Public Service, 21 June 2016), p. 14, https://ourpublicservice.org/.
17. DOD, *Medical Standards for Appointment, Enlistment, or Induction into the Military Services,* DOD Instruction 6130.03 (Washington, DC, 2018), https://www.esd.whs.mil/.
18. Joe Schuman, "Department of Disqualified: Fixing the Broken Military Medical Accessions Process," *War on the Rocks,* 20 November 2018, https://warontherocks.com/.
19. Tom Barron, *To Retain Today's Talent, the DoD Must Support Dual-Professional Couples* (Washington, DC: Center for a New American Security, 7 January 2019), https://www.cnas.org/; Brad Orgeron, *Helping Special Needs Families and Improving Military Readiness*

(Washington, DC: Center for a New American Security, 2 April 2019), https://www.cnas.org/; Rosella Cappella Zielinski and Melinda Beyer, "Retain the Family in Today's All-Volunteer Air Force," *War on the Rocks,* 16 May 2019, https://warontherocks.com/; Laura L. Miller et al., *An Early Evaluation of the My Career Advancement Account Scholarship for Military Spouses,* RR-2093-OSD (Santa Monica, CA: RAND, 2018), https://www.rand.org/; Patricia K. Tong et al., *Enhancing Family Stability during a Permanent Change of Station,* RR-2304-OSD (Santa Monica, CA: RAND, 2018), https://www.rand.org/.

20. Leo Shane III, "The Military's Lingering Readiness Problem: Lack of Daycare," *Military Times,* 8 February 2019.
21. *National Cyber Strategy.*
22. Exec. Order No. 13,870, 3 C.F.R. 20523 (2019), https://www.govinfo.gov/content/pkg/FR-2019-05-09/pdf/2019-09750.pdf.
23. DOD, *Summary DOD Cyber Strategy 2018.*
24. *Defense Science Board Task Force on Cyber as a Strategic Capability: Executive Summary* (Washington, DC: U.S. Defense Dept., June 2018), p. 4, https://dsb.cto.mil/.
25. "Army Cyber: Cyber Direct Commissioning Program," *U.S. Army,* last updated 24 January 2020, https://www.goarmy.com/; Lauren Woods, "Airmen Selected to Participate in New Cyberspace Direct Appointment Program," *U.S. Air Force,* 14 February 2018, https://www.af.mil/; Jared Serbu, "New DoD Personnel System Hires Cyber Workers Faster, but Numbers Still Small," *Federal News Network,* 19 March 2019, https://federalnewsnetwork.com/.
26. DOD, "DOD Expands Tech Talent Initiative to Develop Critical Cyber Capabilities," *U.S. Dept. of Defense,* 25 October 2018, https://dod.defense.gov/; "The Latest," *Defense Innovation Unit,* accessed 17 February 2020, https://www.diu.mil/news-events.
27. Joe Pappalardo, "The Air Force Will Treat Computer Coding like a Foreign Language," *Popular Mechanics,* 13 September 2018; Jim Perkins, "The Next New Military Specialty Should Be Software Developers," *War on the Rocks,* 22 January 2018, https://warontherocks.com/.
28. Jeffrey D. Morris and Frederick R. Waage, *Cyber Aptitude Assessment: Finding the Next Generation of Enlisted Cyber Soldiers* (West Point, NY: Army Cyber Institute, 16 November 2015), https://cyber.army.mil/.
29. Dorothy Aronson, "NSF Looks for Innovative Technology to Prepare for the Workforce of the Future via the Career Compass Challenge," *CIO Council,* 12 December 2018, https://www.cio.gov/; "Federal Cyber Reskilling Academy," *CIO Council,* accessed 17 February 2020, https://www.cio.gov/; Sharon Anderson, "Recruiting, Training and Maintaining Talent in the Cyber Workforce," *CHIPS,* July–September 2013, https://www.doncio.navy.mil/chips/.
30. "National Centers of Academic Excellence," *NSA/CSS,* accessed 17 February 2020, https://www.nsa.gov/.
31. "DoD Cyber Scholarship Program (CySP)," *Chief Information Officer, U.S. Department of Defense,* accessed 17 February 2020, https://dodcio.defense.gov/Portals/0/Documents/Cyber/dodcyspfastfacts.pdf; "STEM Programs," *Department of Defense DoDSTEM,* accessed 17 February 2020, https://dodstem.us/stem-programs/programs.
32. For more insight on these, see Lindsay Cohn's recommendations laid out in her testimony, *Military Service Hearing: Increasing Awareness among Young Americans and Lessening the Civil-Military Divide,* testimony before the National Commission on Military, National, and Public Service, 16 May 2019, https://www.inspire2serve.gov/_api/files/270.
33. Raj M. Shah, *Military Service Hearing: Creating New Pipelines to Service and Fostering Critical Skills,* testimony before the National Commission on Military, National, and Public Service, 16 May 2019, https://www.inspire2serve.gov/_api/files/268.
34. Scott Shane and Daisuke Wakabayashi, "'The Business of War': Google Employees Protest Work for the Pentagon," *New York Times,* 4 April 2018.
35. See Jacquelyn G. Schneider, "Blue Hair in the Gray Zone," *War on the Rocks,* 10 January 2018, https://warontherocks.com/.
36. Margaret Seymour, *A Lack of Support Leaves the Reserves Broken* (Washington, DC: Center for a New American Security, 5 February 2019), https://www.cnas.org/; Claude Berube, "All Sane Men Believe in Reserves," *War on the Rocks,* 21 March 2019, https://warontherocks.com/.
37. For more on the transition from a strategic reserve to an operational reserve, see Miranda

Summers Lowe, "The Gradual Shift to an Operational Reserve: Reserve Component Mobilizations in the 1990s," *Military Review* 99, no. 3 (May–June 2019), pp. 119–26, https://www.armyupress.army.mil/.

38. *Cyberspace Solarium Commission Report* (Washington, DC, April 2020), https://www.solarium.gov/report.
39. Shah, *Military Service Hearing.*

CHAPTER TEN

Defining and Measuring Cyber Readiness

BRIG. GEN. PAUL STANTON, USA; AND LT. COL. MICHAEL TILTON, USA

Readiness in the cyberspace domain rests on common foundational principles applicable across all warfighting domains, with important variations tailored to the unique characteristics of cyberspace. Recognition of these characteristics led the deputy secretary of defense to modify readiness standardization for cyber protection teams at the beginning of fiscal year 2020. The traditional model of service-developed force design and combatant-command employment was adjusted to authorize a combatant command to have a more direct role in shaping how the services build its cyber forces. The decision was reinforced with the approval of U.S. Cyber Command (USCYBERCOM) models for combat mission teams and combat support teams in April 2020. These decisions represent major steps in the Department of Defense and USCYBERCOM effort to define and measure sustainable readiness of cyberspace forces.

Readiness across the Department of Defense

At its core, readiness "determines our ability to fight and win our nation's wars. More specifically, it is the capability of our forces to conduct the full range of military operations to defeat all enemies regardless of the threats they pose."[1] Readiness is thus essential to the ability of armed forces to compete, fight, and win. When forces are assigned to a combatant command, whether a functional command such as U.S. Transportation Command or a regional command such as U.S. Central Command, the combatant commander is responsible for assessing the ability of assigned forces to execute the command's plans and orders. Without a foundation of readiness, a force is unable to execute its missions confidently.

Commander, U.S. Cyber Command (USCYBERCOM) has "the authority to balance risk across the Joint Force by focusing cyber capacity where it is most needed, both in time and space. This strategic approach to military cyberspace assets will allow us to deter and respond to or preempt cyber threats in all phases of conflict and to synchronize cyberspace operations globally."[2] Readiness for cyberspace forces is the metric for

assessing whether we can *sustain* cyber capacity against adversaries. The question we examine is how the Department of Defense is learning to judge the readiness of the nation's cyberspace operations forces as they have evolved from the initial stages of force generation to a maturing capability.

Traditional readiness standards across the department have two components: *capacity,* or a unit's level of manning, training, and equipping; and *capability,* or the measurement of ability to accomplish predetermined mission-essential tasks (METs) as a unit. For forces in the physical domains, Department of Defense policy charges the services with the responsibility for designing and building forces, using their particular domain expertise to set standards for manning, training, and equipping warfighters and units.

To offer a simple example, the U.S. Army draws on its "land domain" expertise to establish the manning, training, and equipping (i.e., capacity) standards for an armor battalion. The Army determines myriad details, such as the optimal number of tanks in a battalion, how many mechanics are needed to keep those tanks operational, and the training qualifications that tank crews should achieve. The Army will also develop the armor battalion's core METs, which will likely include such specific tasks as "Conduct a Movement to Contact" and "Conduct an Attack." The commander will then assess the battalion's ability to accomplish these METs, resulting in the battalion's core-capability assessment. When the armor battalion is deemed ready in terms of capacity and core capability, the Army will "present" it to a combatant command for potential deployment to a geographic area of operations. That command's plans and orders, in turn, will include the tasks that the armor battalion is responsible for accomplishing, which may be specifically tailored to the operating environment and threats in the region.

From Whiteboard to Full Operational Capability: Build-Assess-Build

The Cyber Mission Force (CMF) is the operational arm that USCYBERCOM employs to maneuver in cyberspace. Using experience at the time and best estimates of how cyberspace operations would evolve, in late 2012 the architects of the CMF concurred with a proposal to fund approximately six thousand billets from across the services. These billets created 133 teams, of five types: combat mission teams and combat support teams to deliver offensive effects under Department of Defense (DOD) authorities; cyber protection teams to defend the Department of Defense Information Network (DODIN) and other select U.S. networks; and national mission teams and national support teams to defeat significant cyberspace threats to the DODIN and the nation. USCYBERCOM published the Cyber Forces Concept of Employment (CFCOE, pronounced "sif-coe") to constitute the plan to bring the CMF concept to reality. At the root of the CFCOE is the cyclical concept of *Build-Assess-Build,* acknowledging the need to begin building and operating, then assess, improve on the basis of those assessments, and build again.

As USCYBERCOM undertook the challenge of assessing the initial build, it developed criteria for certifying a CMF team as having reached initial operational capability (IOC) and later full operational capability (FOC). Throughout DOD, IOC refers to a state when a capability is available in its minimally useful form. IOC is a good reference point for gauging any refinements necessary before proceeding to FOC, the state where the capability is fully developed. IOC and FOC criteria for cyberspace forces largely focused on quantitative measures, particularly counts of schoolhouse-trained individuals and resources available to conduct missions. These basic criteria provided a useful method for tracking service investment in personnel and training during the initial build.

Cyber IOC and FOC standards loosely followed the traditional DOD readiness framework, measuring capacity as a function of manning, training, and equipping. For manning, the command declared a team IOC at 50 percent manning, including a predetermined ratio of critical positions filled. These critical positions were a selection of work roles (depending on the team type) that were essential for the team to perform its range of assigned missions. IOC standards for training simply required that training requirements be identified and submitted to USCYBERCOM J7, the directorate that manages the available training resources. As a team built toward IOC, moreover, equipping standards minimally measured the assigned personnel's allocated space to perform duties—that is, seats and access to relevant networks, including access to data required to perform their missions. To achieve FOC, teams were measured against standards that served as a proxy for traditional DOD readiness metrics. An FOC team had to reach 85 percent manning, with at least 80 percent of those personnel trained and qualified in their specific work roles. A team also had to certify unit competency, on the basis of a subjective assessment.

Until May 2018, when USCYBERCOM declared all 133 teams FOC, the DOD focus in the cyberspace domain was building the Cyber Mission Force. This absolutely essential five-year effort resulted in close to six thousand service members joining the ranks of the CMF. During this build phase, USCYBERCOM gained operational experience and expertise necessary to assess its CFCOE plan.

Assessing the Initial Build

Most of the methods available to assess readiness for cyber mission forces are the same as those used to assess readiness for traditional forces. However, there is a crucial difference between the CMF and traditional forces—CMF teams are always assigned to USCYBERCOM and do not return to service control for foundational training or a force-generation cycle. As a result, a team still assigned to, and with responsibility for conducting, a mission needs to train and account for losing and replacing personnel. Moreover, a newly assigned team member requires individual qualification training

to be qualified to serve in his or her position, leaving a deficit at the team level until the new member is certified. As a result, USCYBERCOM needs to track the manning, training, and equipping status of operating forces while also shaping their design, because forces must *always* be presented.

To return for a moment to our earlier example of the armor battalion: a geographic combatant commander will not need as detailed an understanding of the manning levels of an armor battalion as the U.S. Army does, because the battalion was deemed ready to deploy before the combatant command "accepted" it. A comparison with the components of the CMF in the absence of the standard redeployment and force-generation cycle, however, quickly made clear that the readiness model for this emergent cyber capability needed to differ from that of traditional forces. In addition, as discussed in chapter 8, "Joint Operations in Cyberspace," the CMF teams are built to be joint. Army and Navy teams, for example, must be prepared to execute the same tasks regardless of network owner. They operate on the same terrain and under operational chains of command that cross service and geographic boundaries. This is significantly different from the traditional model of service force generation and presentation to a combatant command.

An Inflection Point in a New Domain

After nearly ten years of design, development, and operations, USCYBERCOM has reached an inflection point, at which it can learn from operational experience and shape its next decade of evolution. USCYBERCOM has built a roughly six-thousand-member force. It has been elevated to a functional unified combatant command. It has successfully performed countless operations against adversaries. It has received strategic guidance and authorities that shape its priorities and empower its forces. These changes have created both the opportunity and necessity to reevaluate initial assumptions about how best to employ the Cyber Mission Force strategically and to execute operations tactically. Lessons learned from past successes also revealed a need to evolve the cyber readiness model.

The key to defining "readiness" effectively is a firm understanding of how we fight. We must ask ourselves, "For what are we to be ready?" Absent an informed answer, we risk squandering resources, wasting time, and compromising preparedness—all undermining USCYBERCOM's ability to perform its missions. During the 2019 fiscal year, USCYBERCOM established the cross-functional CMF Review Team to study lessons learned and conduct a comprehensive analysis of functions, missions, force structure, readiness requirements, and training standards.

Consensus on how to fight drives the organizational construct for employment—that is, how best to organize. Organizing to fight requires aligning the correct skill sets to individuals and then combining the individuals into small units capable of mission execution. As USCYBERCOM capitalizes on experience, the initial organizational focus has been on structuring the correct "unit of action" for tactical operations. For example, USCYBERCOM learned that basic defensive cyberspace operations require a combined insight derived from analyzing host systems and the networks that support system communication. The technical details and complexity of effectively analyzing hosts and networks, however, mean that very different skills are required. Thus, in building even a basic unit of action for defending networks, the command blends together individuals with at least those particular skills for mission success.

The proper combination of skilled individuals shapes the definition of tactical units of action, which are modeled after similar constructs in other warfighting domains. Just as the Army combines the skills of a gunner, loader, driver, and tank commander into a tank crew, the cyber domain aggregates technical skills into cyber *mission elements* that form the foundational organizational building blocks for operations.[3]

Next, USCYBERCOM had to determine the appropriate "weapons platform" for the unit of action to support how we plan to fight. How do we then equip the mission element? Achieving effects in the cyber domain requires some ability to see and manipulate data through code at the right place and time. Maneuver requires posturing a mission element at that correct place with the right data access to manipulate the system according to an objective. A cyber weapons platform, then, must equip the individuals within a mission element with the appropriate situational-awareness capability so that each member can support the team's maneuver to achieve or deliver effects. Crews achieve effects via weapons platforms in every other operational domain, and the cyberspace domain is no different. An F-35 crew employs the airframe to maneuver to the correct location to deliver a payload, just as a cyber mission element maneuvers through the network with the correct infrastructure and tools to achieve an effect.

Having defined a new organizational construct with an appropriate weapons platform that combines individual tasks according to how we fight, the command has had to rethink the definition of the proper collective tasks for this new mission element. The unit of action must function in unified fashion to support maneuver in the cyberspace domain with clearly defined tasks that synergistically combine individual skills into effective unit operations. To leverage the tank example, the crew members individually provide no meaningful combat power—if they cannot combine their skills to maneuver the tank, load ammunition, and fire the main gun, the vehicle is not useful. The crew must work together to provide the unmatched capabilities of our armored force, and the crew's collective tasks to shoot, move, and communicate define how the individuals

must operate together. So, too, must we combine the individual tasks in the cyber domain for our mission elements. Determining how data and information derived from one individual's actions feed another member's activities defines the cyber collective tasks. One collective task, for instance, may require that an individual study a computer's operating system and combine his or her findings with another's analysis of host memory and then further integrate yet another team member's network traffic information in a way that dynamically correlates all this information on the cyber weapons platform so as to confirm or deny the presence of an adversary. Defining these repeatable processes produces the team's set of collective tasks. Further determining which collective tasks are necessary to achieve the core responsibilities of how we fight results in the mission element's METs.

Training the Force

Armed with a standardized definition of the mission-essential tasks, a weapons platform, and a mission element for execution, USCYBERCOM can define an appropriate model to train and objectively assess the effectiveness of the mission element.

USCYBERCOM has assessed readiness through tracking a sequence of individual courses known colloquially as the "training pipeline." The pipeline, however, provides education, not training; it ensures that individuals understand the fundamentals of their responsibilities, but it does not give them experience operating as a mission element on the systems they will use in cyberspace operations. Moving forward, the command needs to define the right mission element–level training requirements, those that support an objective assessment of collective task proficiency. USCYBERCOM plans to mirror crew-qualification models from other domains to ensure a clearly defined minimum standard.

Of equal importance for assessment is the less tangible necessity of raising every mission element to an established measure of proficiency. Without an effective training model, we run the risk of being overly dependent on a small cadre of effective mission elements, while leaving others out of the fight. The command's revised training model ensures that every mission element is capable of fundamental tasks, ultimately increasing the available combat power to meet the ever-increasing demand for cyber forces.

The readiness model for cyberspace operations now mirrors that for every other domain, with adjustments for particular circumstances and requirements. USCYBERCOM organizes and mans its force according to well-defined skill sets, trains the teams according to mission-essential tasks, and equips teams with a weapons platform. Within the model, the command can now objectively assess the unit of action according to metrics. Does the mission element have the right number of personnel? Is the mission

element, collectively, trained to operate the weapons platform according to assigned mission-essential tasks? Does the mission element have a weapons platform? Is the weapons platform fully operational and serviceable? Answering these questions directly aligns the cyber readiness model with readiness as it is understood across the Department of Defense.

Global Integrator of Cyberspace Operations Forces

The president of the United States, through his Unified Command Plan (UCP), has assigned the commander of U.S. Cyber Command responsibilities as the joint force provider and joint force trainer for cyberspace operations forces (COF). Until December 2019 neither the UCP nor DOD policy ever defined "COF," limiting the command's ability to execute its responsibility to establish training and readiness standards across the cyber operations forces. Lacking that clear scope, the command focused first on the CMF teams, a clear subset of COF, as detailed above. With the secretary of defense policy memorandum signed in 2019, the department now has a clear definition of COF. This new definition will be integrated into DOD policy and includes groups such as the subordinate command elements, DOD cybersecurity service providers, and forces purposely organized to execute offensive or defensive cyber operation response actions. This action has set in motion several command efforts to assess the design and readiness of forces and command elements well beyond the teams of the CMF.

Moving forward, USCYBERCOM will also work to establish and standardize manning and training requirements for the two-and-three-star Joint Force Headquarters, with operational control of most of the CMF; the joint mission operations centers, the facilities that host the joint cyberspace operations infrastructure; and the cyberspace operations–integrated planning elements, the joint teams embedded with other combatant command staff to bring cyberspace effects into those plans and orders. The implementation of these requirements will enable USCYBERCOM to conduct the "joint force provider" function of identifying and recommending joint sourcing solutions for cyberspace operations forces. This role makes USCYBERCOM the global integrator for cyber operations forces, responsible for responding to strategic challenges and opportunities on the horizon around the globe. An additional dimension—one that the command is just beginning to understand but will undoubtedly be critical in the future—is the opportunity to include National Guard and Reserve forces into the commander's arsenal.

Policy Shifts to Support Foundational Readiness

The policy decisions that bookend this chapter—the approval of the combatant command force-structure recommendation and the clear definition of COF—represent but two of the changes needed to build sustainable readiness in this domain.

USCYBERCOM has made significant strides by assessing the initial build of the CMF and developing the next phase of the build. The command continues to develop, operate, and gain experience daily. Coupled with a clearer understanding of the full scope of the nation's cyber operations forces, this puts USCYBERCOM well on its path to defining standardization and readiness requirements throughout the cyberspace domain. This will enhance the effectiveness of cyberspace planning and operations, as well as the ability of our cyberspace forces to support, enable, and complement effects delivered in the air, land, sea, and space domains.

Notes

1. Mark A. Milley, "Army Readiness Guidance, Calendar Year 2016–17," official memorandum, Washington, DC, 2016, https://www.army.mil/.
2. U.S. Senate, *Statement of Admiral Michael S. Rogers, Commander, United States Cyber Command, before the Senate Committee on Armed Services,* 115th Cong., Washington, DC, 2018, https://www.armed-services.senate.gov/.
3. A "mission element" is the smallest piece of a Cyber Mission Force team that can execute mission and the readiness of which can be measured.

CHAPTER ELEVEN

The Role of Technology and Innovation in Implementing U.S. Cyber Strategy

PETER DOMBROWSKI AND NINA KOLLARS

New commercial technology will change society and, ultimately, the character of war. The fact that many technological developments will come from the commercial sector means that state competitors and nonstate actors will also have access to them, a fact that risks eroding the conventional overmatch to which our nation has grown accustomed. Maintaining the Defense Department's technological advantage will require changes to industry culture, investment sources, and protection across the national security innovation base.[1]

For great powers in the industrial age, military strength was the product of so-called smokestack and metal-bending industries. Railways, tanks, artillery pieces, trucks, and ships were manufactured in vast factory complexes. Factories produced small arms, uniforms, rations, and munitions to arm, feed, and clothe large armies. But the difference between the materials required to prepare for and fight wars and those produced for commercial sale was relatively small. The factories that could build automobiles could also build trucks of various sorts and even, with conversion of machine tooling and production lines, armored vehicles. Locomotives and ocean liners in military use were not all that different from their respective equivalents that fed domestic consumption or moved exported goods. When there were serious differences, as increasingly was the case with warships, the government produced the military equipment itself in yards and arsenals. When war broke out, mobilization meant essentially expanding and modifying public and private production lines to support the increasing size of forces deployed.

In the information age the relationship between military power and the civilian economy has changed. For many nations, including the United States, the industries that were the backbones of wealth and power in the industrial era are no longer the drivers of economic growth, much less military power. Key industries such as steelmaking and shipbuilding have either migrated offshore or have been greatly transformed. For example, American private shipyards today specialize in high-technology naval warships, while government yards either no longer exist or perform only specialized work, such

as repairs. The shipbuilding industry would be hard-pressed to produce rapidly large numbers of destroyers, much less aircraft carriers, at the onset of war. It would in fact be impossible, given the relative absence of commercial shipyards to construct hundreds of simply designed transports as was done during World War II. Defense requirements today are far more specialized.

The United States, Japan, and most of Europe are increasingly reliant on the information and communications technology (ICT) sectors of their economies.[2] The drivers of each national economy and much of the global economy are not smokestack industries or commodity production. Likewise, contemporary military powers rely heavily on their ICT sectors. This has become especially true over the past three decades as the global economy has shifted and militaries have begun what some have called an "information technology revolution in military affairs" (IT-RMA).[3] One key component of the IT-RMA is the emergence of cyberspace as a warfighting domain.[4] Armies, navies, and air forces increasingly rely on computers, networks, sensors, processing technologies, and telecommunications grids to conduct operations in peacetime and wartime.

The misalignment between the commercial ICT sector and the needs of defense production threatens to diminish the military's capacity for innovation in cyber planning and execution. Whereas in the twentieth century the challenge was to generate the knowledge inputs for an easily aligned defense industrial base, the contemporary challenge for militaries, and in particular in the cyber domain, is to seek new alignments along new standards with an eye toward rapid adaptive change. The challenge is innovation in an environment that changes at the rate of code—far "outside the wheelhouse" of the acquisition community of the Department of Defense (DOD) or of subunits such as U.S. Cyber Command, which is only now achieving independent procurement authority.[5]

This chapter will begin to examine the implications of these challenges for the implementation of U.S. cyber strategies. It will focus on two dimensions: the roles of the commercial technology sectors and the specific demand for cyber innovation. It will conclude that in the long run the competitive balance between the United States and its potential adversaries in the cyber domain will depend largely on the success of the American ICT sectors—with robust, innovative private-sector firms operating at the frontier of technological possibilities—or their failure. If the Department of Defense, U.S. Cyber Command, and the U.S. government as a whole hope to remain ahead of adversaries, they will have to find the means to encourage private-sector engagement and innovation.

Cyber Technology and Innovation in the Trump Administration

The 2017 *National Security Strategy* has made the significance of cyber for the United States clear: "Cyberspace offers state and non-state actors the ability to wage campaigns against American political, economic, and security interests without ever physically crossing our borders."[6] As a result, the summary of the *2018 National Defense Strategy* makes cyber a priority: "We will also invest in cyber defense, resilience, and the continued integration of cyber capabilities into the full spectrum of military operations."[7]

The Trump administration also promised to safeguard "American prosperity by nurturing a secure, thriving digital economy and fostering strong domestic innovation."[8] If the impact of cyberspace on warfare and conflict remains highly contested, its contribution to global, national, and local economic growth and prosperity is almost universally acknowledged. Scholars may quarrel over the extent of the contribution and the mechanisms by which information technologies drive economies, but few question their importance.[9] Moreover, information technologies are viewed as an important factor leading to innovation in all commercial sectors and processes, ranging from scientific research and consumer behavior to management techniques. In short, for modern economies the ICT sectors make cyberspace possible and are thought to constitute an essential ingredient for economic success.[10]

At the global level, as Joseph Nye explains, "the characteristics of cyberspace reduce some of the power differentials among actors, and thus provide a good example of the diffusion of power that typifies global politics in this century."[11] It is possible to remain relatively underdeveloped economically but be powerful in some of the key elements of cyberpower. Take for example the attack on Sony, during which North Korea demonstrated that even a pariah state with sharply limited digital connectivity and sophistication could carry out an attack on the United States. The reluctance by DOD to recognize this implication was remarkably telling: initially "experts challenged the reliability of technical evidence cited by the FBI, questioned North Korean technical competence, and described alternative theories such as a 'false flag' operation impersonating North Korea or even cooperation from disgruntled employees."[12]

This is not to say that traditional great powers and those countries with strong economies are necessarily incapable of retaining dominance in cyberspace. All is not lost. While cyber capabilities are available, to one degree or another, to all actors, state and nonstate alike, great powers can still enjoy advantages, provided they harness the technological prowess and institutional arrangements (public and private) required to exploit the emerging cyber sphere.

But the United States, like other great powers, needs to make the necessary institutional adjustments sooner rather than later if it is to take full advantage of the opportunities

of the information age. To this end, the Trump administration has pledged to "work with the private sector to facilitate the evolution and security of 5G, examine technological and spectrum-based solutions, and lay the groundwork for innovation beyond next-generation advancements."[13] Further, "it will . . . protect America's security and commercial interests by strengthening United States industry's competitive position in the global digital economy."[14] The controversial U.S. efforts to rein in Huawei could be understood as a high-risk opening salvo in an effort to protect American security and commercial interests.[15]

For the United States to have an effective cyber strategy in a world where cyber plays an increasing role in military operations and is a major component of a nation's economy, three things are necessary. First, the United States must recognize that the private sector, not the public sector, is the ultimate driver of cyber capabilities. Second, its government must acknowledge that the private sector is the source of the most innovative technologies—including both hardware and software—required to remain on top of the global-power ranks. Finally, it is incumbent on the U.S. government to develop the private/public arrangements that will allow it to take advantage of the private sector's dominance—in investments, innovations, and human capital. The following pages will first outline the private sector's dominance in cyberspace, examine the nature of innovation in cyberspace, and then consider how the nation might take advantage of American and global private sectors to further its strategic ends.

Private-Sector Dominance in the Information Age

Understanding and interpreting the breadth of the information age economy is difficult, especially in the context of how it affects national security and military capabilities. Even in 2020 definitions remain highly contested. Myriam Dunn Cavelty argues that "eight of the most important technologies of the current internet-enabled scientific-technical revolution are as follows: advanced computing, networking, and semiconductors; cellular/wireless technology; digital transmission/compression; fiber optics; improved human/computer interaction; and satellite technology."[16] Other scholars identify an even broader list of technologies:

> Cyber physical systems combine communications, IT, data and physical elements integrating a number of core technologies:
>
> - Sensor networks (receptors)
> - Internet communication infrastructure (IP)
> - Intelligent real-time processing and event management (CPUs)
> - Actors for mechanical activities
> - Embedded Software for logic

- Big Data and Data Provisioning
- Automated operations and management of system activities
- Advanced Robotics
- 3D/4D Printing[17]

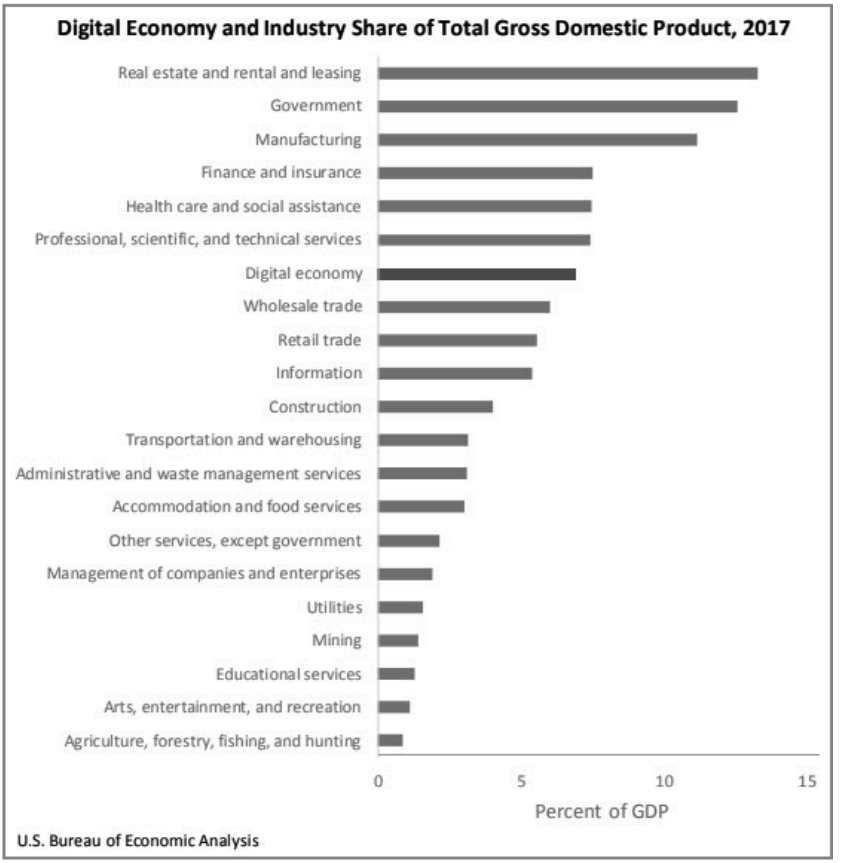
Klaus Schwab characterizes the fourth industrial revolution as a "fusion of technologies that is blurring the lines between the physical, digital, and biological spheres."[18] Related framing from other disciplines includes the knowledge economy, which emphasizes "a greater reliance on intellectual capabilities than on physical inputs or natural resources," and the digital economy of digital-enabling infrastructure, e-commerce transactions, and digital media.[19]

Although the terminologies are contested, all these formulations share a fundamental assumption that the world's economic and technological futures will be driven by the private sector—the inevitable embedding of ICT technologies into economic life, including growth, consumer demand, and product innovation. Although governments may support private-sector actors using industrial policy, regulatory regimes, science and technology and research and development investment, and highly specialized demand signals (for specific noncommercial products), the emerging economy will be driven by private decisions.

Information Age Investment

Measuring how much the United States as a whole or even its government invests in "cyber" is exceedingly difficult; determining how the United States invests compared with its geopolitical competitors is even harder. First, there are many definitional issues: What exactly constitutes "cyber" investment? Second, data collection by the U.S. government has not kept pace with the changing economy. The same holds true, only more so, regarding both global aggregates and transnational descriptive statistics. One rough stand-in is government spending on cybersecurity: "The FY [fiscal year] 2019 President's Budget includes $15 billion of budget authority for cybersecurity-related activities, a $583.4 million (4.1 percent) increase above the FY 2018 [President's Budget]."[20] This total underestimates spending in sensitive accounts and obscures the large growth of Department of Defense expenditures versus those of civilian agencies. Further, of course, cybersecurity is only one dimension of funded cyber activity that, broadly defined, might also include the information grid and the various ICT structures linking and defensive systems intended to support kinetic operations. The Trump administration plans (at this writing) to increase cybersecurity spending further in FY 2020, although figures reported in new accounts are incommensurable.[21]

TABLE 1



One thing is clear, however. Despite the prominence accorded the ICT sectors, they remain a relatively modest portion of the American economy. The U.S. Bureau of Economic Analysis suggests the digital economy represents only 6.9 percent of the entire economy, only seventh out of the twenty-one sectors and well behind government and finance (see table 1).[22]

Firms and Organizations

In the mid-1990s, proponents of the IT-RMA speculated that the United States would rely less and less on traditional defense industries. The proverbial metal-bending industries would be replaced by ICT firms (Microsoft and Cisco, for example) and Silicon Valley start-ups that would break into the defense marketplace. Such predictions proved to be premature. Detailed scholarship has since revealed that traditional defense industries were, and are, far more resilient than that:[23] "Well-established, long-trusted

vendors with core competencies in dealing with the needs of the military will remain in the forefront of [the IT] sector, while potential new competitors from the IT world will generally remain subcontractors."[24] Defense industrial firms, especially prime contractors such as Lockheed Martin, Boeing, and BAE Systems, proved remarkably robust at the onset of the IT-RMA, twenty years ago. They possessed structural, political, and cultural advantages over potential new entries into the defense sector. It was their business to understand the requirements of the military and the baroque acquisition processes and laws that govern defense procurement. They had long cultivated access to international markets and now relentlessly exploited them, with the assistance of American officials. Industry experts watched security-related developments closely to understand the changing nature of warfare and thus the ways in which the U.S. military would seek to arm itself over the medium-to-long term.

However, we may finally be seeing the emergence of new actors in the defense sector, especially with regard to cyber capabilities. Moreover, firms that have specialized in building platforms (for example, ships, aircraft, and military vehicles) are now transitioning toward IT-centric lines. From the early days of USCYBERCOM traditional defense contractors such as Grumman and Lockheed Martin were reportedly vying with information technology companies such as CACI International, Symantec, and McAfee for contracts with the new command.[25] More recently, between FY 2011 and FY 2016, the six firms with more than a billion dollars in federal contracts for various aspects of cybersecurity and operations were Leidos, Northrop Grumman, Booz Allen Hamilton, IBM, Hewlett Packard, and General Dynamics. The next-tier firms—Dell, SAIC/Leidos, CSRA, CACI, Lockheed Martin, Harris, and Raytheon—earned hundreds of millions of dollars.[26] While most of these are long-term government contractors, many (including Raytheon, Northrop Grumman, and Lockheed Martin) have either acquired firms specializing in cyber or built divisions focused on cyber and other ICT arenas over the last decade. Raytheon, for example, made a big bet on cyber in the mid-2010s—it acquired fourteen cyber-related firms, including Forcepoint.[27]

Global Markets

Martin Libicki has argued that the American IT sector has supported American military, political, and economy primacy in telecommunications and information processing for generations. American firms pioneered many of the key technologies and processes that enable global modern information networks. Such firms as IBM, Apple, Cisco, Google, Facebook, and Amazon are collectively the gold standard internationally. For the most part they lead global markets with technologies and systems. Their customers and clients number in the billions and are found everywhere on the globe. American intelligence agencies have exploited the centrality of American firms in global

communications and commerce to an extent long known but seldom acknowledged.[28] The National Security Agency and other U.S. intelligence entities have routinely cooperated with American and other telecommunication firms to eavesdrop on all manner of communications.

In the last decade, Chinese and, to a lesser extent, European firms have risen to challenge American firms. Huawei has emerged as a direct challenge to American IT dominance globally. With a unique business model built on China's vast domestic market, state support for growth and investment through preferential financing, and a deliberate, considered choice to pursue indigenous intrafirm technology and product development, it has earned a large share of the world marketplace.

Meanwhile, the relative importance of the United States and other OECD (Organisation for Economic Co-operation and Development) countries to global trade in ICT goods and services has diminished over the last decade. China exports increased by 49 percent from 2008 to 2015, while those of the OECD decreased by 15 percent (see table 2). On the other hand, while China remains one of the top ten exporters of ICT services, it continues to lag its OECD competitors (table 3).

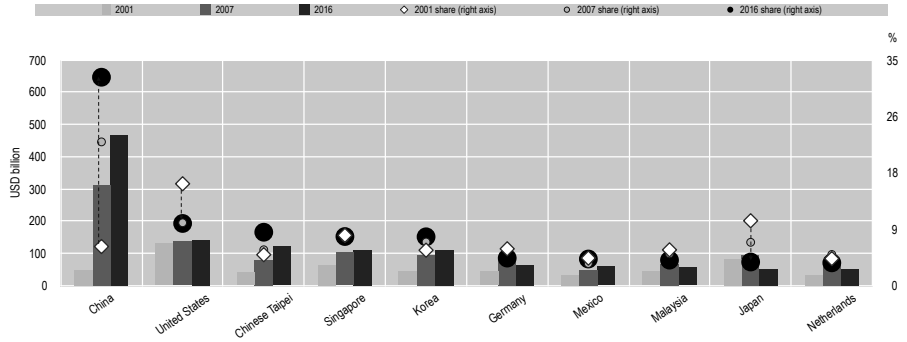
The global ICT service trade is growing, with OECD leading the way but China, at least in terms of goods, including telecommunications systems, growing even faster. The ability of the United States to remain dominant over or even keep pace with economic competitors (and potential military adversaries) like China may be eroding. If it is true that the capabilities of the United States to implement a successful cyber strategy in the short and long terms rely on American firms, technologies, and exports, these are worrisome trends.[29]

Buying Cyber Innovation

Given the diminishing OECD lead in global ICT and the misalignment of industry with direct application to defense acquisitions, it is unclear whether and how an effective cyber strategy might be achieved. In the long run the dominance of the U.S.-based commercial ICT sectors is not guaranteed, and the ability of the government to develop usable systems and cyber instruments remains in question. In the interim, more-innovative thinking is required.

Ultimately what is needed is change. If that cannot be provided by the systems that have previously assured U.S. military dominance, then we must look elsewhere—if only in the medium term—for solutions. The rhetorical term of art for thinking about systems change in business, military acquisition, and academic discourse is "innovation."[30] Innovation, generically, is the implementation of new processes and products to achieve new gains. Within DOD, however, the use of the word itself speaks to core

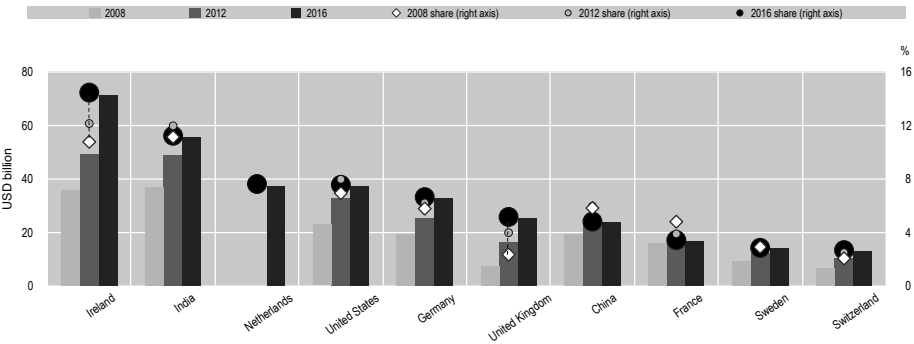
TABLE 2
Top Ten World Exporters of ICT Goods



Notes: World is estimated adding up all declaring economies that reported ICT exports in all three years; world excludes reimports for the People's Republic of China ("China" in the figure) and reexports for Hong Kong, China. China's ICT exports are adjusted for reimports. 2016 data for China and the Netherlands are estimates based on reported values in 2015.

Source: OECD, "STAN bilateral trade database by industry and end-use category. ISIC Rev. 4," *STAN: OECD Structural Analysis Statistics* (database), http://oe.cd/btd (accessed July 2017).

TABLE 3
Top Ten World Exporters of ICT Services



Notes: ICT services are defined here as telecommunications, computer, and information services. China = the People's Republic of China.

Source: UNCTAD, "Services (BPM6): Exports and imports by service-category, shares and growth, annual, 2005–2016," http://unctadstat.unctad.org/wds/TableViewer/tableView.aspx?ReportID=87017 (accessed June 2017).

American military beliefs regarding the link between "thinking forward" in terms of technology and the ongoing global political interactions between states and their subunits. Thus, there exists an entire separate academic field of research, commonly referred to as "military innovation," that posits theories regarding how and through what variables change can occur for militaries, as distinct from markets, firms, and the global economy. There are two general orientations within its literature. One is outward facing and based on military effects—some variable introduced by one force produces victories over another.[31] The other is based on an internal dynamic—some new variable creates

change in the doctrine, organization, training, matériel, leadership, personnel, facilities, policy, or the entirety of an agency or department.[32] Both internal- and external-facing approaches are necessary to understanding the process of change for militaries—one explains the factors that spur militaries to want to change, the other the processes that must take place if change is to become institutionalized.

What is still lacking, however, for our purposes, is alternative models or theories that connect private-sector solutions to military problems. To that end, in the fall of 2018 came out the *2018 National Defense Strategy,* which laid down eleven defense objectives, including "establishing an unmatched twenty-first century National Security Innovation Base [NSIB] that effectively supports Department operations and sustains security and solvency."[33] Although the *National Defense Strategy* does not define the NSIB, it appears (the list is elusive) to point to the components of the U.S. private, commercial sector responsible for technological advancements—presumably including Silicon Valley's tech-centric start-up community. As a rubric, the NSIB has had only one real advocate, the Reagan National Defense Forum, and has otherwise received almost no follow-on attention.[34] This neglect is presumably due in part to the buzz-phrase saturation of Washington, DC; it is also a result of the murky nature of the relationships between the dot-mil (military), dot-gov (government), and dot-com (business) environments. We believe that for the NSIB concept to be effective as part of the national security endeavor, it must be made to recouple the industrial production elements that fell out of alignment at the end of the last century or to fashion de novo an alternative system.

Ultimately, the national security innovation base has very few qualities in common with the defense industrial base. From a systemic perspective, the chief advantage of its difference is that the defense industrial base is innately bound up in the Federal Acquisition Regulation system. The NSIB need not be the same. Therefore, from the NSIB could likely emerge the kind of meaningful cultural changes needed to create the innovative agility necessary to deal with state and nonstate cyber threats, resolve critical infrastructure vulnerabilities (commonly and generically referred to as "cyber threats") associated with digital connectivity, and manage the DOD Information Network's own cyber vulnerabilities. We offer below some potential models of how that relationship might be developed.

Toward Innovation for Cybersecurity: Two Pathways

Innovation in military acquisition is an oxymoron in most circles, but it is the aspect of cyber implementation that matters most. What is needed is alternative vehicles for acquiring and developing our cyber assets and platforms in a way that capitalizes on the naturally agile, fail-fast model of Silicon Valley. There exist, contrary to criticism, several methods of agile development and acquisition around which a reasonable acquisitions

strategy might be built. We categorize these as internal and external to DOD. We offer these examples not necessarily as fully successful but rather as paths along which to investigate further models that might produce a successful strategy for maintaining and leveraging our NSIB.

Internal-to-DOD Innovation: Making Use of Expertise

An alternative model leverages the expertise of the people already in DOD jobs. That is, the everyday insights of existing talent can be leveraged to make organizational as well as technological advances. The Air Force's Kessel Run is just one version of this.[35] Kessel Run brings people inside the government who know their systems well together with coders from both inside and outside DOD to resolve bottlenecks in development and implementation. The brilliance of Kessel Run is that it manages to connect operators within the services to external support to solve existing problems without an extensive contracting process. This saves the department money but more importantly time. Kessel Run, when a nascent and unproven program, nearly died several times, but now it has the unwavering support of the Air Force and will likely continue to produce software at a much-appreciated pace. Kessel Run is an example of a highly adaptive mechanism for writing and rewriting code, something desperately needed for updating DOD systems. Ultimately, the advantage of utilizing internal DOD perspectives is that they can lead to simple shifts that make immediate impacts. The disadvantage of programs like Kessel Run is that they lack the "innovative" long-sighted future-software vision. Such programs are innovations in themselves but are unlikely to come up with paradigm-shifting software that will meet the demands of emerging technology and increasingly forward-leaning, technologically adept adversaries. Kessel Run produces solutions for problems we already know we have; thus it is only part of the solution for a robust NSIB.

For internal models to be successful in making more than incremental shifts to efficiency, Kessel Run and the like will need more exposure to the private sector's thinking. The good news is that many of the most talented minds in cybersecurity are former employees of the National Security Agency and U.S. Cyber Command. Those former DOD employees have the benefit of understanding government systems but also a broader exposure to the less-constrained thinking of the private sector. Reaching out to those former employees may make sense in designing cybersecurity for future systems.

The United Kingdom already has such a model, in the National Cyber Security Centre's Industry 100 program. Industry 100 selects leading private-sector firms and invites them to help resolve government cyber issues over several months with no implied payment or contracts thereafter. Leading private-sector firms have responded with enthusiasm thus far, agreeing to allow their experts to remain on salary while working

toward a stronger, more secure internet for the United Kingdom.[36] Industry 100 does not require the aid of former defense employees, but if this model is to work in the United States, given sensitivities and classification issues here, it may need to solicit such aid, at least at first.

External-to-DOD Innovation: Moving the Risk/Liability Calculus from Things to People

One technique that the Defense Department's intelligence agencies have attempted to utilize is making early bets on emerging technological trends in Silicon Valley. DOD has its "own" venture-capital entity (In-Q-Tel) that can invest early in products or small start-ups with potentially useful hardware or software.[37] The key advantage to the venture-capital model is that early buy-in permits DOD to shape the trajectory of the technology's implementation and increase the odds that a reasonable application can be built for defense should the investment yield a product. In-Q-Tel is a privately held, not-for-profit venture-capital firm that provides cutting-edge, mature technologies to the Central Intelligence Agency and Defense Department intelligence agencies.

There is an important distinction to be made with respect to venture-capital funding. The Defense Department's technology development and acquisition process already sees itself benchmarking funding against the "promise" of a technology—in accordance with its own requirements process. But venture-capital models broaden the scope to invest in more than potential technologies. They also invest in the people operating the start-ups.

While investing in technological promise is likely more comfortable in the defense arena, its compliance with current acquisitions laws being well established, the second model is already common in the private sector. Elon Musk, Bill Gates, and Steve Jobs are household names, and in the private sector trust is often driven by the reputation of the person rather than putative merits of the product. Investing in people shifts the risk to the creativity of the person. To be clear, In-Q-Tel positions itself less as a venture-capitalist firm investing in people than as a claim verifier and matchmaker between promising start-ups and the needs of U.S. intelligence agencies.[38] Thus, as seemingly radical initiatives go, it is somewhat conservative. However, follow-on attempts to emulate venture-capital models for defense could be more accepting of risk.

In fact, historically speaking, the U.S. Department of Defense has a long history of making bets on people rather than their products. In the post–World War II years and the Cold War, the strategy for developing innovative weapons emerged through people-centered talent management, not things-based purchasing. The United States resolutely funded the research of the leading scientists without specific promise of product. People like Richard Feynman, Norbert Wiener, and Claude Shannon were men

with reputations for bizarre, near-lunatic behavior and radicalism.[39] They were also the leading minds in the creation of the technologies of the current era—microcomputing, communications, and quantum theory.

Programs like In-Q-Tel allow the government to access such minds, at a distance. Moreover, the challenge the United States now faces in choosing whom to fund is perhaps easier than it was in the era of the Feynmans and Shannons. According to American artificial intelligence expert Kai-Fu Lee, who operates in China, the inherent strength of that nation's advantage in developing artificial intelligence is not that it pushes science forward but that it pushes solutions out through as many outlets as possible.[40] The question is less what emerging science to invest in but who has the best reputation for applying and implementing that science. Thus, the challenge, at least for current hardware and software innovation, lies in implementation.[41] Insofar as this is the case, investing in people with proven track records of effective implementation of existing innovations is less risky than trying to peer into the minds of wild-eyed geniuses with crazy ideas. This is precisely how most of the world came to know Gates and Jobs (Musk is perhaps a different case); they were thought to be leaders on all the ways in which new software could be implemented across hundreds of products. Investing in persons permits the government to invest at scale rather than piecemeal in a few painfully chosen and shepherded projects.

Conclusions

Efforts to understand the changing relationship between economies and military power in the information age remain in the early stages.[42] Unfortunately, many scholars "ignore the economic roots of power."[43] Perhaps even worse, when it comes to cyberspace or what we call the digital economy some national security analysts do the opposite: they assume the overwhelming importance of the digital economy to the health of the U.S. national economy and, by extrapolation, the global economy. ICT industries are viewed as drivers, and nurturing, protecting, and building them up as essential aspects of geoeconomic competition with our global rivals. This view ignores what some economists identified early on, that "despite the exponential growth in computing power, economic growth remains comparatively sluggish."[44]

To be sure, from the perspective of innovation and new models of production neither the internal nor the external model of potential private-sector partnering is a particularly robust solution to what is a systemic misalignment in a global marketplace wherein our great-power adversaries are better positioned than we and have much larger labor bases. Both solutions merely tinker around the edges and attempt to maintain the illusion that DOD dominance in technology can continue to funnel the benefits of private-sector production directly into defense capabilities. Defense, however, cannot ignore that those same capabilities (albeit perhaps slightly less powerful or rugged) are

being made available in the marketplace to anyone with an Amazon Prime account. The point is that states used to be able to harness systemic production alignments to produce leap-ahead technologies or to exert some semblance of control. At the current rate of development in technology, however, states can at best hope for a "Red Queen's race."[45] That is, even the most agile of states can expect only to keep up with the software and hardware change that pulses daily throughout the global system. More research and theory are needed for thinking beyond the implementation rush of the next decade toward the inevitable next round of big breakthroughs.

In this chapter we have begun exploring the relationship between two major dimensions of cyberspace as it relates to U.S. national security strategy: the macroeconomy and innovation. We believe that much work needs to be done, and we hope to join with other scholars and analysts sorting through the myriad of issues raised above. Among the important and outstanding questions that remain are these: Is the U.S. information technology sector up to the challenge of supporting an information age military? And can the American military, or even the government as a whole, draw on the private sector in ways that match in effectiveness those of our great-power competitors?

Notes

1. Department of Defense [hereafter DOD], *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Washington, DC, 2018), p. 3 [hereafter *Summary DOD NDS 2018*], https://dod.defense.gov/.
2. Makada Henry-Nickie, Kwadwo Frimpong, and Hao Sun, "Trends in the Information Technology Sector," *Brookings,* 29 March 2019, https://www.brookings.edu/.
3. For an excellent overview of the IT-RMA, see Dima Adamsky and Kjell Inge Bjerga, "Introduction to the Information-Technology Revolution in Military Affairs," *Journal of Strategic Studies* 33, no. 4 (2010), pp. 463–68.
4. Although whether cyber is in fact a domain like air, land, or sea has been contested. See Peter Dombrowski and Chris C. Demchak, "Cyber War, Cybered Conflict, and the Maritime Domain," *Naval War College Review* 67, no. 2 (Spring 2014), pp. 71–96; and Martin C. Libicki, "Cyberspace Is Not a Warfighting Domain," *I/S: A Journal of Law and Policy for the Information Society* 8, no. 2 (2012), pp. 321–35.
5. Aaron Boyd, "Defense Acquisition Reform Panel Suggests Reevaluating Department CIO," *Nextgov,* 15 January 2019, https://www.nextgov.com/.
6. *National Security Strategy of the United States of America* (Washington, DC: White House, December 2017), p. 12, www.whitehouse.gov/.
7. *Summary DOD NDS 2018,* p. 6.
8. *National Cyber Strategy of the United States of America* (Washington, DC: White House, September 2018), unpaginated cover letter, https://www.whitehouse.gov/.
9. Bart van Ark, "The Productivity Paradox of the New Digital Economy," *International Productivity Monitor,* no. 31 (Fall 2016).
10. Much of the relevant literature begins with Erik Brynjolfsson and Lorin M. Hitt, "Beyond Computation: Information Technology, Organizational Transformation and Business Performance," *Journal of Economic Perspectives* 14, no. 4 (Fall 2000), pp. 23–48.
11. Joseph S. Nye Jr., *The Future of Power* (New York: PublicAffairs, 2011), p. 150.

12. Stephan Haggard and Jon R. Lindsay, "North Korea and the Sony Hack: Exporting Instability through Cyberspace," *AsiaPacific Issues,* no. 117 (May 2015), p. 3.
13. *National Cyber Strategy,* p. 15.
14. Ibid., p. 25.
15. Lorand Laskai, "Why Blacklisting Huawei Could Backfire: The History of Chinese Indigenous Innovation," ForeignAffairs.com, 19 June 2019.
16. Myriam Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (London: Routledge, 2007), p. 19.
17. John Moavenzadeh, "The 4th Industrial Revolution: Reshaping the Future of Production" (presentation, DHL Global Engineering & Manufacturing Summit, Amsterdam, 7 October 2015), https://www.eiseverywhere.com/file_uploads/fe238270f05e2dbf187e2a60cbcdd68e_2_Keynote_John_Moavenzadeh_World_Economic_Forum.pdf.
18. Klaus Schwab, "The Fourth Industrial Revolution: What It Means, How to Respond," *Global Agenda* (blog), *World Economic Forum,* 14 January 2016, https://www.weforum.org/.
19. Walter W. Powell and Kaisa Snellman, "The Knowledge Economy," *Annual Review of Sociology* 30 (2004), pp. 199–220; "Digital Economy," *BEA* [Bureau of Economic Analysis], last modified 11 March 2020, https://www.bea.gov/.
20. Office of Management and Budget, *A Budget for America's Future: Analytical Perspectives—Fiscal Year 2021* (Washington, DC: U.S. Government Publishing Office, 2020), pp. 273–87, https://www.whitehouse.gov/.
21. Aaron Boyd, "Trump's 2020 Budget Requests about $11 Billion for Cyber Defense and Operations," *Nextgov,* 11 March 2019, https://www.nextgov.com/.
22. "Digital Economy Accounted for 6.9 Percent of GDP in 2017," *NTIA Blog, National Telecommunications and Information Administration,* 5 April 2019, https://www.ntia.doc.gov/blog/.
23. Peter Dombrowski and Eugene Gholz, *Buying Military Transformation: Technological Innovation and the Defense Industry* (New York: Columbia Univ. Press, 2006).
24. Peter J. Dombrowski, Eugene Gholz, and Andrew L. Ross, "Selling Military Transformation: The Defense Industry and Innovation," *Orbis* 46, no. 3 (Summer 2002), p. 535, https://doi.org/10.1016/S0030-4387(02)00122-9.
25. "Pentagon Plans New Cyberspace War Command: Report," Reuters, 29 May 2009, https://www.reuters.com/.
26. Shaun Waterman, "Six Big Vendors Dominate a Fragmented Federal Cyber Market, Numbers Show," *Cyberscoop,* 20 April 2017, https://www.cyberscoop.com/.
27. Ross Wilkers, "How Raytheon's Big Cyber Bet Is Paying Off," *Washington Technology,* 3 June 2017, https://washingtontechnology.com/.
28. James Bamford, *The Shadow Factory: The Ultra-secret NSA from 9/11 to the Eavesdropping on America* (New York: Anchor, 2009), esp. pp. 161–270.
29. *OECD Digital Economy Outlook 2017* (Paris: OECD, 2017), esp. pp. 121–25, https://www.oecd-ilibrary.org/.
30. See Geoffrey Parker, *The Military Revolution: Military Innovation and the Rise of the West, 1500–1800,* 2nd ed. (Cambridge, U.K.: Cambridge Univ. Press, 1996); Williamson R. Murray and Allan R. Millett, eds., *Military Innovation in the Interwar Period* (Cambridge, U.K.: Cambridge Univ. Press, 1998); Adam Grissom, "The Future of Military Innovation Studies," *Journal of Strategic Studies* 29, no. 5 (October 2006), pp. 905–34; and Peter Dombrowski and Eugene Gholz, "Identifying Disruptive Innovation: Innovation Theory and the Defense Industry," *Innovations: Technology, Governance, Globalization* 4, no. 2 (Spring 2009), pp. 101–17.
31. This view is associated largely with historians, as well as some social scientists. For example, see John Keegan, *The Face of Battle* (New York: Viking, 1976); William H. McNeill, *The Pursuit of Power: Technology, Armed Force, and Society since A.D. 1000* (Chicago: Univ. of Chicago Press, 1982); Williamson Murray, "Thinking about Revolutions in Military Affairs," *Joint Force Quarterly* 16 (Summer 1997), pp. 69–76; and Parker, *Military Revolution*.
32. This more contemporary turn is largely represented by an abundance of social scientists. For example, see Theo Farrell and Terry Terriff, *The Sources of Military Change: Culture, Politics, Technology* (Boulder, CO: Lynne Rienner, 2002); Grissom, "Future of Military Innovation Studies"; Jon R. Lindsay, "'War upon the Map': User Innovation in American

Military Software," *Technology and Culture* 51, no. 3 (July 2010), pp. 619–51; and Kristen A. Harkness and Michael Hunzeker, "Military Maladaptation: Counterinsurgency and the Politics of Failure," *Journal of Strategic Studies* 38, no. 6 (2015), pp. 777–800.

33. *Summary DOD NDS 2018,* p. 4.
34. Aaron Mehta and Joe Gould, "Here Are Five Ambitious Steps to Grow the Defense Innovation Base and Challenge China," *Defense News,* 5 December 2019, https://www.defensenews.com/.
35. Mark Wallace, "The U.S. Air Force Learned to Code—and Saved the Pentagon Millions," *Fast Company,* 5 July 2018, https://www.fastcompany.com/.
36. "Industry 100," *National Cyber Security Centre,* reviewed 19 December 2019, https://www.ncsc.gov.uk/.
37. *IQT | In-Q-Tel,* accessed 10 April 2020, https://www.iqt.org/; Noah Shachtman, "Exclusive: Google, CIA Invest in 'Future' of Web Monitoring," *Wired,* 28 July 2010, https://www.wired.com/.
38. "How We Work," *IQT | In-Q-Tel,* accessed 25 February 2020, https://www.iqt.org/.
39. Shannon would spend hours staring at clouds; Feynman was known to pick locks and go through his colleagues' papers; Wiener, barely eighteen when he finished his PhD, was widely known to be defiant to the point of radicalism regarding work with the military. Richard P. Feynman, Robert B. Leighton, and Matthew Sands, "The Feynman Lectures on Physics, Vol. I," *American Journal of Physics* 33, no. 9 (September 1965), pp. 750–52; Norbert Wiener, *The Human Use of Human Beings: Cybernetics and Society* (Boston: Houghton Mifflin, 1950), p. 71; Claude Elwood Shannon, "A Mathematical Theory of Communication," *Bell System Technical Journal* 27, no. 3 (July 1948), pp. 379–423.
40. Kai-Fu Lee, "Why China Can Do AI More Quickly and Effectively than the US," *Wired,* 23 October 2018, https://www.wired.com/.
41. Ibid.
42. For an early attempt that remains useful see Emily O. Goldman and Leo J. Blanken, "The Economic Foundations of Military Power," in *Guns and Butter: The Political Economy of International Security,* ed. Peter J. Dombrowski (Boulder, CO: Lynne Rienner, 2005), pp. 35–54, esp. pp. 38–42.
43. Norrin M. Ripsman, "False Dichotomies: Why Economics Is High Politics," in Dombrowski, *Guns and Butter,* pp. 5–44.
44. T. D. Stanley, Hristos Doucouliagos, and Piers Steel, "Does ICT Generate Economic Growth? A Meta-regression Analysis," *Journal of Economic Surveys* 32, no. 3 (July 2018), p. 3.
45. This is a reference to Lewis Carroll's *Through the Looking Glass:* Alice, though she runs faster and faster, cannot win but only keep up. See "The Red Queen Effect: Avoid Running Faster and Faster Only to Stay in the Same Place," *Mental Models* (blog), *Farnam Street,* accessed 25 February 2020, https://fs.blog/2012/10/the-red-queen-effect/.

About the Contributors

Dr. Erica Borghard is a Resident Senior Fellow with the New American Engagement Initiative in the Scowcroft Center for Strategy and Security at the Atlantic Council. Previously, she was an Assistant Professor in the Army Cyber Institute at the U.S. Military Academy at West Point. During that time, Erica also served as the Senior Director and Lead, Task Force One, for the U.S. Cyberspace Solarium Commission. Erica's research focuses on cyber strategy, policy, and operations, and she has published in numerous peer-reviewed academic journals, policy forums, and media and think-tank outlets. Prior to her position at the Army Cyber Institute, Erica was a Council on Foreign Relations International Affairs Fellow, spending the 2017–18 academic year on the Global Cyber Partnerships and Government Strategy team at JPMorgan Chase and at the Cyber National Mission Force at U.S. Cyber Command. From 2014 until 2017, Erica served as an Assistant Professor in and executive director of the Rupert H. Johnson Grand Strategy Program in the Department of Social Sciences at West Point. Erica's coauthored book *Escalation Dynamics in Cyberspace* will be published in 2021 by Oxford University Press's Bridging the Gap series. She is also currently editing a book volume on the research behind the Cyberspace Solarium Commission, as well as writing her forthcoming book on proxy warfare. Erica holds a PhD in Political Science from Columbia University. She is a term member at the Council on Foreign Relations and an adjunct research fellow at the Saltzman Institute of War and Peace Studies at Columbia University.

Dr. Chris Demchak is the U.S. Naval War College's Grace M. Hopper Chair of Cyber Security and Senior Cyber Scholar, Cyber and Innovation Policy Institute (CIPI)—formerly the Center for Cyber Conflict Studies (C3S), which she cofounded and directed. Her research and many publications address global cyberspace as a globally shared, complex, insecure "substrate" underlying the critical organizations of digitized societies, creating "cybered conflict" and in turn a rising "Cyber Westphalia" of sovereign competitive complex socio-technical-economic systems (STESs) and inducing an urgent survival need for a "Cyber Operational Resilience Alliance" (CORA) among advanced democratic allies. Demchak takes a systemic approach in focusing on emergent structures; comparative institutional evolution; adversary/defensive use of systemic cybered tools and all of cyber's offspring, such as AI/ML and autonomous systems; and virtual worlds / gaming for operationalized organizational learning; and on the modeling of systemic resilience ("cybered conflict model") against normal or adversary-imposed

surprises that disrupt or disable large-scale national systems. Having studied the LISP programming language, as well as serving as a military officer, she has taught international security studies and management, comparative organization theory, enterprise information systems, and cybersecurity for international/national security issues. Recent articles include "The Four Horsemen of AI" (in Wright, ed., *Artificial Intelligence, China, Russia, and the Global Order,* 2019) and "'Sea-Hacking' Sun Tsu: Deception in Global AI/Cybered Conflict and Navies" (in Tangredi, ed., *AI at War,* forthcoming 2021). Recent books include *Designing Resilience* (2010 coedit); *Wars of Disruption and Resilience* (2011); and two manuscripts in production tentatively entitled *Cyber Westphalia: States, Economics, Security, and Resilience in Cybered Global Systems Conflict,* and *Cyber Command: Organizational Experiments in National Cyber Defense.*

Dr. Peter Dombrowski is the William D. Ruger Chair of National Security Economics in the Strategic and Operational Research Department at the Naval War College. Previous positions include chair of the Strategic Research Department, director of the Naval War College Press, editor of the *Naval War College Review,* coeditor of *International Studies Quarterly,* Associate Professor of Political Science at Iowa State University, and defense analyst at ANSER, Inc. He has also been affiliated with research institutions including the East-West Center, The Brookings Institution, the Friedrich Ebert Foundation, and the Watson Institute for International Studies at Brown University, among others. Dr. Dombrowski is the author of over sixty-five books, monographs, articles, book chapters, and government reports. Awards include a Chancellor's Scholarship for Prospective Leaders from the Alexander von Humboldt Foundation, the Navy Meritorious Civilian Service Medal, and the Navy Distinguished Civilian Service Medal. He received his BA from Williams College and an MA and PhD from the University of Maryland.

Maj. William Garvey, U.S. Air Force, is the Information Warfare Branch Chief, 616th Operations Center, Joint Base San Antonio–Lackland, Texas. Previously he was Executive Officer to the Commander, Cyber National Mission Force. Major Garvey was commissioned through the Air Force Reserve Officer Training Corps. He has a BA from the University of Michigan and an MA from American Military University.

Dr. Emily Goldman serves as a strategist at U.S. Cyber Command and a thought leader on cyber policy. She was cyber advisor to the Director of Policy Planning at the Department of State, 2018–19. From 2014 to 2018 she directed the U.S. Cyber Command / National Security Agency Combined Action Group, reporting to a four-star commander and leading a team that wrote the 2018 U.S. Cyber Command command vision, *Achieve and Maintain Cyberspace Superiority.* She has also worked as a strategic communications advisor for U.S. Central Command and for the Coordinator for Counterterrorism at the State Department. She holds a doctorate in Political Science from Stanford University and was a Professor of Political Science at the University of California, Davis, for

two decades. Dr. Goldman has published and lectured widely on strategy, cybersecurity, arms control, military history and innovation, and organizational change.

Lt. Gen. Timothy D. Haugh is the Commander, Sixteenth Air Force; Commander, Air Forces Cyber; and Commander, Joint Force Headquarters–Cyber, Joint Base San Antonio–Lackland, Texas. Lieutenant General Haugh is responsible for more than 44,000 personnel conducting worldwide operations. The general leads the global information warfare activities spanning cyberspace operations, intelligence, targeting, and weather for nine wings, one technical center, and an operations center. Previously, he was commander of the Cyber National Mission Force, where he coordinated the prevention and response to cyber incidents and campaigns perpetrated by threat actors to preserve U.S. critical infrastructure and key resources. Lieutenant General Haugh is a graduate of Lehigh University in Bethlehem, Pennsylvania, and holds master's degrees from Southern Methodist University, the Naval Postgraduate School, and the Industrial College of the Armed Forces.

Dr. Nina Kollars is an associate professor of the Strategic and Operational Research Department of the Naval War College and a core faculty member in the Cyber and Innovation Policy Institute (CIPI). She holds a PhD in political science from The Ohio State University, a master's in international affairs from the Elliott School at George Washington University, and a bachelor's from the College of Saint Benedict / Saint John's University. Kollars conducts research in cybersecurity, future-warfare concepts, and military technological integration, specifically the methods and networks through which "white hat" hackers produce security at the national and global levels. Her forthcoming manuscript title "Trustworthy Deviant" leverages more than four years of research in and around the U.S. hacking community. She is a senior adjunct fellow of the Center for a New American Security; a Senior Advisor for the Cyberspace Solarium Commission; and a fellow of the Brute Krulak Center at Marine Corps University. She is also a certified bourbon steward.

MSgt. Ryan Lemmerman, U.S. Air Force, is attending the National Intelligence University in the Master of Science and Technology Intelligence program. Previously he was an Exploitation Analyst for the Cyber National Mission Force (CNMF), in which capacity he planned and executed cyber operations to defeat malicious cyber threats.

Dr. Shawn Lonergan is a senior director in the Cybersecurity, Privacy, and Forensics Practice at PricewaterhouseCoopers. Shawn is also a major in the U.S. Army Reserve, assigned to the 75th Innovation Command, the Reserve component for Army Futures Command. Additionally, Shawn served as a senior advisor to the U.S. Cyberspace Solarium Commission. While on active duty, Shawn assumed multiple leadership positions in the Cyber National Mission Force at U.S. Cyber Command. Prior to that, from 2014

to 2017 he served as an assistant professor in the Department of Social Sciences and as Chief Research Scientist in the Army Cyber Institute. Previously, Shawn helped the U.S. Army stand up its first provisional cyber battalion. In this capacity, he commanded two of the unit's expeditionary cyber operations companies and held leadership positions within the National Security Agency's office of Tailored Access Operations. Shawn also worked in signals intelligence in forward-deployed environments, including during a tour in Iraq in 2007–2008. Shawn holds a PhD in political science from Columbia University. Shawn is a term member of the Council on Foreign Relations and is a Certified Information Systems Security Professional.

Gen. Paul M. Nakasone, U.S. Army, assumed his present duties as Commander, U.S. Cyber Command and Director, National Security Agency / Chief, Central Security Service in May 2018. He previously commanded U.S. Army Cyber Command, from October 2016 until April 2018. General Nakasone is a graduate of Saint John's University in Collegeville, Minnesota, where he received his commission through the Reserve Officers' Training Corps. General Nakasone has held joint and Army command and staff positions across all levels of the Army, with assignments in the United States, the Republic of Korea, Iraq, and Afghanistan. General Nakasone commanded the Cyber National Mission Force at U.S. Cyber Command. He has also commanded a company, battalion, and brigade and has served as the senior intelligence officer at the battalion, division, and corps levels. His most recent overseas posting was as the Director of Intelligence, J2, International Security Assistance Force Joint Command, in Kabul, Afghanistan. General Nakasone has also served on two occasions as a staff officer on the Joint Chiefs of Staff. General Nakasone is a graduate of the U.S. Army War College, the Command and General Staff College, and Defense Intelligence College. He holds graduate degrees from the U.S. Army War College, the National Defense Intelligence College, and the University of Southern California.

Vice Adm. Nancy A. Norton, U.S. Navy, is the commander of the Joint Force Headquarters–Department of Defense Information Network (JFHQ-DODIN) and director of the Defense Information Systems Agency (DISA). As the Commander, JFHQ-DODIN, Vice Admiral Norton directs and synchronizes defensive cyberspace activities, providing unity of command and unity of effort across the Department of Defense. As Director, DISA, Vice Admiral Norton manages a global network and leads more than eight thousand military and civilian personnel who plan, develop, deliver, and operate joint, interoperable command-and-control capabilities and defend an enterprise infrastructure in more than forty-two countries. Vice Admiral Norton, a native of Oregon, graduated from Portland State University with a bachelor's degree in general science. She was commissioned in 1987 through the Navy Officer Candidate School. She holds master's degrees in computer science from the Naval Postgraduate School and in

national security and strategic studies from the Naval War College, where she was the President's Honor Graduate. She served as a fellow on the Chief of Naval Operations (CNO) Strategic Studies Group XXXII. Vice Admiral Norton has served in information warfare billets at all levels, afloat and ashore. Her assignments include naval communications stations in Hawaii and Nevada, as well as command in Bahrain. She developed cybersecurity programs on the staffs of U.S. Pacific Command and Pacific Fleet. She directed communications for Cruiser Destroyer Group 12 on board USS *Enterprise* (CVN 65) and for the U.S. Sixth Fleet and Naval Forces Europe. She served as Director, Command, Control, Communications and Cyber, U.S. Pacific Command. She also served multiple tours for the Office of the Chief of Naval Operations, including as the Director of Warfare Integration for Information Warfare. Prior to her current assignment, Vice Admiral Norton was the vice director of DISA.

Dr. Joshua Rovner is an associate professor in the School of International Service at American University; codirector of American University's Center for Security, Innovation, and New Technology; and managing editor, *H-Diplo International Security Studies Forum*. He served as scholar in residence at the National Security Agency and U.S. Cyber Command in 2018 and 2019. He is the author of *Fixing the Facts: National Security and the Politics of Intelligence* (Cornell, 2011) and coeditor of *Chaos in the Liberal Order: The Trump Presidency and International Politics in the Twenty-First Century* (Columbia, 2018). The author of many articles and book chapters on intelligence and strategy, Rovner also writes a regular column in *War on the Rocks*.

Dr. Jacquelyn Schneider is a Hoover Fellow at the Hoover Institution, is a nonresident fellow at the Naval War College, and was a senior policy advisor to the Cyberspace Solarium Commission. Her research focuses on the intersection of technology, national security, and political psychology, with a special interest in cybersecurity, unmanned technologies, and Northeast Asia. Her work has appeared in *Security Studies, Journal of Conflict Resolution, Strategic Studies Quarterly, Journal of Cybersecurity, The Washington Quarterly,* and *Journal of Strategic Studies*, and she has contributed to Lindsay and Gartzke, eds., *Cross Domain Deterrence: Strategy in an Era of Complexity* (Oxford University Press, 2019). In addition to her scholarly publications, she is a frequent contributor to policy outlets, including the *New York Times, Foreign Affairs,* the Council on Foreign Relations, *Cipher Brief, Lawfare, War on the Rocks,* the *Washington Post, Bulletin of the Atomic Scientists, National Interest, H-Diplo,* and publications of the Center for a New American Security. She has a BA from Columbia University, an MA from Arizona State University, and a PhD from George Washington University.

Brig. Gen. Paul T. Stanton, U.S. Army, is the Deputy Director of Current Operations at U.S. Cyber Command. He is responsible for advising the Director of Operations and

the commander on global and dynamic employment of Cyber Mission Forces and the daily operations of Department of Defense networks. Prior to his current assignment, he commanded the U.S. Army Cyber Protection Brigade at Fort Gordon, Georgia, with the responsibility to train, man, equip, and employ the Army's Cyber Protection Teams in support of national and geographic combatant commanders' priorities. Brigadier General Stanton previously served as Senior Technical Advisor for Army Cyber Command and as the deputy director of the Capabilities Development Group for U.S. Cyber Command. He also taught computer science at West Point. Brigadier General Stanton was commissioned as a U.S. Army infantry officer upon graduating with a bachelor of science degree in computer science from the U.S. Military Academy in 1995. He has served as an Airborne rifle platoon leader and a Bradley platoon leader and commanded B/1-502 IN (AASLT) with the 101st Airborne Division during Operation Iraqi Freedom. Brigadier General Stanton holds a master's degree in computer science from the University of Illinois at Urbana-Champaign and a PhD in computer science from Johns Hopkins University.

Lt. Col. Michael W. Tilton serves as the Deputy Chief for the Force Management Division at U.S. Cyber Command. The Force Management Division is responsible for readiness reporting, Operation Assessments, and Global Force Management for cyber operations forces. Previously, he served in several roles at the National Security Agency, including Aide de Camp for Commander, U.S. Cyber Command / Director of National Security Agency and Chief of Operational Risk Evaluations in Tailored Access Operations. Lieutenant Colonel Tilton was an assistant professor in the Department of Systems Engineering at the U.S. Military Academy from 2009 to 2013. During his teaching tour at West Point he became an Operations Research / Systems Analysis officer in 2009 and served in this analytic capacity in his three most recent assignments. Before 2009, Lieutenant Colonel Tilton was an attack helicopter pilot with operational tours in Germany, Fort Hood (Texas), and Iraq. He holds a bachelor of science in systems engineering from the U.S. Military Academy and a master of engineering in engineering management from Cornell University.

Capt. Erika Volino is an Air Force Junior Officer Cryptologic Career Program Intern at the National Security Agency. Previously, she was a Mission Commander in the Cyber National Mission Force. Captain Volino was commissioned through Officer Training School. She has a BA from the University of Colorado and an MA from the University of South Carolina, both in international relations.

Dr. Michael Warner serves as Command Historian at U.S. Cyber Command. He has written and lectured on cyber and intelligence history, theory, and reform and teaches as an adjunct professor at American University. His forthcoming book, *The Use of Force*

for State Power: History and Future, is coauthored with John Childress. His most recent book, *The Rise and Fall of Intelligence: An International Security History,* was published in 2014. Other writings include "Intelligence in Cyber—and Cyber in Intelligence," in *Understanding Cyber Conflict,* ed. Perkovich and Levite (Georgetown, 2017); "Notes on the Evolution of Computer Security Policy in the U.S. Government, 1965–2003," *IEEE Annals of the History of Computing* 37, no. 2 (April–June 2015); and "Cybersecurity: A Pre-history," *Intelligence and National Security* 27, no. 5 (October 2012). Dr. Warner sits on the board of editors of the peer-reviewed journal *Intelligence and National Security.*

Vice Adm. Timothy "T.J." White commanded U.S. Fleet Cyber Command / U.S. Tenth Fleet from June 2018 until September 2020. White is a 1987 graduate of the U.S. Naval Academy, where he received a bachelor of science degree in mechanical engineering. He holds a master of science in systems technology (command, control, and communications) from the Naval Postgraduate School and a master of science in national resource strategy from the National Defense University–Industrial College of the Armed Forces in Washington, DC. He is a Massachusetts Institute of Technology Seminar XXI fellow. Vice Admiral White was originally a Surface Warfare Officer. He served on board USS *Missouri* (BB 63) as electronic warfare officer, Combat Information Center officer, and assistant operations officer and was a CINCPACFLT Shiphandler of the Year. He was selected for redesignation as a Cryptologist, now Cryptologic Warfare Officer, in 1992 and was assigned to the Operations Directorate at the National Security Agency, Fort George G. Meade, Maryland. Vice Admiral White's operational fleet tours include assignments as assistant cryptologist, Commander, U.S. Naval Forces Central Command / U.S. Fifth Fleet in Manama, Bahrain, and Assistant Chief of Staff for Information Operations, N39, Commander, U.S. Seventh Fleet embarked on board USS *Blue Ridge* (LCC 19), homeported in Yokosuka, Japan. Additionally, White has served on the staff of the Chief of Naval Operations as the Joint Military Intelligence Program and Tactical Intelligence and Related Activities (now Military Intelligence Program) program resources director, as Deputy Director of Intelligence and Chief of Staff, Joint Functional Component Command–Network Warfare, U.S. Strategic Command, and as the Director, Commander's Action Group at U.S. Cyber Command. His command tours include Naval Security Group Activity Bahrain and Navy Information Operations Command Maryland. As a flag officer, he has served as Deputy Director, Tailored Access Operations, NSA and as director for intelligence, J2, U.S. Pacific Command. Vice Admiral White is a previous Commander, Cyber National Mission Force, USCYBERCOM. His focus of effort remains risk assessment and consequence management with respect to cybersecurity, critical infrastructure, supply chain, technology policy, and trust relationships.

The Newport Papers

Taiwan's Offshore Islands: Pathway or Barrier?, by Bruce A. Elleman (no. 44, January 2019).

On Wargaming: How Wargames Have Shaped History and How They May Shape the Future, by Matthew B. Caffrey Jr. (no. 43, January 2019).

Navies and Soft Power: Historical Case Studies of Naval Power and the Nonuse of Military Force, edited by Bruce A. Elleman and S. C. M. Paine (no. 42, June 2015).

Writing to Think: The Intellectual Journey of a Naval Career, by Robert C. Rubel (no. 41, February 2014).

Commerce Raiding: Historical Case Studies, 1755–2009, edited by Bruce A. Elleman and S. C. M. Paine (no. 40, October 2013).

Influence without Boots on the Ground: Seaborne Crisis Response, by Larissa Forster (no. 39, January 2013).

High Seas Buffer: The Taiwan Patrol Force, 1950–1979, by Bruce A. Elleman (no. 38, April 2012).

Innovation in Carrier Aviation, by Thomas C. Hone, Norman Friedman, and Mark D. Mandeles (no. 37, August 2011).

Defeating the U-boat: Inventing Antisubmarine Warfare, by Jan S. Breemer (no. 36, August 2010).

Piracy and Maritime Crime: Historical and Modern Case Studies, edited by Bruce A. Elleman, Andrew Forbes, and David Rosenberg (no. 35, January 2010).

Somalia . . . From the Sea, by Gary Ohls (no. 34, July 2009).

U.S. Naval Strategy in the 1980s: Selected Documents, edited by John B. Hattendorf and Peter M. Swartz (no. 33, December 2008).

Major Naval Operations, by Milan Vego (no. 32, September 2008).

Perspectives on Maritime Strategy: Essays from the Americas, edited by Paul D. Taylor (no. 31, August 2008).

U.S. Naval Strategy in the 1970s: Selected Documents, edited by John B. Hattendorf (no. 30, September 2007).

Shaping the Security Environment, edited by Derek S. Reveron (no. 29, September 2007).

Waves of Hope: The U.S. Navy's Response to the Tsunami in Northern Indonesia, by Bruce A. Elleman (no. 28, February 2007).

U.S. Naval Strategy in the 1990s: Selected Documents, edited by John B. Hattendorf (no. 27, September 2006).

Reposturing the Force: U.S. Overseas Presence in the Twenty-First Century, edited by Carnes Lord (no. 26, February 2006).

The Regulation of International Coercion: Legal Authorities and Political Constraints, by James P. Terry (no. 25, October 2005).

Naval Power in the Twenty-First Century: A Naval War College Review *Reader,* edited by Peter Dombrowski (no. 24, July 2005).

The Atlantic Crises: Britain, Europe, and Parting from the United States, by William Hopkinson (no. 23, May 2005).

China's Nuclear Force Modernization, edited by Lyle J. Goldstein with Andrew S. Erickson (no. 22, April 2005).

Latin American Security Challenges: A Collaborative Inquiry from North and South, edited by Paul D. Taylor (no. 21, 2004).

Global War Game: Second Series, 1984–1988, by Robert Gile (no. 20, 2004).

The Evolution of the U.S. Navy's Maritime Strategy, 1977–1986, by John Hattendorf (no. 19, 2004).

Military Transformation and the Defense Industry after Next: The Defense Industrial Implications of Network-centric Warfare, by Peter J. Dombrowski, Eugene Gholz, and Andrew L. Ross (no. 18, 2003).

The Limits of Transformation: Officer Attitudes toward the Revolution in Military Affairs, by Thomas G. Mahnken and James R. FitzSimonds (no. 17, 2003).

The Third Battle: Innovation in the U.S. Navy's Silent Cold War Struggle with Soviet Submarines, by Owen R. Cote Jr. (no. 16, 2003).

International Law and Naval War: The Effect of Marine Safety and Pollution Conventions during International Armed Conflict, by Dr. Sonja Ann Jozef Boelaert-Suominen (no. 15, December 2000).

Theater Ballistic Missile Defense from the Sea: Issues for the Maritime Component Commander, by Commander Charles C. Swicker, U.S. Navy (no. 14, August 1998).

Sailing New Seas, by Admiral J. Paul Reason, U.S. Navy, with David G. Freymann (no. 13, March 1998).

What Color Helmet? Reforming Security Council Peacekeeping Mandates, by Myron H. Nordquist (no. 12, August 1997).

The International Legal Ramifications of United States Counter-proliferation Strategy: Problems and Prospects, by Frank Gibson Goldman (no. 11, April 1997).

Chaos Theory: The Essentials for Military Applications, by Major Glenn E. James, U.S. Air Force (no. 10, October 1996).

A Doctrine Reader: The Navies of the United States, Great Britain, France, Italy, and Spain, by James J. Tritten and Vice Admiral Luigi Donolo, Italian Navy (Retired) (no. 9, December 1995).

Physics and Metaphysics of Deterrence: The British Approach, by Myron A. Greenberg (no. 8, December 1994).

Mission in the East: The Building of an Army in a Democracy in the New German States, by Colonel Mark E. Victorson, U.S. Army (no. 7, June 1994).

The Burden of Trafalgar: Decisive Battle and Naval Strategic Expectations on the Eve of the First World War, by Jan S. Breemer (no. 6, October 1993).

Beyond Mahan: A Proposal for a U.S. Naval Strategy in the Twenty-First Century, by Colonel Gary W. Anderson, U.S. Marine Corps (no. 5, August 1993).

Global War Game: The First Five Years, by Bud Hay and Bob Gile (no. 4, June 1993).

The "New" Law of the Sea and the Law of Armed Conflict at Sea, by Horace B. Robertson Jr. (no. 3, October 1992).

Toward a Pax Universalis: A Historical Critique of the National Military Strategy for the 1990s, by Lieutenant Colonel Gary W. Anderson, U.S. Marine Corps (no. 2, April 1992).

"Are We Beasts?" Churchill and the Moral Question of World War II "Area Bombing," by Christopher C. Harmon (no. 1, December 1991).

Newport Papers are available online (Acrobat required) at www.usnwc.edu/Publications/Naval-War-College-Press/.


THE UNITED STATES NAVAL ACADEMY
VIRIBUS MARI VICTORIA