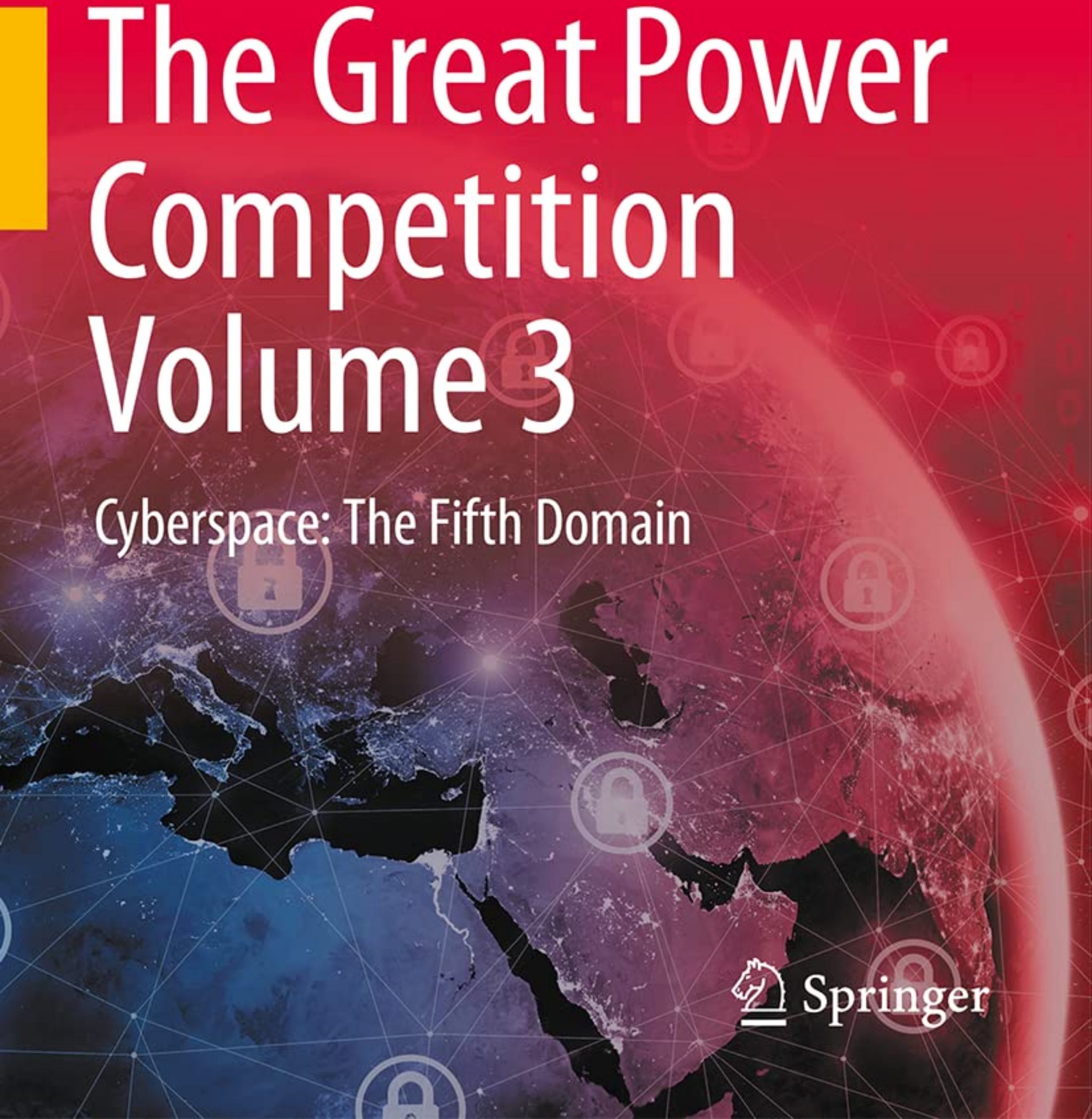
Adib Farhadi
Ronald P. Sanders
Anthony Masys *Editors*

The Great Power Competition Volume 3

Cyberspace: The Fifth Domain



Springer

About this book

For millennia, humans waged war on land and sea. The 20th century opened the skies and the stars, introducing air and space as warfare domains. Now, the 21st century has revealed perhaps the most insidious domain of all: cyberspace, the fifth domain. A realm free of physical boundaries, cyberspace lies at the intersection of technology and psychology, where one cannot see one's enemy, and the most potent weapon is information.

The third book in the Great Power Competition series, *Cyberspace: The Fifth Domain*, explores the emergence of cyberspace as a vector for espionage, sabotage, crime, and war. It examines how cyberspace rapidly evolved from a novelty to a weapon capable of influencing global economics and overthrowing regimes, wielded by nation-states and religious ideologies to stunning effect.

Cyberspace: The Fifth Domain offers a candid look at the United States' role in cyberspace, offering realistic prescriptions for responding to international cyber threats on the tactical, strategic, and doctrinal levels, answering the questions of how *can* we respond to these threats versus how *should* we respond? What are the obstacles to and consequences of strategic and tactical response options? What technological solutions are on the horizon? Should the U.S. adopt a more multi-domain offensive posture that eschews the dominant "cyber vs. cyber" paradigm? To answer these questions, experts examine the technological threats to critical infrastructure; cyber operations strategy, tactics, and doctrine; information influence operations; the weaponization of social media; and much more.

The Great Power Competition Volume 3

Adib Farhadi · Ronald P. Sanders · Anthony Masys
Editors

The Great Power Competition Volume 3

Cyberspace: The Fifth Domain

Springer

Editors
Adib Farhadi
College of Arts and Sciences
University of South Florida
Tampa, FL, USA

Ronald P. Sanders
Florida Center for Cybersecurity
University of South Florida
Tampa, FL, USA

Anthony Masys
College of Public Health
University of South Florida
Tampa, FL, USA

ISBN 978-3-031-04585-1 ISBN 978-3-031-04586-8 (eBook)
https://doi.org/10.1007/978-3-031-04586-8

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Foreword

Cybersecurity has been an important topic of debate in the United States for over 30 years but has only recently gained bipartisan traction as a national strategic focus, especially in terms of its impact on our national security. In that regard, *cyberspace* has emerged as a domain of warfare in its own right (along with land, sea, air, and space domains), and as such, it has become a key component of our national security strategy and our military's "way of war."

Unfortunately, our Nation's digital dependence has enabled other nation-states—those that aspire to Great Power status like Russia and China, as well as other regional geopolitical rivals—and their non-state proxies to gain asymmetric strategic advantage over the US, as they have unlawfully and covertly accessed our Nation's data, systems, and networks—including elements of our Defense Industrial Base and our critical infrastructure—for purposes of exploitation, theft of intellectual property, espionage (economic and otherwise), and, at least potentially, sabotage…as a part of and/or precursor to more kinetic forms of warfare.

That is what this book is about. Entitled *Cyberspace: The Fifth Domain*, this work examines the various cybersecurity threats facing the United States and its allies and provides realistic response options that range from the tactical to the strategic. Based in large part on the third Great Power Competition Conference hosted by the University of South Florida, US Central Command, and the National Defense University's Near East South Asia Center for Strategic Studies, it elaborates on many of the topics and ideas raised during that dynamic event, held in April 2021.

The authors—all of whom come from a national security background—address critical cyberspace topics, including the risk associated with cybersecurity threats, adversary capabilities and intentions, and the pros and cons of various U.S. responses. Further, the authors consider a U.S. offensive cyberspace posture and explore strategic military and technological cyberoperations to combat (or deter) foreign cyberspace activities.

Through expert examination of the cyberspace threats the United States faces today, *Cyberspace: The Fifth Domain* serves to contribute to this important discussion. Accordingly, I hope that our many readers—including military leaders, scholars, and policymakers—find that the following pages challenge your thinking and

enlighten your perspective on the often-subtle influence cyberspace operations have on our national security, both defensively and offensively.

HON J. Michael “Mike” McConnell, VADM, USN, Retired
Executive Director, The Florida Center for Cybersecurity
Former Director of U.S. National Intelligence
Former Director of the National Security Agency
Chair Emeritus, National Intelligence University Foundation
Tampa, USA

Acknowledgments

The editors would like to extend their sincerest gratitude to the entire University of South Florida and National Defense University Near East South Asia Center for Strategic Strategies for their work on the Great Power Competition Conferences Series and the resulting edited volume.

They would like to express their appreciation to Dr. Eric Eisenberg, USF Dean of College of Arts and Science, for his continued and enthusiastic support for the initiative.

A most heartful thanks to Kathleen Whitaker, Arman Mahmoudian, Dr. Dianna Donnelly, Andrew Roberts, Sarah T. White and the contributing authors for making this book possible.

Dr. Adib Farhadi would like to thank his wife, Elaha, children, Adam, Sophia, and mother, Maliha, for their support, patience, and love, not only in regard to this project but in everything that life brings.

Overview

Influence Operations

Alternate Reality—The Use of Disinformation to Normalize Extremism

By Elie Alhajjar

Disinformation is becoming abundant in our civic society, and it poses a national cyberthreat to our democracy. While some conspiracy theories are born spontaneously (in the heat of the moment), others are premeditated by near-peer nation-states such as Russia, China, and their proxies. In this chapter, it is argued that our enemies are using game-like cognitive tactics to reach a large number of people within the United States and radicalize their beliefs. By turning random events and unrelated pieces of information into an alternative reality in which the vulnerable population is getting immersed, a new cognitive state is being established that can basically justify any extreme thought one might have.

The Commercialization of Influence Operations

By Sean Ryan, Ian Conway, and Kathleen Cassedy

This research establishes a clear threat to U.S. national security through the information domain. Influence exercised through this domain impacts domestic stability and internal political processes in the United States. Scenarios presented demonstrate deliberate activities that focused on influencing the U.S. and allies. Scenarios demonstrated actual intent by Russia, China, and regional actors like Iran, to impact the perceptions of target audiences in U.S., Europe, and Africa working by, with, and through commercial platforms to both obfuscate attribution and corrupt objectivity in reporting. Going further, this research connects activities by Great Power competitors, namely, Russia and China, to the subversion of commercial enterprises for the primary purpose of influencing media outlets that provide information to the American (and global) public, and to lever the global business environment to their advantage. Exploiting commercial relationships built legally through overt and clandestine corporate ventures is a primary vehicle for exerting influence in Great Power

Competition. Loopholes in antiquated U.S. laws and policies allow such exploitation to go unchecked and often unobserved. High net worth individuals, multinational corporations, sovereign wealth funds, and NGOs are tied to political support leading to subversion and corruption through the direct use of finance and digital information. Finally, recommendations are made to tighten loopholes in U.S. policies and statutes to mitigate foreign exploitation of information aimed at distracting and disrupting the United States in Great Power Competition for global influence.

The Future of Cyber-Enabled Influence Operations: Emergent Technologies, Disinformation, and the Destruction of Democracy

By Joe Littell

Nation-states have been embracing online influence campaigns through disinformation at breakneck speeds. Countries such as China and Russia have completely revamped their military doctrine to information-first platforms (Cunningham, 2020) to compete with the United States and the West. The Chinese principle of "Three Warfares" and Russian Hybrid Warfare have been used and tested across the spectrum of operations ranging from competition to active conflict. With the COVID-19 pandemic limiting most means of face-to-face interpersonal communication, many other nations have transitioned to online tools to influence audiences both domestically and abroad (Strick, 2020) to create favorable environments for their geopolitical goals and national objectives. This chapter focuses on the landscape that allows nations like China and Russia to attack democratic institutions and discourse within the United States, the strategies and tactics employed in these campaigns, and the emergent technologies that will enable these nations to gain an advantage with key populations within their spheres of influence or to create a disadvantage to their competitors within their spheres of influence. Advancements in machine learning through generative adversarial networks (Creswell et al., 2018) that create deepfakes (Whittaker; Letheren and Mulcahy, 2021) and attention-based transformers (Devlin et al., 2018) that create realistic speech patterns and interaction will continue to plague online discussion and information spread, attempting to cause further partisan divisions and decline of U.S. stature on the world stage and democracy as a whole.

Countering Influence Operations

The Need to Inoculate Military Servicemembers Against Information Threats: The Case for Digital Literacy Training for the Force

By Peter W. Singer and Eric Johnson

Every minute of every day, men and women in uniform are attacked by a weapon that threatens them, their services, and the nation. Yet the U.S. military has not trained them to prepare for this onslaught. It is time for this to change.

Over the last several years, misinformation and deliberately spread disinformation, pushed by both foreign and domestic sources, have proliferated online. They have shaped not just what people read and believe, but also how they act. This "weaponization of social media" has created a formidable challenge in nearly every

policy area, from aiding the forces of terrorism and extremism to being a tool of great power competition to damaging the vitality of our democracy.

This challenge is not just to our wider national security, but also to the military itself. Every day, millions of service members at every rank use social media. In so doing, they regularly are targeted by and engage with the viral spread of false information online. The resulting effects on them and the military affect operational security, force reputation, and even the physical health of service members.

Regional Cyber Issues

Countering Violent Extremism in Central Asia and South Asia: Islamophobia and Cyber-Radicalization in the Digital Era

By Adib Farhadi

Widespread political and economic uncertainty following the COVID-19 pandemic, along with increased access to social media and digital messaging in rural areas, has rendered vulnerable populations in Central Asia and South Asia (CASA) even more susceptible to misinformation and population targeting by violent extremists. More, studies show that violent radicalization is inextricably linked to Islamophobia—which is on the rise alongside an endless stream of digital news reporting. Violent extremists capitalize on publicized Islamophobic events to spread misinformation and lure disenfranchised recruits. Compounding these issues in the CASA region is a severely debilitated Afghanistan, ripe for the proliferation of violent extremist activity that will reach far beyond its borders. To mitigate the proliferation of violent extremism in Central Asia and South Asia, Islamophobia must be addressed in earnest at home and abroad. The need for more effective mitigation of Islamophobia and violent Islamic radicalization in the region remains particularly acute during this period of intense insecurity in Afghanistan.

Cyber and Great Power Competition in the Western Hemisphere

By Alexander Crowther, Fabiana Perera, and Brian Fonseca

Great Power Competition is happening in every geographic region and across most domains. The People's Republic of China, Russian Federation, the United States, and other actors are engaged globally, regionally, and even locally. Not everyone competes everywhere, but there is no country in the world today that is not on a field of competition. The United States own neighborhood, the western hemisphere, has seen competition increase as the People's Republic of China, Iran, North Korea, and Russian Federation have all sought to engage to contest historical US hegemony over the region.

Competition in the western hemisphere and in other regions is happening across all three major domains—land, sea, and air. It is also happening in the cyberdomain. This chapter discusses great power competition in the cyberdomain in the western hemisphere. It summarizes the interests and activities of US near-peers in the western hemisphere and presents an overview of their operations in cyberspace. The chapter argues that each of the US near-peers is pursuing different tools for different aims within the western hemisphere. However, in all cases, advances from US near-competitors in the cyberdomain are facilitated by weak governance of the defense sector, and weak capabilities in the cyberdomain in the target countries.

Cyberspace Leadership

The Cyber Pandemic that Could Redefine the Great Power Competition: Preparing the Defense Industrial Base

By Adib Farhadi, Ian Galloway, and Ayman Bekdash

The Fourth Industrial Revolution (4IR) stands poised to transform the geopolitics and geoeconomics of the Great Power Competition (GPC) as digital and cyberworlds permeate societies, governments, and nation-states. The United States must reconceptualize its public-private approach to cybersecurity, starting with the Defense Industrial Base (DIB). As policymakers continue to grapple with the COVID-19 pandemic, the World Economic Forum (WEF) warns that "we should prepare for a COVID-like global cyber pandemic that will spread faster and further than a biological virus, with an equal or greater economic impact" (Davis and Pipkaite 2020). Despite this warning, the new cybersecurity regulations being rolled out under what is commonly known as Cybersecurity Maturity Model Certification (CMMC) are inadequate to protect the DIB from future cyberthreats. Underpinned by the conceptual framework of stakeholder capitalism, this chapter posits that cybersecurity regulations must be reimagined to foster greater process and systems agility, transparency, and trust between the government and the private sector.

Cyber Leadership in the Era of the Great Power Competition

By Garrett Potts

In an effort to consider what the U.S. can do to mitigate threats to the relatively new battlefield of cyberspace, this chapter calls readers' attention to how critical infrastructure and software breaches often happen. Next, the chapter engages with questions regarding who can help us to learn from the breaches further. An answer is provided in light of the ideal type of the "Cyber Leader"—defined herein as someone who demonstrates craft-expertise in the practice of cybersecurity to promote the internal goods of privacy and security. A partial account of what virtues cyber leaders require is also sketched before chapter conclusions are drawn.

Deterrence in Cyberspace

Cybersecurity and Strategic Deterrence: Changing Adversary's Risk Versus Reward Calculations

By Hon J. Mike McConnell, VADM, USN, RET, and Mark Grzegorzewski

This chapter is an extension of the April 16, 2021 panel discussion at the University of South Florida-Cyber Florida Great Power Competition conference series titled "Cybersecurity: The Fifth Domain." Frank Cilluffo moderated the panel "Cybersecurity and Strategic Deterrence" which included the following panelists: HON Mike McConnell; VADM, USN; RET., HON Michael Chertoff; and LTGEN Dennis Crall, USMC.

SolarWinds, Microsoft Exchange Server, JBS, Colonial Pipeline, Kaseya…cyberattacks, cyberintrusions, and exploitation breaches keep mounting, not only from cybercriminals but from nation-states, most notably Russia and China. While cyberattacks against U.S. companies and U.S. Government organizations are not new, the scale and frequency are increasing at an alarming rate. With the U.S. becoming increasing "digitally dependent," this problem has reached strategic proportions. Why is this the case? How can the most military-capable country in the world be so exposed to cyberattacks and not forcefully respond? We proffer the answer can be found in General (GEN) Paul Nakasone's 2018 Senate confirmation as Commander of USCYBERCOMMAND. Responding to Sen. Dan Sullivan's line of inquiry as to why the United States is the "cyber punching bag of the world," GEN Nakasone responded, "I would say right now they do not think that much will happen to them." He added, "they don't fear us" and "the longer that we have inactivity, the longer that our adversaries are able to establish their own norms." In essence, the U.S. is not deterring its adversaries in cyberspace since they do not fear a consequence. Part of their risk-reward calculation surely assesses that although the U.S. may have some of the most exquisite cybercapabilities, it also has many more unpatched cybersecurity vulnerabilities and consequently lacks cyberspace resiliency. Thus, adversarial states assess that the reward of carrying out an action through cyberspace far exceeds any potential cost.

While there are certainly factors constraining how the U.S. can respond, it should not mean the U.S. government (USG) could not respond beyond its current efforts. The cliché that the U.S. lives in the largest glass house and is therefore reluctant to throw stones can only hold for so long. It is well past time the USG fortify its glass house, through cyberresiliency, so it can make its adversaries fear consequences for their actions. In this chapter, we propose a way in which the United States can respond, namely, through cyberresiliency (i.e., deterrence by denial), to build toward establishing a more effective overall deterrence posture.

In what follows, we extend the important insights shared during the "Cybersecurity and Strategic Deterrence" panel. First, we address the risk inherent in the U.S.' large attack surface. This overview provides context to our argument that increased cyberresiliency could bolster overall U.S. national security. Second, we present our thesis to the reader. Our central premise is that the U.S. needs to strengthen its cyberresiliency to deter more effectively, and we demonstrate this claim by illuminating

the scope of the problem and providing specific recommendations for changing the risk versus reward calculations of U.S. adversaries. We also address challenges to our recommendations. We then layout what is meant by deterrence and cyberdeterrence, so that the reader can have a deeper appreciation of its complexity and understand how cyberresiliency is just one part of a larger calculation. Finally, we critique the nuclear deterrence-cyberdeterrence analogy before moving to a summation of our chapter.

Cyberspace Strategy and Doctrine

Great Power Competition: Critical Infrastructure

By Morey Haber

The tensions between adversarial nations have escalated far beyond the physical build up troops and machines of war. It has long been predicted that the next conflict would use the Internet as a new battle field to cripple critical infrastructure and disrupt the financial and business operations in the theater of conflict. Whether a cyberattack occurs first, like in the Operations of Desert Storm in 1990, crippling the Iraq power grid or through Stuxnet to interfere with Uranium production in Iran, the fact remains a well-coordinated cyberattack can be an effective weapon during a nation-state mission or as a precursor to war. There is no doubt that the opposing forces are considering cyberwarfare as a part of their offensive and defensive strategy. While the world has generally condoned chemical and biological weapons that could cause mass causalities outside of traditional war fighters, cyberattacks against critical infrastructure could cause the poisoning of civilians, disruptions in the food supply chain, and even the ability to provide life-saving health services to civilians. To that end, politicians, the military, and all realms of technology professionals must consider critical infrastructure as a target and the threats and mitigation strategies are something we will explore in this chapter.

Examining Systemic Risk in the Cyber Landscape

By Dr. Anthony Masys

Cyberattacks and incursions have certainly emerged as a national security issue. Globally we are seeing the effects of such attacks not only on the financial domain but also in health care, government, and critical infrastructure (Masys, 2014, 2021a). Understanding the extent of the impact of cyberincursions and attacks requires understanding the systemic cyberrisks "…of risks spreading across interdependent systems" (Welburn et al., 2021). The World Economic Forum (2016) defines Systemic cyberrisk as "…the risk that a cyber event (attack(s) or other adverse event(s)) at an individual component of a critical infrastructure ecosystem will cause significant delay, denial, breakdown, disruption or loss, such that services are impacted not only in the originating component but consequences also cascade into related (logically and/or geographically) ecosystem components, resulting in significant adverse effects to public health or safety, economic security or national security." Lucas et al (2018) argue that "…systemic risk refers to a potential collapse of a system of potentially global importance and criticality to services that humans

urgently need. This dimension of a large potential threat within a complex web of interacting elements distinguishes systemic from other types of risk." As such traditional risk management approaches are not sufficient for dealing with them IRGC (2018:5). This chapter explores systemic risk across the cyber landscape through the non-traditional security lens (Masys, 2021b) and presents applications of systems thinking, scenario planning, and High-Reliability Security Organizations to support systemic risk awareness and management.

When the Levee Breaks: A Global Trend of Cyber-Physical and Cyber-Operational Attacks Against Critical Infrastructure and Future Implications on the Great Power Competition

By Steve Sin, and Rhyner Washburn

Cyber-physical systems (CPSs) refer to systems that connect computers, communication channels, and physical devices. They lie at the heart of today's critical infrastructure. CPSs are currently one of the most targeted systems of adversarial actors operating in the cyberdomain. Cyber-physical and cyber-operational attacks on critical infrastructures via attacks on CPSs have the potential to damage physical infrastructure assets and have widespread consequences for national security as well as society. We analyzed 427 publicly reported cyber-physical and cyber-operational attacks conducted against critical infrastructures globally between January 1, 1992 and July 9, 2021. We find that of the attacks that can be attributed to an actor type, state actors (including state-affiliated and state-supported actors) were found to be the predominant actors that conduct cyber-physical attacks while state and non-state actors occupied approximately the same ratio of attacks for cyber-operational attacks. We also find espionage to be the most statistically significant motivation for the state actors to conduct cyber-physical and/or cyber-operational attacks. Additionally, we find the rivalry between the attacker and the target to be the most statistically significant international security-relevant variable. Finally, we provide an assessment of the implications of cyber-physical and cyber-operational attacks on critical infrastructure in the contexts of current and future irregular warfare and great power competition.

Training and Talent

The Cyber-Grand Strategy Gap

By Jacob Shively

This chapter finds that America's central cyberstrategic challenge is a massively skewed risk/reward calculation that favors peer competitors. Leading proposals to address this imbalance are technical and operational, but such solutions are inadequate for an unbalanced strategic environment. This study applies a grand strategy framework to discussions of national security and cyberarticulated by senior officials, military commanders, and other experts at the April 2021 Great Power Competition

conference. For attackers, the consequences of being seen as a cyberthreat by the United States are relatively minor compared to the rewards of hacking US systems, stealing intelligence and intellectual property, conducting information warfare, and developing capabilities to quickly devastate critical infrastructure. In short, the benefits of violating US cybersystems are specific and valuable. The costs are diffuse and, attackers seem to agree, manageable. These are classic conditions favoring offensive behavior. In response, professionals at the conference recommended operational and technical solutions. These focused on versions of deterrence, namely, collective defense and defending forward. Here, collective defense refers to cooperation and collaboration among private US actors and the US government. It is designed to convince attackers to redirect their efforts because US systems are resilient and difficult to penetrate. Defending forward refers to US agencies launching persistent, offensive attacks that keep adversary resources distracted, and adversary operators worried about US reprisals. Viewed in the context of grand strategy, these are necessary but not sufficient policy solutions. US planners need to bridge the gap between a current strategic context that favors challengers and a future in which that balance favors US defenders. As in prior eras of technological change, policymakers likely need to pair technical and operational prowess with statecraft and other diplomatic tools.

The War for Cyber Talent: Can the US Win It?

By Ronald Sanders

Our Nation has become increasingly digitally dependent, and, in so doing, it has also become more vulnerable in cyberspace. A significant part of that vulnerability concerns people. For example, people—users like us—are still the principal cause of cybersecurity breaches; over three-quarters of them the result of some socially engineered attack vector, with the remaining breaches more technical (and technically sophisticated) in nature, and as a consequence, people must also stand guard against those incursions. The latter is the focus of this chapter…the people who are responsible for protecting our data and our networks, including those who engage in what are arguably deterrent offensive cyberoperations. In that regard, our Nation's cyberworkforce has become a major factor in its ability to protect our critical—and increasingly vulnerable—information and communications technology (ICT) infrastructure…as well as to project power in the cyberspace domain to influence the behavior of other aspiring "Great Powers" like Russia and China, their proxies, and other regional geopolitical rivals. However, this is not a war in the benign, labor market sense. One involving the competition to talent, although that is part of it. No, the US is in a real "people" war in the cyberspace domain, with real consequences for national security. To that end, the chapter will begin with a brief introduction that seeks to define the cybersecurity talent gap that is the basis of that war, and then it will then discuss the size of that gap, and/or how the US can attempt to measure it. The chapter will then discuss how the US can begin to close that gap, especially with respect to the pipeline that ultimately produces cyber talent that may be deployed in the US national interest, beginning with efforts to attract more young people to

cyberspace-related academic disciplines in elementary and secondary schools, post-secondary vocational schools, and colleges and universities (the most obvious "raw" source of cyber talent), before eventually finding their way into cyberspace-related professions. In so doing, the chapter compares and contrasts how our Great Power competitors develop such talent and offer some suggestions on how the US's "supply side" cyberpipeline may be improved. The chapter will then narrow its focus to the Nation's largest employer of such talent: The US government, including its armed forces and its civilian and contractor workforce. And as we will see, the Federal government is also potentially the largest producer and supplier of that talent, both directly and indirectly, and the chapter will close with a description of the US government's current efforts in that regard, as well as with some recommendations on how those efforts may be accelerated to help close the national security cyber talent gap. For that gap—between the US and its global geopolitical rivals, particularly those that aspire to Great Power status and otherwise—is real and growing.

Leveraging Talent to Dominate in Cyber War—An Army Perspective

By Colonel Chad Bates and Major Charlene Rose

DISCLAIMER: The views expressed in this work are those of the author(s) and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, or the Department of Defense.

In order to dominate in a persistent engagement with the nation's adversaries in cyberwarfare, the United States Government must posture a mature and experienced force through a strategic, nationwide partnership for a whole-of-society defense against adversarial threats. In order to recruit and maintain such a high-performing workforce requires an innovative talent management plan that will prevail in an expanding war on acquiring these highly skilled cyberexperts. This plan will assist the United States Cyber Command (USCYBERCOM) to effectively enforce the nation's cybersecurity objectives in the growing great power competition within cyberspace. In this domain, adversarial cyberstrategies range from malicious and sporadic, to calculating and cohesive. Requiring an agile national U.S. cybersecurity posture to engage against these threats through innovative technological solutions, maximizing cyberhuman capital, and continuously evaluating adversarial cyberstrategies. The ingenuity of the human brain is critical in meeting the nation's strategic goals in the cyberdomain. While also leveraging technological advancements in order to enable the pursuit for dominance in this great power competition. Across the continuum of engagement within cyberspace, the country must leverage its cyber talent across all sectors in order to more effectively meet cybersecurity demands through streamlined lateral linkages as a whole-of-society defense. Nationwide partnerships will support the response rate necessary for the evolving cyberdomain, leading to an agile cyber-workforce reinforced by the matrix of U.S. cyberagencies and organizations. The cyberposture strategy must consider talent recruitment, development, and retention to successfully meet talent management goals. This paper will review the U.S. Army Cyber Command's perspective of these key talent management components as it relates to a national, whole-of-society cybersecurity concept.

Contents

Editors and Contributors

About the Editors

Dr. Adib Farhadi is an Assistant Professor, Faculty Director of Executive Education, and lead editor of the Great Power Competition book and conference series at the University of South Florida. His research is at the intersection of religion, politics, economics, and conflict, with a particular focus on the Central and South Asia (CASA) Region. He is the author of *Countering Violent Extremism by Winning Hearts and Minds* and a frequent presenter on the topics of Strategic Competition, Countering Violent Extremism (CVE), and Strategic Negotiations & Communication. Formerly, Dr. Farhadi served in senior positions for Afghanistan and has extensively advised the United States government and various other international organizations. He earned his Ph.D. in Economics from the University of Canberra, M.A. from New York University, and B.S. from East Carolina University.

Dr. Ronald P. Sanders is a Fellow of the National Academy of Public Administration and a decorated, 20-year member of the US government's Senior Executive Service, he currently serves as Staff Director for the Florida Center for Cybersecurity, where he helps to coordinate cybersecurity research, education, and outreach efforts among Florida's 12 State University System (SUS) institutions. From 2017 to 2020, he served as the Director of the University of South Florida's School of Public Affairs, where he oversaw various graduate education and research programs in public administration and urban and regional planning, as well as its Florida Institute of Government. In addition, until his unintentionally well-publicized resignation in October 2020, he chaired the US Federal Salary Council (a Presidential appointment), which makes recommendations on pay raises for the Federal government's 2M+ white-collar employees. He also served on the Advisory Board of the National Security Agency and Vice Chair of the National Intelligence University Foundation.

In addition to his USF appointments, he has served in senior leadership positions in both public and private sectors. For example, he was Vice President of the consulting firm Booz Allen Hamilton and the firm's very first Fellow (2010 to 2017);

the first Associate Director of National Intelligence for Human Capital (2005–2010), where he earned one of Harvard University's *Innovations in American Government Awards* and the National Intelligence Distinguished Service Medal; the first Associate Director of the US Office of Personnel Management for Policy (2002 to 2005); the Internal Revenue Service's first Chief Human Resource Officer (1998 to 2002); and the US Defense Department's Director of Civilian Personnel (1991 to 1998). He has also served on the faculties of Syracuse University's Maxwell School of Citizenship and Public Affairs (from 1995 to 1996) and the George Washington University's School of Business and Public Management (from 1997 to 1998) and directed research centers at both institutions, and he has co-authored four other books, including two published by the Brookings Institution and one by NAPA, as well as numerous articles and monographs in both academic and professional outlets.

Dr. Anthony Masys is an Associate Professor and Director of Global Disaster Management, Humanitarian Assistance and Homeland Security. A former Senior Air Force Officer, he has a BSc in Physics and MSc in Underwater Acoustics and Oceanography from the Royal Military College of Canada and a Ph.D. from the University of Leicester. He is Editor in Chief for Springer Publishing book series: Advanced Sciences and Technologies for Security Applications and holds various advisory board positions with academic journals and books series. He is an internationally recognized author, speaker, and facilitator and has held workshops on security, visual thinking, design thinking, and systems thinking in Europe, Canada, South America, West Africa, and Asia. He has published extensively in the domains of physics and the social sciences. He supports the University of Leicester (U.K.) as an Associate Tutor in their Distance MSc Program on Risk Crisis and Disaster Management.

Contributors

Alhajjar Elie United States Military Academy, West Point, NY, USA

Bates Colonel Chad U.S. Army War College, Carlisle Barracks, PA, USA

Bekdash Ayman DGC International, McLean, VA, USA

Cassedy Kathleen West Liberty University, West Liberty, WV, USA

Conway Ian West Liberty University, West Liberty, WV, USA

Crowther Alexander Florida International University, Miami, FL, USA

Farhadi Adib University of South Florida, Tampa, FL, USA

Fonseca Brian Florida International University, Miami, FL, USA

Galloway Ian DGC International, McLean, VA, USA

Grzegorzewski Mark St. Petersburg College, St. Petersburg, Tampa, FL, USA

Haber Morey BeyondTrust, Johns Creek, USA

Johnson Eric New America, Washington, DC, USA

Littell Joe Army Cyber Institute at the West Point, United States Military Academy, West Point, NY, USA

Masys Anthony University of South Florida, Tampa, FL, USA

McConnell Hon J. Mike University of South Florida, Tampa, FL, USA

Perera Fabiana National Defense University, Washington, D.C, USA

Potts Garrett University of South Florida, Tampa, FL, USA

Rose Major Charlene United States Military Academy, West Point, NY, USA

Ryan Sean West Liberty University, West Liberty, WV, USA

Sanders Ronald University of South Florida, Tampa, FL, USA

Shively Jacob University of West Florida, Pensacola, FL, USA

Sin Steve University of Maryland, College Park, MD, USA

Singer Peter W. Arizona State University, Tempe, AZ, USA

VADM, USN, RET University of South Florida, Tampa, FL, USA

Washburn Rhyner University of Maryland, College Park, MD, USA