

THE CYBER DEFENSE REVIEW

COVID-19 IMPLICATIONS FOR CYBER

COVID-19 and the Cyber Challenge

General (Ret.) Keith B. Alexander

Jamil N. Jaffer



Achieving Systemic Resilience in a Great
Systems Conflict Era: Coalescing against
Cyber, Pandemic, and Adversary Threats

Dr. Chris Demchak

Seven Cybersecurity Lessons the Coronavirus
Can Teach the Armed Forces (and Us All)

Dr. Mike Lloyd

Ray Rothrock

Unleash the Dragon: China's Strategic
Narrative during the COVID-19 Pandemic

Mark Bryan Manantan

COVID-19 and Cyber – Foreshadowing
Future Non-Kinetic Hybrid Warfare

Rob Schrier

INTRODUCTION

Cybersecurity within a Pandemic Environment

Col. Jeffrey M. Erickson

BOOK REVIEW

Censored: Distraction and Diversion

Inside China's Great Firewall

by Margaret E. Roberts

Cadet Tommy Hall

THE CYBER DEFENSE REVIEW

◆ SPRING EDITION ◆

THE CYBER DEFENSE REVIEW

A DYNAMIC MULTIDISCIPLINARY DIALOGUE

DIRECTOR, ARMY CYBER INSTITUTE

Col. Jeffrey M. Erickson

CHIEF OF STAFF, ARMY CYBER INSTITUTE

Col. Stephen S. Hamilton

SENIOR FACULTY MEMBER, ARMY CYBER INSTITUTE

Dr. Edward Sobiesk

EDITOR IN CHIEF

Dr. Corvin J. Connolly

MANAGING EDITOR

Dr. Jan Kallberg

ASSISTANT EDITORS

West Point Class of '70

AREA EDITORS

Dr. Harold J. Arata III

(Cybersecurity Strategy)

Lt. Col. Todd W. Arnold, Ph.D.

(Internet Networking/Capability Development)

Prof. Robert Barnsby, J.D.

(Cyber & International Humanitarian Law)

Maj. Nathaniel D. Bastian, Ph.D.

(Advanced Analytics/Data Science)

Dr. Aaron F. Brantly

(Policy Analysis/International Relations)

Dr. Dawn Dunkerley Goss

(Cybersecurity Optimization/Operationalization)

Dr. David Gioe

(History/Intelligence Community)

Col. Paul Goethals, Ph.D.

(Operations Research/Military Strategy)

Dr. Michael Grimaila

(Systems Engineering/Information Assurance)

Dr. Steve Henderson

(Data Mining/Machine Learning)

Ms. Elsa Kania

(Indo-Pacific Security/Emerging Technologies)

Maj. Charlie Lewis

(Military Operations/Training/Doctrine)

Dr. Fernando Maymi

(Cyber Curricula/Autonomous Platforms)

Lt. Col. Erica Mitchell, Ph.D.

(Human Factors)

Lt. Col. William Clay Moody, Ph.D.

(Software Development)

Sgt. Maj. Jeffrey Morris, Ph.D.

(Quantum Information/Talent Management)

Ms. Elizabeth Oren

(Cultural Studies)

Dr. David Raymond

(Network Security)

Lt. Col Robert J. Ross, Ph.D.

(Information Warfare)

Dr. Paulo Shakarian

(Social Threat Intelligence/Cyber Modeling)

Dr. David Thomson

(Cryptographic Processes/Information Theory)

Dr. Robert Thomson

(Learning Algorithms/Computational Modeling)

Lt. Col. Natalie Vanatta, Ph.D.

(Threatcasting/Encryption)

Lt. Col. Mark Visger, J.D.

(Cyber Law)

EDITORIAL BOARD

Dr. Andrew O. Hall, (Chair.)

Marymount University

Dr. Amy Apon

Clemson University

Dr. Chris Arney

U.S. Military Academy

Dr. David Brumley

Carnegie Mellon University

Col. (Ret.) W. Michael Guillot

Air University

Dr. Martin Libicki

U.S. Naval Academy

Dr. Michele L. Malvesti

Financial Integrity Network

Dr. Milton Mueller

Georgia Tech School of Public Policy

Col. Suzanne Nielsen, Ph.D.

U.S. Military Academy

Dr. Hy S. Rothstein

Naval Postgraduate School

Dr. Bhavani Thuraisingham

The University of Texas at Dallas

Ms. Liis Vihul

Cyber Law International

Prof. Tim Watson

University of Warwick, UK

Prof. Samuel White

Army War College

CREATIVE DIRECTORS

Sergio Analco

Gina Daschbach

LEGAL REVIEW

Courtney Gordon-Tennant, Esq.

PUBLIC AFFAIRS OFFICER

Maj. Lisa Beum

KEY CONTRIBUTORS

Clare Blackmon

Nataliya Brantly

Kate Brown

Neyda Castillo

Erik Dean

Debra Giannetto

Anton Hubbard

Col. Michael Jackson

Lance Latimer

Alfred Pacenza

Diane Peluso

Michelle Marie Wallace

CONTACT

Army Cyber Institute

Spellman Hall

2101 New South Post Road

West Point, New York 10996

SUBMISSIONS

The Cyber Defense Review

welcomes submissions at

mc04.manuscriptcentral.com/cyberdr

WEBSITE

cyberdefensereview.army.mil

The Cyber Defense Review (ISSN 2474-2120) is published by the Army Cyber Institute at West Point. The views expressed in the journal are those of the authors and not the United States Military Academy, the Department of the Army, or any other agency of the U.S. Government. The mention of companies and/or products is for demonstrative purposes only and does not constitute endorsement by United States Military Academy, the Department of the Army, or any other agency of the U.S. Government.

© U.S. copyright protection is not available for works of the United States Government. However, the authors of specific content published in The Cyber Defense Review retain copyright to their individual works, so long as those works were not written by United States Government personnel (military or civilian) as part of their official duties. Publication in a government journal does not authorize the use or appropriation of copyright-protected material without the owner's consent.

This publication of the CDR was designed and produced by Gina Daschbach Marketing, LLC, under the management of FedWriters.

The CDR is printed by McDonald & Eudy Printers, Inc. ∞ Printed on Acid Free paper.

★★★★★
SPECIAL
EDITION

COVID-19 IMPLICATIONS FOR CYBER

INTRODUCTION

Col. Jeffrey M. Erickson

9

Cybersecurity within a
Pandemic Environment

SENIOR LEADER PERSPECTIVE

General (Ret.) Keith B. Alexander
Jamil N. Jaffer

17

COVID-19 and the Cyber Challenge

Rob Schrier

29

COVID-19 and Cyber – Foreshadowing
Future Non-Kinetic Hybrid Warfare

PROFESSIONAL COMMENTARY

Dr. Mike Lloyd
Ray Rothrock

41

Seven Cybersecurity Lessons the
Coronavirus Can Teach the Armed Forces
(and Us All)

RESEARCH ARTICLES

Dr. Chris Demchak

51

Achieving Systemic Resilience in a Great
Systems Conflict Era: Coalescing against
Cyber, Pandemic, and Adversary Threats**Mark Bryan Manantan**

71

Unleash the Dragon: China's Strategic
Narrative during the COVID-19 Pandemic

NON-COVID-19 RESEARCH ARTICLES

Nataliya D. Brantly

93

Homefront to Battlefield: Why the U.S.
Military Should Care About Biomedical
Cybersecurity

Lance Y. Hunter, Ph.D.
Craig Douglas Albert Ph.D.
Eric Garrett

111

Factors That Motivate State-Sponsored
Cyberattacks

BOOK REVIEW

Cadet Tommy Hall

131

*Censored: Distraction and Diversion
Inside China's Great Firewall*
by Margaret E. Roberts

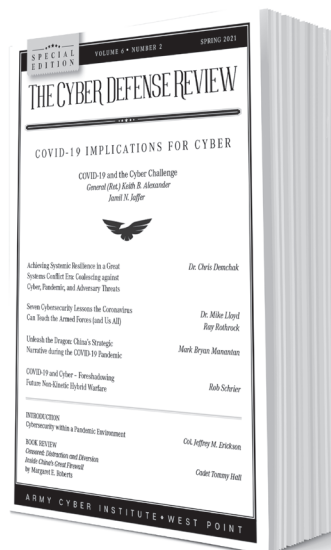
THE CYBER DEFENSE REVIEW

◆ INTRODUCTION ◆

VOL. 6 ♦ NO. 2

The Cyber Defense Review: Cybersecurity within a Pandemic Environment

Colonel Jeffrey M. Erickson



Welcome to the COVID-19 Special Edition of *The Cyber Defense Review* (CDR). In this issue, we are examining how the pandemic has impacted cybersecurity, and how pandemics may impact it in the future.

The genesis of this issue occurred in early Spring 2020. The COVID-19 pandemic was emerging, infection numbers were rising, and the world began shifting to a telework-focused workplace to mitigate the spread. Immediately, the cyber threat space became much more complex as attack surfaces multiplied. Organizational information security officers and IT departments had to immediately focus on employees' home systems, networks, and Internet Service Providers (ISP) while maintaining the security of existing company networks. Teleconference capability providers, such as Zoom, instantly became household names and experienced unprecedented growth (Zoom, for example, saw a 30-fold increase in its use),^[1] and Virtual Private Networks became commonly used among the growing teleworking population.

This is a work of the U.S. Government and is not subject to copyright protection in the United States. Foreign copyrights may apply.



Colonel Jeffrey M. Erickson is the Director of the Army Cyber Institute at the United States Military Academy (USMA) located at West Point, New York. As Director, COL Erickson leads a 60-person, multi-disciplinary research institute focused on expanding the Army's knowledge of the cyberspace domain. He began his Army career as an Armor officer before transitioning to the Simulation Operations functional area, where for the last 15 years, he has been using simulations to train from the individual to the Joint and Combatant Command levels. He has a B.S. in Computer Science from the United States Military Academy, an M.S. in Management Information Systems from Bowie State University, and an M.S. in National Resource Strategy from the Eisenhower School (formerly the Industrial College of the Armed Forces). His fields of interest are simulations for live-virtual-constructive training, testing, and wargaming.

In addition to the technical challenges of this environment, we witnessed many interesting second and third-order effects that impact cybersecurity, including:

- ◆ Scammers intent on grifting money implemented some of the principles of Information Operations (IO) by appealing to users' emotions through powerful narratives such as fake charity funds for first responders.^[2]
- ◆ The merging of work and home life (which had been happening over the last few decades with the addition of home PCs, e-mail, smartphones, etc.) suddenly shot forward. Now, it is common for employees to be just as productive from home as in the office. Still, the expectation for responding to taskings (even after hours or on weekends) has almost obliterated the boundary between the private and work worlds.
- ◆ As telework became widely accepted, many companies began to realize potential savings by reducing high-cost office space.^[3] Likewise, employees realized some cost savings with reduced commutes and the ability to move to lower cost of living areas.
- ◆ The e-commerce economy saw impressive growth as consumers avoided in-store shopping. In many cases, this was the deathblow for many brick-and-mortar stores (with closings up to 10,000 by one estimate).^[4]
- ◆ As the pandemic continued, it became more politicized so that simple actions, even one such as wearing a mask, became divisive.^[5] Hostile actors (both domestic and foreign) leveraged these divisions to sow further dissent.
- ◆ The Anti-Vaxxer movement found new life as issues surrounding vaccination hesitancy, the US history of unethical medical testing, and government distrust came to the forefront.^[6]

As we look forward, it is possible (even likely) that we will be in an annual cycle of pandemic responses. Even with widespread vaccinations, it is probable that the annual flu season (usually a minor inconvenience for most Americans) will become a more significant event with widespread implications across the networked economy.

In this VUCA (Volatile, Uncertain, Complex, and Ambiguous) environment, our authors have produced a series of fascinating articles to help provide deeper understanding of the cybersecurity challenges and potential solutions. At the strategic level, in “COVID-19 and the Cyber Challenge,” GEN (Ret.) Keith Alexander and Mr. Jamil Jaffer assess the current situation’s complexity and reinforce the need for a whole-of-society approach, including the public and private sectors. Additionally, they highlight the need for clearly communicated and enforceable rules of behavior when dealing with threats.

Considering that a crisis to one is an opportunity to another, Mr. Rob Schrier asserts that future asymmetrical hybrid attacks could be used in the pandemic environment and similarly argues for a whole-of-nation approach in “COVID-19 and Cyber – Foreshadowing Future Non-Kinetic Hybrid Warfare.” In “Seven Cybersecurity Lessons Coronavirus Can Teach the Armed Forces (and Us All),” Mr. Ray Rothrock and Dr. Mike Lloyd use the current viral pandemic as an analogy for cybersecurity best practices, the application of cyber hygiene, and some insights into building resiliency.

In our Special Edition Research Articles, Dr. Chris Demchak argues that, in a rapidly changing world, we face a paradigm shift from Great Power Competition to Great Systems Conflict, and the need to build cyber resilience domestically and with allies. For those interested in understanding how the cyber environment can be used to support strategic narratives, Mr. Mark Bryan Manantan describes how the COVID-19 pandemic provided China the opportunity to further its strategic narrative using information warfare in “Unleash the Dragon: China’s Resilience in a Great Systems Conflict Era.” Continuing with a focus on China is United States Military Academy Cadet Tommy Hall’s book review of *Censored: Distraction and Diversion Inside China’s Great Firewall* by Margaret Roberts.

For a more holistic look at medical technology, Ms. Nataliya Brantley takes a broader look at the use of medical devices and their potential risks and vulnerabilities in “Homefront to Battlefield: Why the U.S. Military Should Care About Biomedical Cybersecurity.” Finally, in “The Initiation of State-Sponsored Cyberattacks,” Dr. Lance Hunter, Dr. Craig Albert, and Eric Garrett conduct an analysis of the factors that may indicate which types of states, in terms of capability and governance, are most likely to initiate cyberattacks against competitors. The authors provide some exciting results regarding asymmetrical conflict by looking at the Council on Foreign Relations Cyber Operations Tracker. You might be surprised who the likely aggressors are.

My hope is that you find these articles thought-provoking and perhaps motivate the larger community to apply these concepts not only to our current environment but to potential pandemics of the future. I want to thank and recognize the creativity and dedication of Michelle Marie Wallace, Sergio Analco, Gina Daschbach, LTC Mark Visger, SGM Jeff Morris, and Courtney Gordon-Tennant. The brilliant editing of the West Point Class of '70: Joe Reeder, Bill Spracher, Chip Leonard, and Bill Lane decidedly enhanced this special edition with their scholarly commitment and tireless effort.

Stay safe, stay alert, and stay informed. 🛡️

NOTES

1. N. Sherman, “Zoom sees sales boom amid pandemic,” British Broadcasting Corporation (BBC), June 2, 2020, accessed April 5, 2021, <https://www.bbc.com/news/business-52884782>.
2. “Coronavirus scams – consumer resources,” Federal Communications Commission (FCC), accessed April 5, 2021, <https://www.fcc.gov/covid-scams>.
3. R. Kailath, “Do I really need this much office space? Pandemic emptied buildings, but for how long?” NPR, September 1, 2020, accessed April 5, 2021, <https://www.npr.org/2020/09/01/906767790/do-i-really-need-this-much-office-space-pandemic-emptied-buildings-but-how-long>.
4. “US and UK Store Closures Review 2020 and US Outlook 2021,” Coresight Research, January 28, 2021, accessed April 5, 2021, <https://coresight.com/research/us-and-uk-store-closures-review-2020-and-us-outlook-2021/>.
5. E. Rabinovitch-Fox, “The battle over masks has always been political,” The Washington Post, November 18, 2020, accessed April 5, 2021, <https://www.washingtonpost.com/outlook/2020/11/18/battle-over-masks-has-always-been-political/>.
6. D. Thompson, “Anti-vaxxers wage campaigns against COVID-19 shots,” WebMD, January 29, 2021, accessed April 5, 2021, <https://www.webmd.com/vaccines/covid-19-vaccine/news/20210129/anti-vaxxers-mounting-internet-campaigns-against-covid-19-shots>.

THE CYBER DEFENSE REVIEW

◆ SENIOR LEADER PERSPECTIVE ◆

COVID-19 and the Cyber Challenge

General (Ret.) Keith B. Alexander
Jamil N. Jaffer

EXECUTIVE SUMMARY

Over the past year, a massive public health crisis has gripped the world, fundamentally changing the way individuals and entities work and interact with one another. This global pandemic has also caused new cyber threats to surface, along with the expansion of existing threats from criminal organizations and nation-states as well. This introductory piece sets out some of the key threat vectors in the cyber domain specific to COVID-19 that have emerged in the past year. It also highlights some potential paths forward to mitigate the risk presented in this new environment, including implementing critically important public-private collaboration to mitigate threats going forward.

THE VIRUS

In late December 2019, the World Health Organization (WHO) noted initial media statements emanating from China's Wuhan Province about "viral pneumonia" cases.^[1] Within weeks, researchers determined these cases were caused by a novel, rapidly spreading, and life-threatening coronavirus. Nations began assessing how they might protect their populations, with many instituting travel bans and the like, but the spread of the disease proved significantly hard to control,^[2] particularly given the globalized economic environment and the existence of rapid, long-distance travel. On March 11, 2020, the WHO determined that the spread and severity of COVID-19 had reached pandemic levels,^[3] and by early 2021, the virus had infected over 140 million individuals and killed over 3 million worldwide.^[4] With vaccines now approved and in distribution,^[5] some degree of relief appears on the horizon. Much depends however, among other things, on vaccine efficacy—particularly against new virus strains—and optimal vaccine distribution.

© 2021 General (Ret.) Keith Alexander, Jamil N. Jaffer



GEN (USA, Ret) Keith B. Alexander, former director of the National Security Agency and founding commander of U.S. Cyber Command, now serves as chairman, president, and co-CEO of IronNet Cybersecurity, a start-up technology company focused on securing public and private networks and systems from major cyber threats. He also serves on the Advisory Board of the National Security Institute at George Mason University's Antonin Scalia Law School.

The COVID-19-Driven Cyber Threat Environment

The COVID-19 pandemic, while principally a public health crisis, also hugely impacts how people work and interact with those around them. In parallel with these changes to the work and social environments of the global populace, we have seen a significant increase in cyber threats across the spectrum. For example, in August 2020, INTERPOL reported a major increase in cybercrime, with the INTERPOL Secretary General starkly warning that cybercriminals were developing new attacks at an “alarming pace, exploiting the fear and uncertainty caused by the unstable social and economic situation created by COVID-19.”^[6] The range of issues raised by the INTERPOL report includes potential threats from: (1) online scams and phishing attempts, with criminals posing as government and health authorities, looking to leverage concerns about and interest in the COVID pandemic in two-thirds of INTERPOL member countries; (2) disruptive malware, including ransomware and distributed denial of service attacks, targeting healthcare institutions and other critical infrastructure; (3) data harvesting malware used to obtain information, compromise systems and networks, extract data, and steal money; (4) malicious domains under COVID-related keywords to support criminal activities, with INTERPOL receiving nearly 600% increase in reported malicious domain registrations in a two-month period early in the coronavirus outbreak; and (5) a significant increase in misinformation and disinformation activities designed to raise anxiety, cause internal discord, and, in some cases, facilitate cyberattacks.^[7] INTERPOL reports in late 2020 also highlighted organized crime efforts to target vaccine storage facilities and distribution networks, with the INTERPOL Secretary General referring to vaccines as “liquid gold,” as well as exploitation of the COVID-19 pandemic by terrorist groups seeking to “reinforce their power and influence, particularly among local populations, or to expand their external financial resources.”^[8]



Jamil N. Jaffer, former chief counsel and senior advisor to the Senate Foreign Relations Committee who also served in senior national security roles in the Bush Justice Department and the White House, now serves as senior vice president for strategy, partnerships, and corporate development at IronNet Cybersecurity. He also serves as founder and executive director of the National Security Institute and is an Assistant Professor of Law at George Mason University's Antonin Scalia Law School.

One key change we have seen around the globe is that, where possible, companies, government agencies, and other organizations have largely pivoted to a remote work environment.^[9] One May 2020 estimate indicates that some 300 million globally now work from home.^[10] Moreover, while many organizations will return to a traditional working environment due to need or preference, employers and employees increasingly anticipate that many organizations will remain in a hybrid remote work posture going forward, with significantly more employee flexibility.^[11] This new work environment opens up potential new threat vectors in the cyber domain, as organizations adapt security practices to fit this new environment and extend their perimeter and other cyber defenses to home networks by using virtual private networks (VPNs) and other mechanisms. These systems are important to protect corporate content, but they can also expose a key route of access into corporate systems that attackers may be able to compromise.^[12]

In the US, the Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Agency (CISA) highlighted various cyber-related scams and threats seeking to exploit the COVID-19 pandemic and the new work environment. In mid-April 2020, the Secret Service and FBI jointly issued a warning that “the COVID-19 pandemic provides criminal opportunities on a scale likely to dwarf anything seen before,” warning that “[t]he speed at which criminals are devising and executing their schemes is truly breathtaking” and noting that the “sheer variety of frauds already uncovered is itself shocking.”^[13] These agencies also highlighted pandemic-related cyber fraud “targeting websites and mobile apps designed to track the spread of COVID-19 and using them to implant malware to steal financial and personal data,” threat actors “posing as national and global health authorities...to conduct phishing campaigns...designed to trick recipients...into downloading malicious code,” and major efforts to deploy code exposing vulnerable individuals and businesses to ransomware.^[14]

At the same time, cybersecurity companies had already begun reporting large increases in ransomware attacks, up nearly 150% between February and March 2020 alone.^[15] Moreover, in April 2020, CISA and the UK's National Cyber Security Centre (NCSC) issued an alert flagging a key increase in the number of financial attacks by malicious cyber actors exploiting the COVID-19 pandemic.^[16] Specifically, CISA and NCSC noted that SMS and email phishing campaigns, including campaigns designed to deploy malware, were exploiting interest in the coronavirus pandemic.^[17] CISA and NCSC also highlighted increased efforts to take advantage of the new work-from-home environment, with threat actors exploiting publicly known vulnerabilities in remote access software including Citrix and Microsoft RDP.^[18] The FBI likewise highlighted threats to business, including those arising out of the use of telework applications, such as remote desktop software, video conferencing, and Voice over Internet Protocol (VoIP) conference call systems, as well as potential supply chain threats stemming from computer rentals from foreign sources and an increase in Business Email Compromise (BEC) scams.^[19] In the same month, Google reported 18 million daily COVID-related malware and phishing emails, and more than 240 million COVID-related daily spam messages.^[20] Furthermore, in June 2020, FBI leadership testified before the Senate Judiciary Committee, reporting that the use of virtual assets and encrypted devices to launder stolen money as part of COVID-19 scams made it "increasingly difficult to track illicit finance flows and identify the criminal actors behind them."^[21] They also noted a significant uptick in "virtual asset fraud schemes related to COVID-19, including blackmail attempts, work-from-home scams, paying for non-existent treatments/equipment, and investment scams."^[22]

These trends have continued and expanded over the course of the pandemic, taking on a more nation-state-oriented focus. In May 2020, the FBI and CISA highlighted the potential threat to US organizations conducting COVID-19-related research from Chinese cyber actors, including efforts to obtain intellectual property (IP) and data related to vaccines, treatments, and testing.^[23] In late July 2020, the Justice Department announced charges against two Chinese hackers working for themselves and the Chinese Ministry of State Security (MSS), targeting companies, governments, non-governmental organizations, and individuals, stealing terabytes of data by targeting computer networks of companies developing COVID-19 vaccines, testing technology, and treatments.^[24] In May 2020, CISA and the UK's NCSC confirmed investigations of advanced persistent threat (APT) activity targeting healthcare and essential services, including pharmaceutical companies, universities, medical research organizations, and local governments, in part to obtain information on COVID-19-related research efforts.^[25] These actors were using techniques including password spraying and scanning targets for unpatched vulnerabilities, including those in Citrix software and VPN products from Pulse Secure, Fortinet, and Palo Alto, many of the systems also used to enable and protect the new at-home workforce.^[26] CISA and NCSC further noted significantly increased risk to international business supply chains because APT actors saw these supply chains as weak links, potentially enabling access to otherwise well-protected targets.^[27]

Likewise, the international financial system faces significant operational risks from well-resourced nation-state and key non-nation-state attackers, as remote work increasingly forces banks to identify and onboard new customers online and as regulatory bodies provide relief on typical anti-money laundering requirements.^[28] These risks are rendered even more serious because they arise in the context of a strong ongoing effort by the US and other governments worldwide to inject capital into their national and regional economies.^[29] Specifically, given the new pandemic environment, key international financial organizations assess that it is increasingly likely that online financial services will be used for money laundering, and that there is a major and growing risk of corruption and misuse of government stimulus funds and international financial aid.^[30]

Of course, we have also seen increased misinformation and disinformation by nation-states during the pandemic, whether to blame the US for the coronavirus, as in the case of China, Russia, and Iran,^[31] or to suggest that authoritarian governments may have an edge in fighting such diseases.^[32] All of these threats, taken together, demonstrate that the global geopolitical environment, particularly in cyberspace, is getting more dangerous as the pandemic continues forward.

Managing the Nation-State Cyber Threat During the COVID Epidemic

Given all this, key questions that authors in this special edition of *The Cyber Defense Review* will grapple include identifying and stopping cyber threats enabled by this global pandemic, addressing pandemic-related social media exploitation by nation-states, and ensuring government and industry continuity of operations. This edition's authors analyze these cyber risks with all the usual key policy and public issues in play, including data privacy, surveillance, the exploitation of public fears by adversarial nation-states, anxiety, existing social upheaval, national security, increased geopolitical risks, and ensuring appropriate national and international preparedness and resilience. Indeed, one of the key themes that surfaces across the various articles in this volume is the criticality of building strong and sustainable operational relationships within and across the public and private sectors and across international boundaries.

For far too long, the cybersecurity policy community has accepted as given the idea that organizations, both in the government and private sector, should each be primarily responsible for their own defense, whether against run-of-the-mill cyber adversaries or nation-state advanced persistent threats. However, as we argued in these pages nearly four years ago, if the goal is to create a truly defensible national (or international) cyber architecture, this approach makes little sense, at least against nation-state-level threat actors.^[33] The pandemic further highlights this challenge. Whether one discusses the threat to the vaccine development and distribution infrastructure posed by Chinese or Russian nation-state cyber actors, or nation-state efforts to undermine public confidence in private sector entities developing these capabilities, and regardless of whether such efforts are aimed at national political or economic goals, neither private nor public sector entities standing alone can realistically be

expected to defend themselves—or this nation—against nation-state-level threat actors in the cyber domain. Even the most capable of these entities—large financial sector organizations that have long faced significant, sustained cyber-attacks from a wide range of threat actors and which recognize such attacks as presenting “the biggest threat to the US financial system”^[34]—remain vulnerable when it comes to defending effectively. And, as noted above, such organizations have been a priority focus of nation-state and other key threat actors throughout the COVID-19 pandemic.^[35]

It is not just us nor the authors in this volume who have identified this serious challenge. Indeed, the Cyberspace Solarium Commission highlighted this same issue in its March 2020 report, in which the commissioners unanimously called for the public and private sectors to “arrive at a new social contract of shared responsibility to secure the nation in cyberspace.”^[36] As the Commission put it, creating true “collective defense in cyberspace requires that the public and private sectors work from a place of truly shared situational awareness and that each leverage its unique comparative advantages for the common defense.”^[37] Likewise, other authors in this journal recently highlighted the critical importance of public-private partnerships and collaboration noted in the Commission’s report.^[38] Moreover, as the pandemic has all too well highlighted, recent years have seen a fundamental shift in the cyber threat landscape, as attackers who once focused on government national security agencies are now pivoting to private sector companies and government institutions farther down the spectrum. The recently disclosed SOLARSTORM hack and associated efforts by the Russian SVR reflect this pivot as do the HAFNIUM hacks conducted against the Microsoft Exchange infrastructure by Chinese actors.^[39] Indeed, this particular hack’s targeting of national security and civilian government agencies and key private sector entities in the supply chain highlights the expanding scope and nature of the current threat.

The pandemic, SOLARSTORM, and HAFNIUM hacks have also illuminated the huge mismatch between threats and defenses in the modern cyber environment that can no longer go unaddressed. We can no longer expect individual companies—driven principally by the need to deliver products and services to consumers or other organizations—nor individual government agencies or states and localities—focused on their own constituencies—to stand alone against the threat posed by nation-state attackers who have access to virtually unlimited human, economic, and technical resources.^[40] Nor can we continue to expect key allies in regions threatened by overaggressive cyber actors—whether Chinese, Russians, Iranians, or North Koreans—to stand alone against these threats.^[41] Consistent with Cyberspace Solarium Commission recommendations, we must enhance the US ability to create shared situational awareness in cyberspace, including creation of a joint collaborative environment in the United States,^[42] as well as similar constructs with European^[43] and other allies.^[44] These capabilities will not only require large-scale collection and sharing of actionable cyber threat intelligence amongst the public and private sectors and with allies, but will also demand significant operational collaboration. Information sharing is but a means to an end. The ultimate

goal is truly enhanced, shared cybersecurity and the creation of a strong, sustainable defensive cyber fabric, which will require us to be highly efficient and effective in operating collectively across traditional divides.

Finally, it is important to note that the cyber threats that have surfaced in the wake of the pandemic, including the recent SOLARSTORM and HAFNIUM hacks, also underscore the vulnerability of our global supply chains, both in the physical world as well as in the cyber domain. Defending ourselves in this space effectively requires immediate action to build out and support an assured allied ecosystem for critical resources, both in technology and related industries, including innovation in cutting-edge communications capabilities, development and testing of semiconductors, mining and processing of the rare earth metals required by computing and other critical technologies, and supporting and expanding advancements in machine learning and quantum computing.^[45] We must also establish a clear, declarative policy on threats to our cyber infrastructure, ensuring the world fully understands our capability and resolve to impose crippling costs, both cyber and physical, on those who would do us harm whether nation-state actors or their proxies. Such policies must apply to those that would engage in, or even threaten, cyber operations that could seriously damage, destroy, disrupt, or modify key data or systems. Our bottom line should be a clear policy: the US will protect itself—both the public and private sectors—and our allies against serious hostile actions or threats against our cyber infrastructure with no less resolve than against threats in the physical domain.

If these recommendations seem edgy or forward-leaning, our experience living through the pandemic has demonstrated that the smart approach, when we see a threat surfacing on the horizon, is to act in advance, rather than waiting for it to arrive on our shores. We can now see clearly the threat that nation-state adversaries present to our modern economy and national security; the question remains whether we finally have the resolve and fortitude to do what is necessary to meet it head on.🛡️

NOTES

1. World Health Organization, *Listings of WHO's Response to COVID-19*, June 29, 2020, <http://who.int/news/item/29-06-2020-covidtimeline/>.
2. Chad R. Wells, et al., *Impact of International Travel and Border Control Measures on the Global Spread of the Novel 2019 Coronavirus Outbreak*, Proceedings of the National Academies of Sciences of the United States of America (March 31, 2020), <https://www.pnas.org/content/117/13/7504>.
3. World Health Organization, *Listings of WHO's Response to COVID-19*, *supra* n. 1.
4. World Health Organization, *WHO Coronavirus Disease (COVID-19) Dashboard* (February 24, 2021), reporting 111,762,965 cases of COVID-19 worldwide and 2,479,678 deaths, <https://covid19.who.int/>.
5. U.S. Food and Drug Administration, COVID-19 Frequently Asked Questions, (noting that “[o]n December 11, 2020, the FDA issued an Emergency Use Authorization (EUA) for the use of the Pfizer-BioNTech COVID-19 Vaccine...[and] [o]n December 18, 2020, the FDA issued an EUA for the use of the Moderna COVID-19 Vaccine.”), <https://www.fda.gov/emergency-preparedness-and-response/coronavirus-disease-2019-covid-19/covid-19-frequently-asked-questions#biologics>.
6. INTERPOL, *INTERPOL Report Shows Alarming Rate of Cyberattacks During COVID-19* (August 4, 2020), <https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19>.
7. *Ibid.*
8. INTERPOL, *COVID-19 Crime: INTERPOL Issues New Guidelines for Law Enforcement* (November 17, 2020), <https://www.interpol.int/en/News-and-Events/News/2020/COVID-19-crime-INTERPOL-issues-new-guidelines-for-law-enforcement>; INTERPOL, *INTERPOL Warns of Organized Crime Threat to COVID-19 Vaccines* (December 2, 2020), <https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-warns-of-organized-crime-threat-to-COVID-19-vaccines>; INTERPOL, *INTERPOL – Terrorist Groups Using COVID-19 to Reinforce Power and Influence* (December 22, 2020), <https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-Terrorist-groups-using-COVID-19-to-reinforce-power-and-influence>.
9. Rita Zeidner, *Coronavirus Makes Work from Home the New Normal*, Society for Human Resource Management (March 21, 2020), <https://www.shrm.org/hr-today/news/all-things-work/pages/remote-work-has-become-the-new-normal.aspx>.
10. Juan Carlos Crisanto and Jermy Prenio, *Financial Crime in Times of COVID-19 – AML and Cyber Resilience Measures*, *FSI Briefs*, No. 7 (May 2020), <https://www.bis.org/fsi/fsibriefs7.pdf>, 2.
11. PriceWaterhouseCoopers, *It's Time to Reimagine Where and How Work Will Get Done*, PwC's US Remote Work Survey (January 12, 2021), <https://www.pwc.com/us/en/library/covid-19/us-remote-work-survey.html>; Brodie Boland, et al., *Reimagining the Office and Work Life after COVID-19* (June 8, 2020), McKinsey & Co., <https://www.mckinsey.com/business-functions/organization/our-insights/reimagining-the-office-and-work-life-after-covid-19#>.
12. National Security Agency, *Mitigating Recent VPN Vulnerabilities* (October 7, 2019), <https://media.defense.gov/2019/Oct/07/2002191601/-1/-1/0/CSA-MITIGATING-RECENT-VPN-VULNERABILITIES.PDF>; Vijay Sarvepalli, *VPN – A Gateway for Vulnerabilities*, Carnegie Mellon University: Software Engineering Institute (November 13, 2019), <https://insights.sei.cmu.edu/cert/2019/11/vpn---a-gateway-for-vulnerabilities.html>.
13. Federal Bureau of Investigation, *FBI and Secret Service Working Against COVID-19 Threats* (April 15, 2020), <https://www.fbi.gov/news/pressrel/press-releases/fbi-and-secret-service-working-against-covid-19-threats>.
14. *Ibid.*
15. VMWare Carbon Black, *Amid COVID-19, Global Orgs See a 148% Spike in Ransomware Attacks; Finance Industry Heavily Targeted* (April 15, 2020), <https://www.carbonblack.com/2020/04/15/amid-covid-19-global-orgs-see-a-148-spike-in-ransomware-attacks-finance-industry-heavily-targeted/>.
16. Department of Homeland Security, *COVID-19 Exploited by Malicious Cyber Actors*, CISA Alert AA20-099A (April 8, 2020), <https://www.us-cert.gov/ncas/alerts/aa20-099a>.
17. *Ibid.*
18. *Ibid.*
19. Federal Bureau of Investigation, *Cyber Actors Take Advantage of COVID-19 Pandemic to Exploit Increased Use of Virtual Environments*, Alert Number I-040120-PSA (April 1, 2020), <https://www.ic3.gov/Media/Y2020/PSA200401>.

NOTES

20. Steven Musil, *Google Blocking 18M Malicious Coronavirus Emails Every Day*, CNET (April 15, 2020), <https://www.cnet.com/news/google-seeing-18m-malicious-coronavirus-emails-each-day/>.
21. Calvin A. Shivers, *Statement Before the Senate Judiciary Committee: COVID-19 Fraud: Law Enforcement's Response to Those Exploiting the Pandemic* (June 9, 2020), <https://www.fbi.gov/news/testimony/covid-19-fraud-law-enforcements-response-to-those-exploiting-the-pandemic>.
22. Ibid.
23. Federal Bureau of Investigation, *People's Republic of China (PRC) Targeting of COVID-19 Research Organizations* (May 13, 2020), <https://www.fbi.gov/news/pressrel/press-releases/peoples-republic-of-china-prc-targeting-of-covid-19-research-organizations>.
24. Department of Justice, *Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including COVID-19 Research* (July 21, 2020), <https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion>.
25. Cyber and Infrastructure Security Agency, *APT Groups Target Healthcare and Essential Services*, Alert AA20-126A (May 5, 2020), <https://us-cert.cisa.gov/ncas/alerts/AA20126A>.
26. Ibid.
27. Ibid.
28. Crisanto and Prenio, *Financial Crime*, *supra* n. 10, 2-4, 6-8.
29. Tim Maurer and Arthur Nelson, *COVID-19's Other Virus: Targeting the Financial System*, Carnegie Europe (April 21, 2020), <https://carnegieeurope.eu/strategieurope/81599>.
30. Crisanto and Prenio, *Financial Crime*, *supra* n. 10, 2.
31. Natasha Bajema and Christine Parthemore, *How to Counter China's Coronavirus Disinformation Campaign* (March 29, 2020), *Defense One*, <https://www.defenseone.com/ideas/2020/03/how-counter-chinas-covid-19-disinformation-campaign/164188/>; Julian Barnes, et al., *As Virus Spreads, China and Russia See Openings for Disinformation* (March 28, 2020); *The New York Times*, <https://www.nytimes.com/2020/03/28/us/politics/china-russia-coronavirus-disinformation.html>; U.S. State Department, *Iran: COVID-19 Disinformation Fact Sheet* (March 23, 2020), <https://www.state.gov/iran-covid-19-disinformation-fact-sheet/>.
32. Will Knight, *China Flexes Its Soft Power With 'Covid Diplomacy'*, *Wired* (April 2, 2020), <https://www.wired.com/story/china-flexes-soft-power-covid-diplomacy/>.
33. Keith B. Alexander, et al, *Clear Thinking About Protecting the Nation in the Cyber Domain*, *The Cyber Defense Review*, Vol. 2 No. 1, 29, 33, (2017), https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/Clear%20Thinking%20About%20Protecting_Alexander_Jaffer_Brunet.pdf?ver=2018-07-31-093723-563.
34. Jamie Dimon, *Letter to Shareholders*, 35, JP Morgan Chase (April 2019), <https://www.jpmorganchase.com/corporate/investor-relations/document/ceo-letter-to-shareholders-2018.pdf>.
35. Jamil N. Jaffer, *Prepared Statement of Jamil N. Jaffer on Cybercriminals and Fraudsters: How Bad Actors Are Exploiting the Financial System During the COVID-19 Pandemic*, Subcommittee on National Security, International Development and Monetary Policy, United States House of Representatives Committee on Financial Services (June 16, 2020), <https://nationalsecurity.gmu.edu/wp-content/uploads/2020/06/Jaffer-House-Financial-Services-Subcommittee-Testimony-on-Financial-Sector-Cyber-Threats-For-Circulation-6.15.20.pdf>.
36. Cyberspace Solarium Commission, *Commission Report* (March 2020), 96, <https://www.solarium.gov/report>.
37. Ibid.
38. Joe Reeder and Robert E. Barnsby, *A Legal Framework for Enhancing Cybersecurity through Public-Private Partnership*, *The Cyber Defense Review* (Fall 2020), https://cyberdefensereview.army.mil/Portals/6/Documents/2020_fall_cdr/CDR%20V5N3%2003_Reeder_Barnsby.pdf.
39. Federal Bureau of Investigation, et al., *Joint Statement by the Federal Bureau of Investigation, the Cybersecurity and Infrastructure Security Agency, the Office of the Director of National Intelligence, and the National Security Agency (NSA)* (Jan. 5, 2021), <https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure>.

NOTES

40. Keith B. Alexander and Jamil N. Jaffer, *The Other Crisis: U.S. Companies Still Need Help Against Cyberattacks*, *Barron's* (March 26, 2020), <https://www.barrons.com/articles/cyberspace-solarium-commission-urges-collective-defense-51584364449>.
41. Keith B. Alexander and Jamil N. Jaffer, *Ensuring US Dominance in Cyberspace in a World of Significant Peer and Near-Peer Competition*, 19 *Geo. J. Int'l Aff.* 51, 52-58 (Fall 2018), <http://nationalsecurity.gmu.edu/wp-content/uploads/2018/10/GJIA-19-1-FINAL-rev-57-72.pdf>.
42. *Cyberspace Solarium Commission Report*, *supra* n. 35, 101-102.
43. Keith B. Alexander (with Jamil N. Jaffer), *A Transatlantic Alliance Is Crucial in an Era of Cyberwarfare*, *Financial Times* (September 4, 2018), <https://www.ft.com/content/c01a7f94-af81-11e8-87e0-d84e0d934341>.
44. Keith B. Alexander and Jamil N. Jaffer, *Iran's Coming Response: Increased Terrorism and Cyber Attacks?* *The Hill* (May 15, 2019), <https://thehill.com/opinion/national-security/443610-irans-coming-response-increased-terrorism-and-cyber-attacks> (Middle East allies); *Ensuring U.S. Dominance*, *supra* n. 38, 52-58 (Asian and other allies); Jamil N. Jaffer, *U.S.-India Relations on Cybersecurity: An Important Moment for Strategic Action on Collective Cyber Defense* in *ENHANCING U.S.-INDIA STRATEGIC COOPERATION* (Manchester University Press, 2021, forthcoming).
45. Keith B. Alexander and Jamil N. Jaffer, *China Is Waging Economic War on America. The Pandemic Is an Opportunity to Turn the Fight Around*, *Barron's* (August 4, 2020), <https://www.barrons.com/articles/china-is-waging-cyber-enabled-economic-war-on-the-u-s-how-to-fight-back-51596587400>.

COVID-19 and Cyber – Foreshadowing Future Non-Kinetic Hybrid Warfare

Rob Schrier

ABSTRACT

2020 was a year like no other in our lifetime. The COVID-19 Pandemic had a broadly evident and devastating impact on our health, our society, and our economy. Less evident have been adversaries' attempts to employ cyber-attacks^[1] to exacerbate the pandemic through cyber-based disruption, exploitation and cyber-driven disinformation. The focus of this essay is on the nexus between cyber security and our future biological threat security (biothreat security). This article begins with a few key questions. What have we learned from observing adversary cyber tradecraft this year? What can we surmise our adversaries have learned from trying to take advantage of the current pandemic that they will use against the US in the future? More importantly, what can we extrapolate from these observations for the future of cyber-attack as the key element of strategic hybrid non-kinetic warfare?

My worst-case version of the future envisions adversaries creating or taking advantage of biothreat security events (or natural disasters) and using cyber-attacks and disinformation in multiple ways to aggravate the situation in a new form of hybrid non-kinetic warfare. We must predict the adversary's potential strategies for the future cyber-driven hybrid non-kinetic warfare and we must determine what we must do to prevent, preempt, or counter that future with our own disruptive campaigns. As a nation we need a level of resolve we do not have today to defend ourselves against cyber-attacks and their effects. While biothreat security is the sole focus of this essay, many of these ideas can be applied to climate events and other disruptions that impact key areas of the critical infrastructure, and our security more generally.



Rob Schrier is the Chief of Staff of Asymmetric Operations Sector of Johns Hopkins Applied Physics Laboratory. He leads research on military cyber and information operations (IO). He moved to the Laboratory after retiring from the DoD Senior Executive Service after a thirty-six year career. He served as the Deputy to the Commander, Cyber National Mission Force (CNMF), U.S. Cyber Command. Mr. Schrier was a plank holder on the team who established U.S. Cyber Command and served as the initial Deputy Director for Current Operations. Throughout his career, he held a variety of DoD leadership positions after beginning his career as an analyst. Mr. Schrier has more than ten years' experience as a leader in cyber operations. Mr. Schrier earned a Bachelor of Arts Degree from the University of Maryland, a Master of Science Degree in Applied Behavioral Science from Johns Hopkins University and attended the Chairman, Joint Chiefs of Staff CAPSTONE Course.

2020 OBSERVATIONS

The 2020 pandemic with its societal impacts provided a rich environment for cyber adversaries. While COVID-19 has had global impact, so have the increases in 2020 cyber-attacks, and this confluence has prompted several pundits to characterize 2020 as the year of “the Cyber Pandemic”.^[2] The 2020 cyber-attack landscape was quite widespread. We witnessed direct cyber-attacks on health organizations including the World Health Organization, pharmaceutical companies, medical research organizations and individuals through health-focused phishing emails. There were undoubtedly cyber-attack attempts to impact the outcome of the 2020 US federal election. We witnessed a surge in ransomware attacks against a range of targets including hospitals, schools, and local governments, some of which seemed motivated to exacerbate both the health and societal impacts of the pandemic. We witnessed perhaps the deepest, broadest supply-chain attack ever observed against the US government, and private industry.^[3] Growing cyber-enabled disinformation attacks were a major feature of the 2020 cyber landscape. While it is hard to measure their long-term impact yet, there undoubtedly was some significant impact. As the American workforce largely transformed overnight from an office workforce to a remote workforce, we collectively became far more vulnerable to cyber-attack. In October 2020, 58% of the American workforce worked remotely either all or some of the time. The number was even higher in April 2020.^[4] There is the prospect that a significant increase in remote work is here to stay. Also, much as the aftermath of 9/11 saw an increased focus on security against terror threats, an increased focus on biothreat security will hopefully be here to stay.

How Adversaries Can Employ Cyber-Attack

The focus for the rest of this article is about how our adversaries will use cyber-attacks to achieve strategic non-kinetic hybrid warfare objectives in the future and

what we should do to keep them from being successful. Too many of us regard cyber-attacks as being for “cyber sake” and do not focus attention on cyber as a means to a strategic end. While none of this is new, our experiences with the 2020 pandemic have raised the likelihood of cyber-attack being the critical ingredient of future strategic hybrid non-kinetic warfare, especially events involving biothreat security.

2020 has clearly shown how vulnerable our security against biothreats is, whether against natural biological events, manmade biological attacks or adversary-driven natural biological attacks. The impacts of the COVID-19 pandemic, beyond the pure health aspects, are indisputable and they have exposed cyber vulnerabilities in every facet of our health ecosystem. They have also exposed vulnerabilities in our broader supply chain and redefined how we view the supply chain. For example, early in the pandemic, normally routine daily items like toilet paper, paper towels, cleaning and disinfecting products were in short supply and therefore a huge focus of the population and a potentially exploitable vulnerability. There was also a variety of domestic and global food supplies that had trouble reaching the shelves of grocery stores, creating a sense of a food shortage, even though there never actually was a food shortage in the US.^[5] Finally, cyber-driven disinformation has clearly exacerbated the impact of the pandemic, our processes to measure and quantify their specific impacts are immature and still evolving.

Health Ecosystem Cyber Threat Landscape

So, I would like to offer my incomplete layperson’s view of the health ecosystem cyber threat landscape as an adversary might see it. This is by no means a comprehensive examination by a biothreat security expert, so it is bound to be incomplete.

There are key vulnerabilities in every facet of the health ecosystem, including data security and health privacy information, health infrastructure and process security which also include research, clinical health practices, communications and public health, and public and government perceptions of the validity of the science and data. As adversaries look to employ cyber to achieve outcomes against this ecosystem, the following are exemplars of both public and private vulnerable areas they may target, though again this is by no means a comprehensive list:

- ◆ Medical equipment and medically relevant cyber systems used for research, medical storage, testing and treatment, to include remote care, in both the private, non-profit and public domains
- ◆ Medical equipment and their cyber systems used in creating or distributing pharmaceuticals and active pharmaceutical ingredients (APIs)
- ◆ Cyber systems associated with medical databases, health surveillance data, patient information and health records
- ◆ Cyber systems associated with government organizations overseeing healthcare and managing research, such as the CDC, NIH, FDA and others

- ◆ Medical communications systems that convey medical appointments, test results and other information through cyber driven communications systems (generating emails, text messages, etc. to patients or staff)
- ◆ The underlying supply chain driving the entire health ecosystem
- ◆ The private and professional emails of doctors, researchers, nurses, local, state, tribal, and federal government officials associated with the health ecosystem
- ◆ Disinformation against the general population and personnel in the health ecosystem.

While each of these cyber vulnerable areas is threatened individually, an even more serious strategic threat comes from an adversary mounting a campaign with attacks in several of these areas, planned in a way to achieve a specific strategic goal. Our adversaries have gained a tremendous amount of open-source intelligence by observing the pandemic this year through the lens of categories such as those listed above.

Cyber Driven Hybrid Non-Kinetic Warfare Scenarios

This leads us to the future of cyber-driven hybrid non-kinetic warfare and the central role that cyber may play in every facet of non-kinetic conflict. So, let's walk through a few representative, realistic future scenarios.

These scenarios could begin with either a natural biological event or with a manmade biological attack. For purposes of these scenarios, we focus on a natural biological event. An adversary will employ cyber-attacks in a number of ways to transform the biological event into a far more strategically consequential attack. The adversary will consider the primary outcomes it wishes to bring about. Does it want to focus on increasing loss of life or number of ill/casualties, overwhelming our healthcare system? Sow confusion to impact our economy, create societal friction, or undermine confidence in the government? Sow mistrust among US Allies? Degrade some industry or service to increase its own international market share or international political standing? While we may never know the precise motivation behind an adversary's cyber actions, it is important to regard the adversary in terms of the strategic motivations that may drive its coordinated actions.

To realize these goals, an adversary may want to cause failures (either recognized or not recognized) in medical equipment or databases, which will result in degrading healthcare delivery. It can corrupt health surveillance data that will impact decision making, testing and treatment. The adversary may attack actual medical equipment or accompanying infrastructure and communications to disrupt our response, such as within testing or manufacturing equipment. For example, if an adversary blocks or deletes a database that contains the list of patients eligible and prioritized for a vaccine or treatment, then long lines waiting for that vaccine or treatment will grind to a halt and healthcare will be delayed for a large number of people. A similar scenario involves an adversary interdicting an automated process to notify

patients via text message or email of their medical appointment times for tests, vaccines, or treatment, that then send a large number of patients to healthcare locations to overwhelm and confuse the healthcare system.

The adversary may take steps to disrupt the medical research process. It can achieve this through compromising research equipment or the integrity of the research data, or by using disinformation through the introductions of false reports (variants of concern, vaccine efficacy, vaccine resistance, greater disease transmission, higher lethality, false alternative treatments, etc.) and combining this disinformation with the cyber compromises.

There are even more insidious or nefarious potential scenarios. An adversary can interfere with or corrupt the manufacture and distribution of pharmaceuticals, APIs, vaccine, or testing. The adversary can conduct cyber exploitation of the entire health ecosystem to gain intelligence advantage and targeting data. As part of this scenario, undoubtedly a part of any adversary cyber-attack campaign will include the attack and exploitation of email accounts associated with public or private healthcare officials through phishing attacks and other means. The adversary will then use disinformation as a weapon to exacerbate the strategic impact of any of the above scenarios. The disinformation will be critical to getting our general population to lose confidence in vaccines, testing, treatments, and overall effectiveness of the public and private health care system. Almost all information paths are cyber-based (or at least cyber-influenced); therefore, the cyber and cognitive elements of disinformation are intertwined.

The most troubling aspect of the scenarios above is that a determined adversary will weave together several of its cyber-attack capabilities into a focused campaign. That is why the above scenarios are representative and not meant to be comprehensive. The key point is that an adversary's campaign approach poses a very serious strategic danger to the US and our Allies. In a sense the US was lucky in the current pandemic, as it seems no adversary had a multi-faceted campaign already in place and could not take full advantage of cyber vulnerabilities across our entire biosecurity ecosystem. However, some were opportunists with capabilities ready to employ and we should assume they have observed and learned from 2020 actions—theirs and ours.

Accepting the Premise of Cyber-Attack Driven Hybrid Non-Kinetic Warfare, What Steps Can the US Government Take?

I have painted some dire scenarios for the future. We must not passively accept these scenarios as inevitable. First, we must face the brutal facts regarding both our level of vulnerability and our adversaries' will and intentions. Second, we must be resolute, even through all the challenges, to gain and maintain an upper hand. We need to be willing both to have a sense of urgency and to regard this as a long game and demand that government, industry, non-profits, and academia put tremendous energy into solving these problems as if our national safety and security depend on it—as it does.

The best way the US can ensure that adversaries can never actualize the above scenarios or other cyber threats to our biothreat security, both in pandemic events but also in broader biothreat events, is to create a whole-of-nation campaign to disrupt our adversaries and keep the cyber risk to our biothreat security very low. The following are the key elements of that campaign.

- ◆ The government must continue to prioritize and significantly expand “persistent engagement” as the cornerstone of our overall cyber defense.^[6] We must continuously contest our cyber adversaries outside of US networks to keep them off balance. We will never successfully defend our health ecosystem from cyberattack just by trying to close down vulnerabilities within our own networks. This tracks with a recommendation from the Solarium Commission’s Recommendation Pillar 6 (Preserve and Employ the Military Instrument of National Power).^[7]
- ◆ The US must develop a comprehensive biothreat security strategy that includes a focused effort to assess and improve cybersecurity and cyber defense across the entire public and private health ecosystem. This will be a major undertaking that will require public, private, non-profit and academic collaboration.
- ◆ Immediately implement the Solarium Commission’s Recommendation Pillar 1 (Reform the U.S. Government’s Structure and Organization for Cyberspace). The government must create a National Cyber Director as outlined in the report to kickstart a whole-of-government approach to national Cyber Defense and accelerate building the public-private partnership.
 - I urge moving beyond one of the Commission’s recommendations and opting for my more aggressive recommendation to create an effective national level 24/7 cyber defense operational capability.^[8]
- ◆ Implement the Commission’s Recommendation Pillar 5 (Operationalize Cybersecurity Collaboration with the Private Sector). Building an operationally credible private-non-profit-international-US government partnership will produce a critical layer of cyber defense which today may be our weakest area. We need to find innovative ways to harness the enormous cyber power of the private sector, who will be critical in securing our health ecosystem including key medical equipment.
- ◆ Finally, we need to develop and implement a national strategy to prevent, counter and mitigate the impacts of disinformation against US and Allied interests. This strategy should be developed with a focus largely on cyber-attack since cyberspace is a key factor in virtually all facets of disinformation and should be developed as part of the broader cyber recommendations and not apart from them. Preempting and countering disinformation must become a key part of our defending forward strategy.

The key will be for the US to execute these recommendations as a continuous campaign, since the strategic biothreat security threats to our nation are here to stay. Our strength will be in coordinating efforts to carry out the above recommendations and combining their effects. While there will be those who disagree with my specific recommendations, my hope and expectation is that my depiction of the threat landscape and representative scenarios will spark further dialogue and debate, so as a nation we can put our tremendous energy into solutions for these problems that our national safety and security can depend on over the long term.🇺🇸

NOTES

1. The term cyber-attack will be used throughout this paper in a broad non-doctrinal definition to represent offensive cyber operations, cyber exploitation and cyber-driven disinformation.
2. Don Lohrmann, Government Technology Magazine, December 12, 2020, “2020: The Year the COVID-19 Crisis Brought a Cyber Pandemic.”
3. Kai Paul, The Guardian, “What you need to know about the biggest hack of the US government in years”, 15 December 2020 and Ellen Nakashima, The Washington Post, February 23, 2021, “Biden administration preparing to sanction Russia for Solar Winds hacks and the poisoning of an opposition leader.”
4. Megan Benan, Gallup News, October 13, 2020, “COVID-19 and Remote Work: An Update.”
5. USDA Report, “Will COVID-19 Threaten Availability and Affordability of our Food?,” posted by Robert Johansson, USDA, Chief Economist in Food and Nutrition Magazine, April 16, 2020; Amy Gunia, Time Magazine, May 8, 2020, “How Coronavirus is Exposing the World’s Fragile Food Supply Chain – and Could Leave Millions Hungry.”
6. Foreign Affairs Opinion, “How to Compete in Cyberspace – Cyber Command’s New Approach,” Authors Paul Nakasone and Michael Sulmeyer, August 25, 2020. In this opinion, the authors write, “Cyber Command implements this defend forward strategy through the doctrine of persistent engagement. The idea behind persistent engagement is that so much of the corrosive effects of cyber-attacks against the United States occur below the threshold of traditional armed conflict. Yet much of Cyber Command’s combat power had been devoted toward preparations in the event of future contingencies. We realized that U.S. Cyber Command needs to do more than prepare for a crisis in the future; it must compete with adversaries today. This doctrine of persistent engagement reflects the fact that one-off cyber operations are unlikely to defeat adversaries. Instead, US forces must compete with adversaries on a recurring basis, making it far more difficult for them to advance their goals over time.”
7. Cyberspace Solarium Commission Report, Cyberspace Solarium Commission - Report, March 2020.
8. Rob Schrier, *The Cyber Defense Review*, Fall 2019, Volume 4, Number 2, 23-26.

THE CYBER DEFENSE REVIEW

◆ PROFESSIONAL COMMENTARY ◆

Seven Cybersecurity Lessons the Coronavirus Can Teach the Armed Forces (and Us All)

Dr. Mike Lloyd
Ray Rothrock

If we have learned anything from the COVID-19 pandemic, it is that very bad things can happen very quickly, especially if we are not sufficiently prepared. It turns out that everything we have been told about the pandemic is also relevant for cybersecurity; as such, the pandemic is an exceptional learning tool for cyber professionals.

Cyberattacks are like biological viruses in several ways: they can spread incredibly fast, their consequences can wreak huge economic damage, and the destruction they cause can be very difficult from which to recover. Viruses spread through human social networks and cyber-attacks exploit our online networks of trust.

Viruses and cybercrime are conceptual and invisible, which can make it challenging to understand how they propagate and how they can be stopped. Analogies can be helpful, and there is a strong connection between COVID-19 and cybersecurity that can increase our understanding. We have been forced to learn what it takes to stop a virus; those lessons are helpful here.

Security leaders have long predicted that a major cyberattack was right around the corner and that it would fundamentally alter society as we know it. In 2013, Secretary of Homeland Security Janet Napolitano predicted, “Our country will, at some point, face a major cyber event that will have a serious effect on our lives, our economy and the everyday functioning of our society.”

COVID-19 proves that the world is truly at great risk of disruption. It should lead those of us in cybersecurity to think of what a COVID-like cyber event might look like: no clear attacker, no clear symptoms, a lot of doubt about who or what has been infected, who is carrying the disease and who is not, a lot of disturbance—and the need to break out of the normal ways of doing things.

© 2021 Dr. Mike Lloyd, Ray Rothrock



Dr. Mike Lloyd is an epidemiologist-turned-chief technology officer of RedSeal, a cloud security company. He holds 21 patents earned over more than 25 years of modeling and controlling fast-moving, complex security and network systems. His leadership as CTO has propelled RedSeal and its technology to win nearly 30 awards for excellence since 2018.

To prepare for this kind of event—one that will spread fast and far and will have an equal or greater economic impact—here are seven lessons security teams can glean from the pandemic.

#1: Understand Lateral Movement

Our lives are globally interconnected, and we spread disease as we connect with each other. The fact is that this pandemic started in one country and spread to even small, remote island communities is the first example in our lifetime that makes this point on a global scale.

Similarly, digital attackers need to only breach one target to start their infiltration. However, despite security teams' best efforts, it is impossible to protect all our networks down to every endpoint all the time.

Once an attacker finds an "in" to the network, it usually takes just a few lateral moves to get from one place to anywhere else on the network. Unfortunately, there are still organizations where, once the intruder gets inside their network, it is too easy to move around. An attacker can stay hidden and move with impunity.

The analogies are so close that it is difficult to distinguish when we are talking about lateral movement of a disease and when we are talking about lateral movement of cyber attackers. They really do behave in similar ways.

In this analogy, air travel and super-spreader events are opportunities for real-world bugs. When we wear masks, wash hands and practice social distancing, we greatly reduce the virus' opportunity for lateral movement. Likewise, digital defenders need to break up lateral movement across their complex networks—essentially social distancing for the network brought about by reducing access to critical assets.



Ray Rothrock is executive chair of RedSeal, and the author of *Digital Resilience: Is Your Company Ready for the Next Cyber Threat?*, one of the Top 10 must-reads on information security. He has three decades of investing in, advising and leading many of the tech and cyber companies that form the fabric of today's networks, and is a member of the Nuclear Threat Institute's Board of Directors and its Science and Technology Advisory Group.

#2: Identify Problem Areas

Some countries—and even cities—have better success in fighting coronavirus because they can quickly identify where the disease really is, and focus efforts to stop its progress. This is why testing is so important and why communities that use contact tracing to identify carriers and their contacts, test them promptly, and quarantine as necessary make strong progress in reducing infection rates.

Digital security is the same. Teams work to know where their network is infected, and then response teams scramble to quarantine or block the intruders. When they are able to know quickly where the problem is, they can respond more effectively and efficiently to prevent its spread.

Unfortunately, the cyber version of contact tracing is much harder because computers communicate across a network in many different and shifting directions. The equivalent would be if contract tracers had to deal with every person on earth flying to at least one new country every day.

The best course of action is to map out a network well ahead of an attack and understand where one's critical assets are. Security teams need to understand all the access pathways and normal information flows for the organization ahead of time. Thankfully, automation products exist to help network managers keep track of all the detail and the constant changes.

#3: Slow the Spread

By sheltering in place and not coming in contact with other people, we impede the coronavirus' ability to spread among the population. As a result, this global effort to stay home and "flatten the curve" reduces strain on our taxed medical systems.

Similarly, when digital defenders wall data and network communications into distinct areas, they can make it harder for attackers to expand their intrusion. We cannot stop every determined attacker or nation-state, but we can slow it down. Ultimately, slowing attackers down buys time to detect them so one can effectively respond by blocking or quarantining them.

#4: Practice Good Hygiene

Basic hygiene is the main way we have to combat the spread of COVID-19. Our first line of defense in this unprecedented pandemic is everyone's consistent use of basic hygiene: hand washing, not touching faces, and using face masks 100% of the time when in public. People not practicing basic hygiene eventually endanger us all by increasing the probability of a viral transfer.

Similarly, not practicing basic cyber hygiene endangers organizations. Poor or inconsistent cyber hygiene includes failing to change passwords regularly, randomly clicking on internet links, or neglecting to enable all available security features on devices, such as firewalls and antimalware.

The good news is that it is possible for people to improve their hygiene habits. The pandemic showed us that hundreds of millions of people can change their behavior if they think they or their loved ones are at risk.

Basic cyber hygiene depends on applying current security advice, not just in one or two places, but consistently across one's entire organization, network, and its component parts. This means the organization will be less likely to battle common cybersecurity issues.

Device hardening, dual-factor authentication, and other practices are critical to tamping down the threats and reducing the attack surface. These may be even more important than the best technological defense.

One must know what devices are on the network; one also wants to make sure those devices are securely configured. One needs to confirm the network is set up as intended, and, when something changes, one needs confirmation that the network's security is up to the challenge. Cyber wargaming plays an important role here. Cyber terrain modeling can automatically map networks and identify defensive weaknesses.

Real-world networks are riddled with unintentional hygiene failures. As with fighting this pandemic, even 95 percent compliance with basic hygiene standards is not enough. It takes only one unintentional exposure for COVID-19 to spread, and it is the same for cyber as well. That is why it is imperative to perform the basics well, everywhere, all the time.

#5: Adapt and Evolve

Humans are the most successful animals on the planet because of their adaptability.

Network defenders need to adapt and evolve, too. What was considered decent security yesterday is routinely out of date today. Tactics keep shifting, new vulnerabilities are continually

discovered, and the rules for defense never settle down. We can continue to get better at blocking certain kinds of cyberthreats, but as soon as we do, the attackers will find a way around. This means our countermeasures must keep changing.

When battling real viruses, we cannot win with rigidity. The only long-term advantage is to maintain adaptability. In cyber, we must be flexible, and we can do that only by modelling and understanding—in effect, to do the equivalent of war games against our networks.

Security teams should plan to become adept at the sort of penetration-testing exercises that the average company currently does only once a year or so. Cyber threats and coronaviruses continually evolve and adapt. One needs to do the same, because every day will present a new and different set of challenges.

#6: Social Distance the Network

Modern computing allows software to run with wild abandon, sharing virtual machines and containers on limited physical resources. At first, this was a great advantage, because we could make one computer do the job of several and we could reallocate inefficiently used resources to where they could make a difference.

However, in the face of the ever-shifting cyber landscape, one of network security teams' greatest challenges is getting overwhelmed. To avoid this, they need to adopt and apply new strategies and ideas. In this case, social distancing is one of the most important lessons to carry from the pandemic into online security.

Security personnel must think like public health professionals: We know interactions—between people and networks—are necessary. As a result, there will always be the risk of something nasty getting inside. Perfect prevention is not an option.

Consequently, we manage the risk of a dangerous world by asking for reasonable accommodations. This compromise results in social distancing for people or, its online equivalent, network segmentation.

While social distancing helps, it does not guarantee perfect protection. Similarly, we must address cybersecurity on the assumption that someone will infiltrate the network. Of course, completely disconnecting from the outside world is not the answer in either case. Networks across all industries—from banking and finance to military, healthcare, and industrial operations—need to connect to perform their functions, deliver value, and provide efficiencies. Creating controls in the network increases the barriers between systems and intentionally keeps separate things separate.

#7: Embrace Resilience

The COVID-19 pandemic is ongoing. Prevention measures like hand washing, social distancing and wearing masks (particularly in enclosed public spaces) are essential but are not always foolproof.

Similarly, to counter cyberattacks, the primary strategy to-date has been prevention. Prevention however, in the form of traditional firewalls and antivirus systems, is falling short. Cyberattacks are now so advanced that, should a hacker's attention turn to one's organization, the attack will almost certainly succeed. Consider this one startling fact: Despite rising cybersecurity budgets that now reach billions of dollars annually, cyber losses continue to outpace cyber investments dramatically.

Clearly, we need more than prevention. We need resilience. For people, that means staying healthy, eating a balanced diet, getting sufficient rest, exercising regularly, keeping stress levels low, etc.

For cybersecurity, the best defense is also to be resilient. Resilience is the ability to take a punch and then continue to function, keep the lights on, and stay productive even while fending off or countering a cyberattack. Resilience means showing one's leaders not just how one intends to protect everything, but also explaining how the organization can quickly recover when the inevitable attacks occur.

CONCLUSION

There are important security lessons we can take from the current pandemic to make modern networks stronger and more resilient. This article has highlighted seven characteristics of the COVID-19 pandemic that have direct parallels with cyber attackers and our network security measures. Whatever the world looks like after this pandemic passes, viruses, hackers, and cyber criminals will continue to develop new ways of attacking their targets. Furthermore, the first and strongest line of defense is, and will always be, basic hygiene. 🛡️

THE CYBER DEFENSE REVIEW

◆ RESEARCH ARTICLES ◆

Achieving Systemic Resilience in a Great Systems Conflict Era

*Coalescing against
Cyber, Pandemic, and
Adversary Threats*

Chris Demchak

ABSTRACT

A converging trifecta of national disruptive threats – pandemic, cyber attacks, and a rising authoritarian China – is draining the wealth, political harmony, and international influence of today’s consolidated democracies. The result is a more palpably apparent decline in the likely future of democracy as the preferred regime alternative world-wide. The collective dismay and frustration may, however, offer a rarely open door for better postures for democracies in facing a more, not less, turbulent future. This article makes three arguments about a new and more accurate characterization of the coming world as Great Systems Conflict, a list of minimal must-do actions for systemic resilience, and the collective structures critical for resilient democracies over the long-term. The article ends with a discussion of two examples of structures meant to build cybered resilience for allied national systems—domestically in the National Cyber Security Centre equivalents and across consolidated democracies in a Cyber Operational Resilience Alliance.

Today, consolidated democracies face a convergence of three major systemic threats: a raging viral pandemic, an ever-growing tsunami of malicious cyber-attacks, and the inexorable rise of a large scale, strategically ambitious, authoritarian adversary. The cumulative effects of these three threats at the same time are draining wealth, political consensus, and global influence, with increasingly poor long-term prospects for democracy as a dominant regime alternative worldwide. Consolidated democracies thus far have demonstrated a limited community response. As individual national socio-technical-economic systems (STES), each country—both democratic and authoritarian ones—varies in their internal responses to adverse health, cyber, or adversary threats, but none has demonstrated the ability to be resilient to all three systemic threats. The growing

This is a work of the U.S. Government and is not subject to copyright protection in the United States. Foreign copyrights may apply.



With degrees in engineering, economics, and comparative complex organization systems/political science, **Dr. Chris C. Demchak** is the US 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 co-founded 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 a resulting, 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 artificial intelligence, virtual worlds/gaming for operationalized organizational learning, and in modeling systemic resilience ('cybered conflict model') against normal or adversary imposed surprises that disrupt or disable largescale national systems.

number, volume, and sophistication of malicious cyber-attacks reduces consolidated democracies' GDP growth by 1-2%, moving some into negative growth for 2020.^[1] Social tolerance, trust, and transparency that distinguish democracies have also palpably declined. While one highlights cyber and state-level adversaries here, the analysis and recommendations also apply to an inability to respond systemically, except negatively, to pandemics. Democracy is at stake in national responses to all three threat streams. As nations bar movements to stall infections, they further decrease the already declining openness of internal and international systems epitomizing democracy and the international liberal economic system.

When the sources of frightening systemic uncertainty converge into a triple threat—a trifecta for short—to overwhelm both the warning time and the resources to respond across most open societies, resilience comes back into policy circles as a popular word. Whether the threats come from increasingly ubiquitous debilitating viruses, from disruptive cyber maliciousness or shoddy programming, or from deliberate campaigns by multiple adversaries, it is well recognized that only a strategy of resilience—properly understood—can structure the necessary narrative and practices of the targeted system's internal responses. The goal is that uncertainty from outside is manageable and insecurity on the inside is minimal. Compounding this challenge, unfortunately, leaders too quickly lose interest in providing for the costs, time, change in behaviors, and updated narratives essential to achieve long-term resilience. The work goes out of fashion as soon as the threat of the moment has passed, whether it is war, a massive breach, or even a pandemic that paradoxically does not kill enough people to be memorable.^[2]

Today's convergent trifecta of nationally disruptive threats may offer a rarely open door for collective change, resilience, and better postures for democracies facing a more, not less, turbulent future. Taking

this unusual opportunity will require a new and more accurate characterization of the coming world as “Global Systems Conflict,” a list of minimal must-do actions for systemic resilience, and the creation of collective structures critical for resilient democracies over the long term. With that goal of capitalizing on this opening to possibly make a different future path for the world’s relatively small community of consolidated democracies, this article makes the following three arguments.

First, emerging as the backdrop to future vitality threats for democracies is “Great Systems Conflict” rather than the more traditional “Great Power Competition.” Its global ubiquity will force collective whole of society resilience to become a primary objective of national security and economic—as well as health and well-being—strategies in the not distant future across like-minded democracies. Second, resilience is an ongoing organization-driven process, not a static achievement, with an empirically identified set of minimum requirements for large-scale, complex socio-technical-economic systems (STES) such as nations. Third, resilience requires strategically coherent structures to manage integration across these requirements in response to pandemics, cyber or its offspring in AI/ML, and national autonomy threats. These structures can be merely dampeners—the speed bumps or near-term barriers—holding off threats for the short term, or they can be the strategic introduction of “slack in time,” furthering the resilience of the overarching system. The article ends with a discussion of two such structures meant to build cybered resilience in Great Systems Conflict for allied national systems—the National Cyber Security Centre and the Cyber Operational Resilience Alliance. These structures can be blended with, or mirrored into, equivalent structures for pandemic resilience as well.

I. “GREAT SYSTEMS CONFLICT” IS THE NEW “GREAT POWER COMPETITION”

Today, the US and its allies are in a “Great Systems Conflict”: a digitized interconnected struggle between national socio-technical-economic systems in terms of their ability to withstand large-scale disruptive threats, whether from relentless adversaries like China, from the massive cyber bad actor community, or the enormous scale of poor programming that undergirds cyberspace globally. Even pandemics pit state systems versus other state systems in terms of their ability to channel incoming infection hosts, block internal transmission, vaccinate appropriately, or accommodate the health and economic disruptions of thousands of extremely sick and infectious people. When the latter health crisis occurs while intelligent adversaries or bad actors are also systemically unchecked, then a threat trifecta of assaults can put nations on their knees in ways that throughout history only military contests in war or sudden global climate eruptions could achieve.^[3]

To better understand our needs going forward, we must update the narrative to reflect the challenges now facing democratic states. Systemic assaults from multiple domains or sectors require systemic readiness and agility not required nor demonstrated in history’s “Great Power” eras. It is time to retire that newly resuscitated term before it leads us away from a clear-eyed understanding of the current and coming world.^[4] In fairness, the current popularity of

the term “Great Power Competition” (GPC) has served its purpose well. Over the past few years, the rising use of the phrase efficiently highlighted a changing world system and alerted those asleep at the wheel or unwilling to let go of the US global dominance *zeitgeist* to acknowledge a new global reality. The hook worked—policymakers are listening.^[5] Now we need to jettison it and adopt more accurate language and interpretation that stimulates, rather than stultifies, strategic thinking.

What this convergence of threats demands of each nation is not the same as was required of geographic sovereign powers one hundred or even forty years ago. As John Mearsheimer pointed out in 1991, the loss of the bipolar world would lead to struggles for hegemony rather than harmony.^[6] In the coming eras, opponents are less likely to leap to the edifying clarity of armed clashes in war than to attempt to achieve the same goal across the defender’s entire internal socio-technical-economic system through digital, economic, and social means. China recognizes this new reality, but advanced democracies are struggling to adjust, whether out of complacency or confusion. Hence, it helps little to keep telling ourselves that we face something we have seen before, and it is particularly disabling when the trifecta of systemic threats is well underway. What one calls something—especially if it has resonance with the past—heavily channels what one pays attention to, interprets, and does. Mislabeling can be strategically misleading and a prelude to defeat.^[7] For example, it was not by accident that the British pre-WWI called their new armored vehicle a tank. It looked like a water tank and so the name served as a good disguise. But it also led them to think of the tank as an infantry support vehicle rather than an assault vehicle, a blindness Germany exploited in World War II.^[8]

Ultimately, to continue to use the “Great Power Competition” label tells us little about how to defend an entire socio-technical-economic system (STES) where adversaries can easily poke thousands of fingers into all of democratic nations’ socio-technical-economic pies.^[9] Today’s struggles do not begin, nor will they continue, in the same dance around the geographies of armed territorial borders that marked the last century’s Great Power competitions and nearly all of the previous ones as well.^[10] This still emergent century is not characterized by a multipolar tumble of shifting alliances in “a multipolar system, a general disregard for rule-based constraints on behavior, and dominantly political-military forms of rivalry.”^[11] While it seems to create a consensus rhetorically, the term itself has too much historical baggage.^[12] Bad analogies lead to bad strategies.^[13]

Such imprecision is not just misaligned with the deeply digitized world around us; it is also strategically dangerous.^[14] The term encourages a rough equivalence in assessments of large state actors as though any nation at the top—irrespective of socio-technical-economic scale and strategic cohesion—could take the global lead at any point. It encourages ignoring the future path channeling effects of Russia’s constant near-term strategy of disrupting and obstructing the US and EU. It strengthens a false view of equivalence between Russia’s goals and China’s longer term, systems-versus-systems strategy to supplant the US. Strategic mischaracterizations

not only lead to missteps in general with each nation. They can also encourage actions that “could end up driving Xi and Putin into each other’s arms,” creating a combination that dramatically increases the strategic scale and complexity of the national security threats.^[15]

A “Great Systems Conflict” (GSC) emerges when large-scale nations engage in adversarial operations to weaken opponents across the multiple, complex, critical sectors within and among nations without the clarity of sides and actions in declared, kinetic wars.^[16] It is the horizontal expansion to all national domains of the cybered conflict spectrum between peace and war. In this GSC, no system is off the table a priori. This free-for-all-who-can taint is especially present if the malicious usage can be skillfully obscured for considerable time in, perhaps, the hijacking of data traffic by Chinese telecommunications companies across the internet exchange points of democratic nations’ cities^[17] or the corruption of critical network management software updates across the Fortune 500 firms as happened with the 2020 SolarWinds Russian campaign.^[18] Nations involved in GSC cannot assume any opportunity to enhance disruption will be neglected, even if the sources seem natural in the form of complex systems surprises such as the failure of Boeing’s 737-Max aircraft^[19] or biological in the form of 2020 pandemic outbreaks. Strategically navigating that multi-domain maze of contestation does indeed include the exquisite targeting of adversaries’ offensive elements to blunt some campaigns. However, above all, it requires withstanding the assaults of millions of hits per hour into and across the integrated digitized systems that keep us viable—our economy, critical infrastructure, and democratic institutions.

It is high time to move to this more accurate term of “Great Systems Conflict.” The more tied to current reality the explanation, the dominant narrative, and its term of art is, the more likely the nation’s community elites and organizations are to recognize their collective security as a need and be open to discussing the benefits and negotiating obligations in systemic resilience. People cannot get behind a strategy that describes a world they do not see. Characterizing this century’s existential competition as a struggle between “Great Powers” seriously departs from the world inhabited by the leaders of our businesses, the civil society community, or the citizenry at large. Defense sounds like a game of kings best left to the political leaders at the top, with no responsibility, obligation, or benefit to anyone else short of war. Systems-versus-systems conflict requires citizen buy-in over the long term to succeed.

The future will be marked by systems-versus-systems manipulation by bad actors and adversaries. Only the transformation of the underlying shoddy cyber substrate, as well as health and economic infrastructures, will truly prepare democracies need to get fully engaged in this mission. As societies become more complex with cyber’s offspring such as AI, especially neural net learning, robotics, and other combinatorial cross-tech advances in bio-sciences, nano, and other advances in the sciences, surprise becomes more common. Attack surfaces massively increase, and adversaries become more emboldened, skilled, and ubiquitous. While disrupting adversary campaigns to signal displeasure or stop harm is

important, “defend forward” operations such as those conducted by U.S. Cyber Command (USCYBERCOM), cannot alone match the scale of inputs of the wider digital environment without wider support from allies and the private sector.^[20] When socio-technical-economic systems are contesting each other within the entire space of their myriad interactions, systemic resilience becomes the priority strategic imperative.^[21]

II. RESILIENCE’S CHALLENGE^[22] FOR SOCIO-TECHNICAL-ECONOMIC SYSTEMS

Resilience is a complex system's capacity to acceptably anticipate, accommodate, and innovate beyond urgent, disruptive, deleterious surprises. A resilient system demonstrates “the capacity for collective action in the face of unexpected extreme events...[involving] processes of sensemaking and creative problem solving...in complex, social systems...[and] actions that range from improvisation to innovation under urgent conditions.”^[23] This definition comes from scholars with years of experience studying resilient systems. Beyond the experts and those practitioners directly engaged in making systems resilient, however, the word has many—one could argue too many—variations in common understandings.

What we know about resilience comes from a handful of literatures focused on biological systems, on crisis management in societies or businesses, and on technological systems crippled by normal accidents or deliberate attacks. The first highlights long-term survival of the whole community or species over individuals; the latter two, on the restoration of the damaged system under review. When abstracted away from the details into a view of parametric stimulus-responses, accommodating adjustments rippling through connections, and finally stabilizing structures, these literatures point to six elements common to all successful resilience stories.

1. **Slack-in-time** through separation to delay the incursions of threat and give warning to decomposable, self-sustaining operational units.
2. **Redundancy-in-knowledge** to give surprised actors or systems the precisely required knowledge.
3. **Discovery-trial-and-error-learning (DTEL)** by each of all decomposable units to foresee and resource for surprise.
4. **Collective sensemaking** before, during, and after across all decomposable units.
5. **Collective proactive action arrangements** and maintenance of capacity to act.
6. **Collective frequent whole-of-system practice** of all responses as group DTEL.^[24]

These six elements are a minimal list of requirements and are listed in logical order according to their clear expression in empirical cases and to the scale and number of the systems—usually organizations, enterprises, government agencies, or communities—involved. Another way to present the list is as a rough approximation of what comes first in human organizational thinking. Faced with huge and usually looming physical threats, humans run to barricade

themselves to separate for some *slack in time* in order to do some *sensemaking* among each other. Once temporarily protected, they may do some preplanning and envisioning to *mentally think through* what they anticipate is coming next and decide *what actions must be performed* by whom, when, and where. They gather *redundant stores* of resources to place them in the locations their *collective vision* of the immediate future indicates as most appropriate for the survival of the entire system.

Recent years have shown this process playing out in fragments across all three threat streams of the trifecta, but rarely are the six requirements fully met by any large complex system throughout history. They are difficult to achieve as the size of the socio-technical-system at risk grows, and as the volume, diversity, harm potential, frequency, and opaqueness of threats balloon as well. The grand challenge of designing a resilient system rests in structuring that volume and simultaneity of complex resilience calculations and actions continuously across the nation's social, technical, and economic domestic ecosystems toward greater achievement of, and integration over, all six requirements. Furthermore, today it is also necessary to accommodate some key variations of the resilience challenge across all three threat streams of the trifecta currently assaulting democracies.

For the vast tsunami of bad actors using cyber, for example, a key and framing distinction is how relatively easy and cheap it still is to use the five offense advantages built into cyberspace by the shoddy coding of the original creators of the Internet. Cybered criminal and adversary actors continue to use massive scale of botnets as attack organizations, and benefit routinely from unparalleled digitized proximity, as well as endless choices in precision of weapons, deception in tools chosen, and opaqueness of one's true origins. All remain readily available in forming attacks or campaigns against distant strangers in foreign socio-technical-economic systems one or many at a time.^[25] Despite everything laid on top of it for security, the underlying, global cybered substrate continues to be built with insecurity in the confidentiality, integrity, availability, nonrepudiation, and transparency of data, not for the resilience of the nations relying on it.^[26]

For pandemics, the list of framing distinctions is even longer. It includes generalized food insecurity leading to the introduction of wildlife viruses into the human food chain, wealth disparities linked globally through international transport of people, insects, plants, and illegal trades in protected or undesirable biological specimens, and wide disparities in national policies, capacity, and attention to biological health of domestic populations. Across history, there have been few pandemics that were predicted before they manifested and actively contained in humans. The events of 2020 and the SARS-COV-2 epidemic suggest in cruel and costly terms how little systemic resilience to this threat stream there is internationally.^[27]

State-level adversaries pose distinctive challenges to achieving resilience in terms of their deliberate use of demographic and economic scale strengths and their intelligent deployment of strategic coherence. While a virus mutates automatically, and the cyber mass of criminal and

malicious actors moves organically away from hard problems in response to adequate systemic resilience, adversary states have strategic interests that do not easily change. They and their proxies are often relentless in diverse multi-domain, multi-sector, and multi-target campaigns. To respond to the adversary's complex systems surprise and the malicious mass of bad actors, defenders will need resilience as the first and primary defense. It is important to note, however, that resilience needs a more pointed response such as the USCYBERCOM's "forward defense" implementation of its "persistent engagement" strategy, to provide legal, coercive options that reinforce defensive deterrence.^[28]

Across all three of these streams then, systemic resilience programs will have to dismantle the five offense advantages of cyber, and effectively orchestrate a coordination of national policies in health, food, and monitoring of viral spread through illegal trade in wildlife at a minimum. Plus, systemic resilience strategies help democracies match the scale and strategic coherence of the major adversaries in order to deny and disrupt adversary campaigns. The first response invariably is intended to generate slack-in-time.

A. Always the First Step: Separators to Build Slack against Threats

Resilience structures are created by a separation architecture, i.e., varieties of openness within the system that allow unfiltered inputs, intended to provide slack-in-time, the first resilience requirement. Empirically, this structuring response is as old as human society when the first clans sought to improve survival through barricades for defense and the division of labor whether in acquisition of food or in capacity for fighting.^[29] Those with one job were separately trained from those with other jobs, and the clan itself. Many modern concepts capture these designs, parsing elements of STES, for example, division of labor in organizations, parent-child objects in software design and self-contained subsystems in engineering, or enterprise product divisions or regional markets in economics. Everywhere separation of elements is used to control inputs that cannot be processed as quickly, efficiently, profitably, safely, and/or securely if left as a completely open input stream.

It feels natural to wall oneself off from threats; reduced internal disruption means reduced uncertainty and the separation offers more time for a response to develop. John Kenneth Galbraith, a seminal author on information systems in organization theory, argued this response was not just instinctive. It was also the only choice if the internal systems could not be made to process overwhelming inputs of information faster than the data came in.^[30] For a similar reason, Thompson argued organizations were always somewhat open to surprises from their environment.^[31] The recommendation to separate clusters for more response time and increased ability to monitor inputs is found in many literatures including engineering resilience research. The well-honed response is to design an overly complex system in a way that limits failures to certain sections or components, allowing for more rapid isolation and diagnosis of a smaller set of candidate components which may then more readily be corrected.^[32] Modern secure cyber architectures also embed separation in forms from micro-segmentation^[33] to con-

tainers in clouds. The goal is to slow the transmission of error from external sources to dampen the internal amplitude of the sequence of failures across linked systems and give the defenders or maintainers more time to respond appropriately.^[34]

Today's pandemic also shows this instinctive reach for slack-in-time through quarantines and travel bans. Pandemic pods are a particular expression of ad hoc and bottom-up separation choices, usually with rules—much like in organizations—that determine who is in or out, what are acceptable levels of out-of-pod activities, and how to communicate threats, errors, or reassurance.^[35]

Slack, however attractive as the first and usually ad hoc response, is only one requirement. All too often, separating from the threat is all that is accomplished in a system, and generally this is short in time, reach, or funding, and usually abandoned or severely reduced when the crisis has passed. Without an integrated systemic response addressing all six resilience requirements, each new major threat event continues to hollow out the nation's future well-being.

B. Second through Sixth Requirements Often Neglected

Slack architectures provide the structures for potential resilience, but this can only buy time. Their mechanisms of separation define the edges of components, organizations, and even borders for states, but cannot provide a missing narrative of cohesion that fosters consensus and the creation of “statecraft”^[36] for action across a nation.^[37] The use of slack cannot compensate for resilience shortcomings that currently are found across all three threat streams. For example, there continues to be a lack of a consistent narrative on the pandemic despite mounting deaths.^[38] Slack responses cannot alone assure the necessary local and collective discovery-trial-and-error-learning (DTEL) processes that would have helped the US in its 2020 pandemic response. Other shortcomings in resilience are common as well. Highly localized or deliberately underfunded redundancy in knowledge restricts urgent, real-time updates to only a few or forms echo chambers in which adversary disinformation can more easily demobilize or falsely mobilize citizens.^[39] DTEL is found only in many small one-off or highly proprietary or classified exercises or simulations, dramatically limiting the learning to small groups.

Collective sensemaking and action arrangements are similarly confined to small, trusted groups or leading industries. The larger the group, the more sensemaking and action preparation become exercises in checking-the-box compliance. Finally, any collective whole-of-system exercises to create whole group DTEL tend to be held by governments or for government agencies with private sector observers, with results classified away from the rest of the society and possible allies. Crucial players in a whole-of-system defense, especially in cyber (e.g., the nation's IT-related private sector), are left out of strategic deliberations, incentives, and commitments. It is worth asking why recent successes in election defense by US agencies have not been immediately pivoted to the defense of the healthcare system wracked by ransomware and IP exploitation intrusions into vaccine research during a pandemic.^[40] The answer is clearly a lack of a resilience mindset and appropriate structures.

III. COHERENT STRUCTURE FOR INTEGRATION ACROSS RESILIENCE REQUIREMENTS

Creating structures for long-term resilience means making and empowering organizations. All systems contain structures that divide the labor or contribution to the whole, assemblages of technical components, and transactional processes among elements of the system. This division of labor is found in organizations separated for a collective and strategic purpose, usually to accomplish something that would otherwise not be so timely, cost-effective, or possible without the overall organizational structure.^[41] An organization is needed to provide strategic coherence in resilience, placing the dampeners throughout the system proactively according to sensemaking needs and action arrangements as adjusted by local and collective DTEL.

A strategically placed and correctly scaled organization to nurture and ensure the proper integration for resilience against threat streams has been repeatedly recommended in the past. Today, however, the revival of interest in resilience and the associated suggestion that the instinctive reach for slack be channeled through an integrating organization is more than a rehash of an old platitude. In the age of Great Systems Conflict, the lack of this integrating mechanism has long-term existential consequences. The turbulence and vigor of GSC will not decline, nor will COVID-19 be the century's final pandemic. A fragmented, ad hoc, siloed, non-resilient response by a democratic STES paves the way for local and global decline in cyber, health, and defensive capacity.

Governing the system containing the assets at risk in GSC helps enormously in defense because the members can agree to reshuffle their internal architecture to direct more efforts in making a higher work factor^[42] for adversaries. Or they can agree to collectively reduce complex systems' surprises by breaking down the whole into parts able to defend more readily and degrade less disruptively.^[43] The more members of the system at risk agree on their sensemaking narrative and accept that their capacities (DTEL and their redundancy in knowledge) can and will be used to forestall, deny, or work through threat assaults, the more systems will be organized, strategically coherent, and able to operate through threat streams. For this to happen, a strategic and managing layer needs to be structured to manage slack placement, redundancy in knowledge development, local and collective DTEL, and the collective agreements in narrative and commitments to action.

Furthermore, any strategic organization dedicated to systemic resilience needs to be scaled to the size of the socio-technical-economic systems under assault and to the character of threat sources. For example, large businesses and nations have internal boundaries that dampen viral or cyber movement and naturally create slack, enhancing their short-term defense against predators who aim to decimate or cripple the community. However, that size may not prevent the harm if the integration of transactions is so rapid that all elements are infected, affected, or disrupted nearly simultaneously.

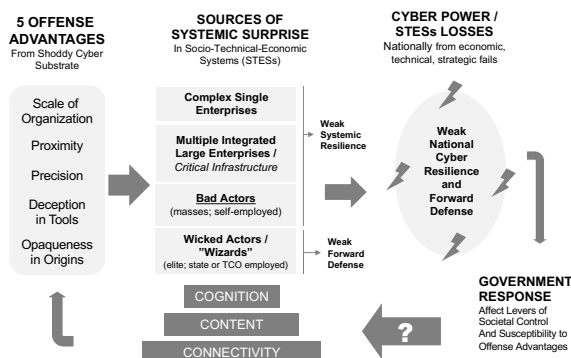
Several nations have already provided organizational experiments in domestic strategic resilience against cyber assaults and adversary campaigns. These exemplars also suggest that, if not already in place or under development, equivalents are necessary for resilience in pandemics.

A. Natural Experiments Suggest Anchor Organizations Critical to Internal Resilience across Complex STESs

Within each national socio-technical-economic system, defense of the entire system—the country—is traditionally left to the government. This makes rough sense in that only the government in a democracy has, in principle, the electorate's mandate to make decisions on their behalf and therefore the legitimacy to enforce those judgements in defeating attacking enemies. However, viruses are not subject to electoral preferences, and, up to now, neither has the cyberspace substrate been subject to many governance intrusions in open democracies. So far, consolidated democratic governments have floundered while trying to integrate responses to cyber assaults. They are highly variable in response to pandemics and too narrow in their reactions to adversary campaigns. The next section will address cyber assaults specifically, with the proviso that the resilience organization discussed here has application for both pandemics and adversaries.

Since its inception, cyberspace has been frequently promoted as a special technology whose generative capacity will be destroyed for the whole society, even the world, if governments attempt to regulate it in any way.^[44] The consequences have been systemically dismaying and costly. Underlying both the cyber and adversary campaign threat streams is a cybered conflict cycle of systemic harm. It began in the 1990s when the US IT capital goods industry created a highly insecure cyberspace substrate that then spread globally—with five embedded offense advantages sent to all bad actors, including states. Democratic government responses have been largely fragmented, derailed by knowledge inadequacies, ownership challenges, and strategic incoherence.^[45] Figure 1 shows this currently endless cycle of malicious use of offense advantages enhancing systemic surprise and poor national systemic resilience with narrowly focused responses by democratic governments unwilling to act to impede their commercial IT producers, thus ensuring the cycle continues.

Figure 1. Cybered Conflict Endless Cycle of Poor Resilience^[46]



The lesson of the past ten years in cyber security and national defense is that leaving the national STES to self-organize a resilience-integrating anchor organization is a fool's errand. Because individual enterprise leaders lack a collective narrative regarding the seriousness of experiences so far, no sufficiently large subgroup has formed to lobby the government for knowledge or action on behalf of the entire system. Governments matter to systemic resilience and must be directly involved in the creation of any organizations designed to break this cycle, integrating the efforts of the whole STES across the six requirements for any threat stream.^[47]

Two experiments in creating an anchor organization for an entire nation in its defense against cybered conflict onslaughts are worthy of mention and future study as they evolve. The first is the United Kingdom's National Cyber Security Centre (NCSC),^[48] and the second is Israel's National Cyber Directorate (INCD).^[49] Each occupies a pivotal position in governance and in access to knowledge. Each already demonstrates some success in influencing the national narrative about cyber security across networks and in the development of cyber's offspring in AI/ML and autonomous technologies. Each also has become the central anchoring point for private sector actors to interact with government points of contact on cyber help, regulations, or threat campaigns. Neither is the perfect solution, but each presents a major step forward in developing strategic coherence for the entire system.^[50]

Other NCSC close equivalents are worthy of further study. Although they are at different levels of collective sensemaking, two examples of government's relationship with the private sector are Netherland's NCSC^[51] and France's ANSSI.^[52] Most of the consolidated democracies, however, struggle with fragmented strategic actors in government and limited private sector involvement in collective cyber sensemaking, action agreements and support, and most forms of DTEL needed for system resilience.^[53] The US shows particular difficulty, thinking in silos of narratives as it has limited private sector involvement save as technology or telecommunications providers. There is no unifying narrative and no single national organization capable of producing a compelling story or the integration required for national resilience. As one of the largest of the beleaguered democracies, the US provides a particularly unfortunate example for the entire community.

At the small end of the demographic scale is Estonia, one of the few democracies to have experienced a potentially devastating cyber-attack by a large-scale adversary and to have innovated through and beyond it. Estonia offers a benchmark for what might be possible in larger democracies. Kohler argues Estonia combines strategic coherence, "just-do-it innovation, commitment, and frugality (it fulfills the NATO target of spending two per cent of GDP on defense), collective defense (it consistently advocates for enhanced cooperation in cybersecurity and a holds strong stance on deterrence), and a persistent norm entrepreneur for the like-minded."^[54] Innovative examples from small states can be quite instructive. If an innovation in structures or policies or socio-technical-economic whole-of-society integration

works in relatively small Estonia, larger states have a reasonable chance that this innovation will work at scale for their STES. If the experiment does not work in the smaller state with its relative advantages in cohesion, there is little chance it will work for larger states. Innovative responses among small states are thus well worth considering for a scaled-up experiment in the more fragmented systems. Both Estonia and Israel serve this purpose as innovation sand-boxes for experiments in better designs of national resilience.

Having an anchor organization integrating all six requirements into a narrative and normalization of shared national practices is critical for domestic systemic resilience. It is also necessary for the like-minded to be able to develop and build on for a larger collective and resilient systemic defense against the relentless assaults of major adversaries, specifically China.

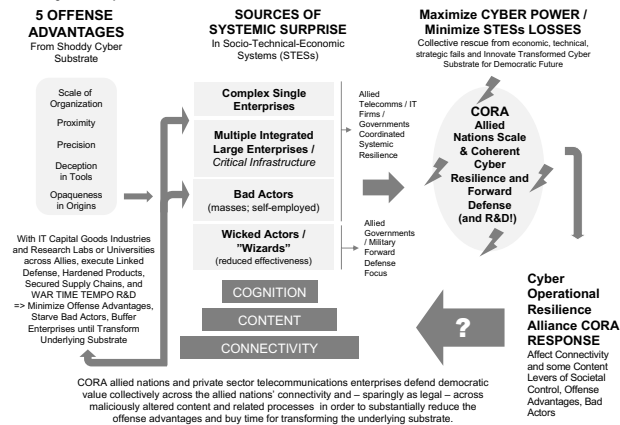
B. Cyber Operational Resilience Alliance (CORA) for Narrative Consensus and Strategic Coherence at Scale

“The point here is not to change the Chinese government or dismember China or something. The point is rather to say, ‘Look, we’ve got a position of power along with people who have similar interests to ours, [and] you can’t dictate to all of us.’”^[55]

If nations can rely on allies for the sharing of difficult requirements such as redundancy of knowledge, the imposition of slack at critical exchange junctures, and the resources for discovery-trial-and-error-learning (DTEL), no single nation faces the adversary alone. The resilience of a nation alone can easily fail facing an ambitious major adversary’s scale and strategic coherence brought to bear from thousands of sources given its global reach. The like-minded defenders need to combine and thus scale up to achieve peer power stature vis-à-vis the adversary. The group needs to manifest strategic coherence in the actions they take to repel and innovate beyond the adversary’s campaigns. If the resilience requirements are absorbed and instantiated across the defenders, the collective scale enlarges the resilience options across all the participant systems.

A structure is needed to ensure allies would collectively be effective. A Cyber Operational Resilience Alliance (CORA) is one way to engage in the collective sensemaking, collective proactive action agreements, mutual support, and group DTEL to continuously improve on all the interrelated practices, knowledge accumulation, and updated narrative. Figure 2 shows how this collective institutionalization can disrupt the cybered conflict cycle of harm and present to the adversary a collectively coherent resilience response. It also shows how each nation needs to develop its own anchor organization and close relations with its IT-relevant private sectors. Its domestic partners agree on a narrative of contribution to systemic defense and then commit to actions in support of that effort nationally and then regionally across industries. Each national anchor organization works to buy time for current defense and to fund the collective transformation of the original inadequate cyberspace into a defensible and democratic digital substrate shared across the CORA nations.^[56]

Figure 2. Cyber Operational Resilience Alliance for the Democratic Like-Minded^[57]



The CORA is not merely an alliance; it is an operational structure built on the anchor organizations and the cooperation across allied government and private sectors. Two examples of how democracies already have relatively successfully achieved this kind of operational collaboration exist in NATO and the EU. Both are *sui generis* and their survival over time despite both budgetary and economic pressures is promising. There are also other reasons to argue that a CORA is doable. A strategically coherent community of more than 900 million citizens will have the economic market weight and the technological talent pool to face an adversary the size and strategic coherence of China as a peer nearly to scale in a conflictual cybered world. Such a unified systemic cyber resilience alliance can orchestrate its own shared adaptive sensor and mitigation systems, massive R&D programs with universities and firms, and the economic and technological talent to transform the collective cyberspace into what it was meant to be when created nearly thirty years ago. The shoddy substrate can be reformulated to be fundamentally secure, fair, open to global trade, democratic in values, and harder to exploit remotely for economic advantage and cybered conflict, including massive disinformation campaigns.

Furthermore, elements of a future CORA already exist across like-minded democracies in various forms. These include routinized and emergency cooperation across operationally functional industry associations, NCSC equivalents in governments, various operational public-private task forces dedicated to solving specific defensive or offensive problems, and a variety of other (mostly too fragmented) practices in the military, critical infrastructure, intelligence, law enforcement, telecommunications, and IT capital goods sectors of these nations. Gathering these mini-experiments along with the private sector actors responsible for them will enable the collective sensemaking and action commitment needed from both government and IT-relevant private sector. As a collectively integrated and coherent global actor, the CORA can provide the framework and urgency to build the necessary civil consensus needed among its component states. Its structure and mission to maintain a unified all-sector response actively engages the private IT capital goods sector in the defense of the democratic economic system

as team players, citizens, while remaining globally vigorous competitors. Only with such an operational alliance can democratic societies afford the necessarily large push to combine talent and investment. This will keep markets healthy with alternative technologies that are able to transform basic Internet technology at the proper scale and defend the economic wellbeing and democratic values of their nations in the future.^[58]

The CORA enables like-minded nations to act in rough unity as a “Great System” in Great Systems Conflict against the authoritarian nations on the rise. Despite being small in number, the community of democratic states acting in unity will be able to present a cybered form of collective statecraft against an adversary’s global capacity. The community will be more cyber-autarkic and resilient, risking neither vassal status nor impoverished isolation. In doing so, the consolidated democratic world will create the robust cyber power needed to negotiate from strength with China for equitable international system rules and acceptable societal well-being in the emerging highly conflictual, systems-versus-systems era. The democratic CORA will also enable a successful democratic model of systemic resilience and prosperity for the rest of world’s populations to consider going forward.

IV. STRATEGIC COHERENCE AT SCALE FOR RESILIENCE IN GREAT SYSTEMS CONFLICT

Imagine a different world for the moment: one in which we recognize that Great Systems Conflict includes the struggle across socio-technical-economic systems to sustain the regime under which one prefers to live. Imagine our situation today if institutions beyond a cyber command were designed to accommodate a national Great Systems Conflict strategy inclusive of major IT capital goods players, telecommunications and other agencies, and relevant cross-sector/domain organizations. Imagine that all are included in an annual grand strategic huddle to allocate resources, and set forth operational responsibilities and cooperative, enforceable standards for performance. The goal is to iterate and agree on next steps, the R&D and operations funding incentives, the regulations, and the narrative about why this is to be done and how it preserves democratic values.^[59] If the world of contesting (and accommodating) multi-sectoral/domain systems were taken as a given, how would it be different now and going forward?

When the democracies show the rest of the world that a democratic CORA can survive under the magnitude of threat sources—even a trifecta—and even innovate beyond the harm, then democracy itself will regain the allure it had fifty years ago, before a shoddy cyberspace, a rising authoritarian behemoth, and a pandemic severely damaged that model. As Ben Franklin famously said, “If we do not hang together, we most assuredly will hang separately.” There is no assured future for democracy in the coming decades unless we act to ensure it now and collectively. In late November 2020, the EU floated a plan offering the US in particular new allied ties on technology (cyber), COVID-19 (pandemic) and “democratic interests.”^[60] The time to move out on collective democratic resilience is clearly now.🛡️

Resilience Foremost, Fires Forward, and Allies Always

All the ideas herein are those of the author and do not reflect the position of any element of the U.S. Government.

NOTES

1. Data from the updated GDP cyber erosion analysis given by Melissa Hathaway in 2019 for GlobSec conference. Melissa Hathaway, "Preparing the Future: Assessing Slovakia's Cyber Readiness" (GLOBSEC 2019 (prepared speech), Bratislava, Slovakia, April 29, 2019). See also Abigail Boatwright and Mark A. Wynne, "Record Global GDP Contraction Indicative of COVID-19's Cross-Country Effect," *Dallas Fed Economics*, October 6, 2020, <https://www.dallasfed.org/research/economics/2020/1006.aspx>.
2. See, for example, the US tendency to learn rarely from previous experiences. R.F. Weigley, *The American Way of War: A History of United States Military Strategy and Policy* (New York: Macmillan, 1973). David Karlin, "What bugs me the most? World+dog just accepts crap software resilience - Flawless applications are for time-rich people with endless cash," *The Register online* (https://www.theregister.co.uk/2019/03/27/software_resilience/), March 27, 2019. Hal Berghel, "Equifax and the latest round of identity theft roulette," *Computer* 50, no. 12 (2017). 72-76, 113-31.
3. Brian Fagan, *The Little Ice Age: How Climate Made History 1300-1850* (London: Hachette UK, 2019).
4. Uri Friedman, "The New Concept Everyone in Washington Is Talking About: How exactly did great-power competition go from being an 'arcane term' a few years ago to 'approaching a cliché'?" *The Atlantic Monthly*, August 6, 2019, <https://www.theatlantic.com/politics/archive/2019/08/what-genesis-great-power-competition/595405/>.
5. U.S. Cyber Command's 2018 Strategic Vision can be found at <https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010>.
6. John J. Mearsheimer, *The Tragedy of Great Power Politics* (New York: W.W. Norton & Company, 2001).
7. Michael J. Mazarr, "This Is Not a Great-Power Competition – Why the Term Doesn't Capture Today's Reality," *Foreign Affairs* (May 29, 2019), <https://www.foreignaffairs.com/articles/2019-05-29/not-great-power-competition>.
8. General Hermann Balck, *Translations of Tape Conversations with General Hermann Balck*, Battelle Tactical Technology Center (Columbus, OH: Batelle Tactical Technology Center, 1979).; W.H. McNeill, *The Pursuit of Power: Technology, Armed Force, and Society Since AD 1000* (Chicago: University of Chicago Press, 1982).
9. R. Smith, "The Utility of Force: The Art of War in the Modern World," in *The Utility of Force* (London: Allen Lane, 2005).
10. Three key pieces include one explaining conflict among states as unitary actors, and one placing the states in a system. Kenneth Neal Waltz, *Man, the State, and War: a theoretical analysis* (New York: Columbia University Press, 2001 (1959)). Robert Gilpin, "The theory of hegemonic war," *The Journal of Interdisciplinary History* 18, no. 4 (1988), 591-613. R. Smith, "The Utility of Force: The Art of War in the Modern World," (London: Allen Lane, 2005).
11. Mazarr, "This Is Not a Great-Power Competition: Why the Term Doesn't Capture Today's Reality."
12. T.C. Jespersen, "Analogies at War: Vietnam, the Bush Administration's War in Iraq, and the Search for a Usable Past," *Pacific Historical Review* 74, no. 3 (2005), 411-26.
13. Emily O Goldman and John Arquilla, *Cyber Analogies*, Naval Postgraduate School Press (Monterrey, CA: Naval Postgraduate Press, 2014). George Perkovich and Ariel E Levite, eds., *Understanding Cyber Conflict: Fourteen Analogies* (Washington, D.C.: Georgetown University Press, 2017).
14. Mazarr, "This Is Not a Great-Power Competition – Why the Term Doesn't Capture Today's Reality."
15. Friedman, "The New Concept Everyone in Washington Is Talking About - How exactly did great-power competition go from being an 'arcane term' a few years ago to 'approaching a cliché'?" <https://www.theatlantic.com/politics/archive/2019/08/what-genesis-great-power-competition/595405/>.
16. P.J. Dombrowski and C.C. Demchak, "Cyber Westphalia: Asserting State Prerogatives in Cyberspace," *Georgetown Journal of International Affairs, special issue on cyber* (2014), 29-38.
17. Chris C. Demchak and Yuval Shavitt, "China's Maxim – Leave No Access Point Unexploited: The Hidden Story of China Telecom's BGP Hijacking," *Military Cyber Affairs Journal* 3, no. 1 (October 21 2018), <https://scholarcommons.usf.edu/mca/vol3/iss1/7/>.
18. Liam Tung, "Microsoft: This is how the sneaky SolarWinds hackers hid their onward attacks for so long – The SolarWinds hackers put in 'painsaking planning' to avoid being detected on the networks of hand-picked targets," *ZDNet online*, January 21 2021, <https://www.zdnet.com/article/microsoft-this-is-how-the-sneaky-solarwinds-hackers-hid-their-onward-attacks-for-so-long/>.
19. Bruno Silveira Cruz and Murillo de Oliveira Dias, "CRASHED BOEING 737-MAX: FATALITIES OR MALPRACTICE?" *GSJ* 8, no. 1 (2020).

NOTES

20. Emily O. Goldman, "The Cyber Paradigm Shift " in *Ten Years In: Implementing New Strategic Approaches to Cyberspace*, ed., Emily Goldman, Jacqueline Schneider, and Michael Warner (Newport, RI: U.S. Naval War College Press, The Newport Papers, 2020).
21. J.L. Casti, *Complexification: Explaining a Paradoxical World Through the Science of Surprise* (New York: Abacus, 1994). Charles Perrow, *Normal Accidents: Living with High-Risk Technologies* (Princeton, NJ: Princeton University Press, 2011).
22. Re-use of old computational science term to mean very hard and as yet unresolved challenges to national security. Personal observation by Dr. Peter Denning, NPS, October 30, 2020.
23. Louise Comfort, Arjen Boin, and Chris Demchak, eds., *Designing Resilience: Preparing for Extreme Events* (Pittsburgh: University of Pittsburgh Press, 2010).
24. Chris C. Demchak, *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security* (Athens, GA: University of Georgia Press, 2011).
25. Chris C. Demchak, "Uncivil and Post – Western Cyber Westphalia: Changing Interstate Power Relations of the Cybered Age," *The Cyber Defense Review* 1, no. 1 (Spring 2016).
26. Andrei Tchernykh et al., "Towards Understanding Uncertainty in Cloud Computing with risks of Confidentiality, Integrity, and Availability," *Journal of Computational Science* 36 (2019), <https://doi.org/10.1016/j.jocs.2016.11.011>.
27. Stephen S. Morse et al., "Prediction and prevention of the next pandemic zoonosis," *The Lancet* 380, no. 9857 (December 1, 2012), 1956-65.
28. As reflected the 2018 U.S. Cyber Command's Vision Statement, the need for targeted offense is often debated, <https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010>. For a discussion of the defense-offense debate in cyber, see also Keir Lieber, "The offense-defense balance and cyber warfare," in *Cyber Analogies*, ed. Emily O. Goldman and John Arquilla (Monterey, CA: Naval Postgraduate School Press, 2014).
29. R.L. O'Connell, *Of Arms and Men: A History of War, Weapons, and Aggression* (London: Oxford University Press, 1989).
30. J.R. Galbraith, *Organization design* (Reading, MA: Addison-Wesley Publishing Co., 1977).
31. James D. Thompson, *Organizations in Action: Social Science Bases of Administrative Theory* (London: Transaction Publishers, 2003 (1967)).
32. Erik Hollnagel, David D Woods, and Nancy Leveson, *Resilience engineering: Concepts and precepts* (Farnham, UK: Ashgate Publishing, Ltd., 2006).
33. Mahmood Yousefi-Azar, Mohamed-Ali Kaafar, and Andy Walker, "Unsupervised Learning for security of Enterprise networks by micro-segmentation," *arXiv preprint arXiv:2003.11231* (2020).
34. L. Sproull and S. Kiesler, *Connections* (Cambridge, MA: MIT Press, 1991).
35. Allyson Chiu, "A pandemic pod could help you get through winter, experts say. Here's how to form one," *The Washington Post*, October 14, 2020, https://www.washingtonpost.com/lifestyle/wellness/pandemic-pod-winter-covid/2020/10/14/214ed65c-0d63-11eb-b1e8-16b59b92b36d_story.html.
36. M. Mastanduno, "Economics and security in statecraft and scholarship," *International Organization* 52, no. 04 (1998), 825-54.
37. Phillip Alvelda, Thomas Ferguson, and John C. Mallery, *To Save the Economy, Save People First: Targeted Measures and Subsidies for Cost Effective COVID-19 Abatement*, Institute for New Economic Thinking (New York, November 18, 2020), <https://www.ineteconomics.org/perspectives/blog/to-save-the-economy-save-people-first>.
38. Editor, "The Quickly Spreading Global Cyber Threat - Interview with Melissa Hathaway," *The Cypher Brief*, February 6, 2019, https://www.thecypherbrief.com/column_article/the-quickly-spreading-global-cyber-threat.
39. Gwen Bouvier, "From 'echo chambers' to 'chaos chambers': Discursive coherence and contradiction in the# MeToo Twitter feed," *Critical Discourse Studies* (2020), 1-17.
40. Comment based on a question asked in frustration during personal conversation with Melissa Hathaway, November 2020.
41. E. Durkheim, *The Division of Labor in Society* (Glencoe, IL: Free Press, 1964). Ramesh Chandra, "Adam Smith, Allyn Young, and the division of labor," *Journal of Economic Issues* 38, no. 3 (2004), 787-805. Jonathan Hearn, "How to Read The Wealth of Nations (or Why the Division of Labor Is More Important Than Competition in Adam Smith)," *Sociological Theory* 36, no. 2 (2018), 162-84.

NOTES

42. John C. Mallery, "A Strategy for Cyber Defense (earlier title: Multi-spectrum Evaluation Frameworks and Metrics for Cyber Security and Information Assurance)" (MIT/Harvard Cyber Policy Seminar, Cambridge, MA, Massachusetts Institute of Technology Computer Science & Artificial Intelligence Laboratory Fall (Spring) 2011 (2009)).
43. For a cyber example of this reshuffling, see Eviatar Matania and Eldad Tal-Shir, "Continuous Terrain Remodelling: gaining the upper hand in cyber defence," *Journal of Cyber Policy* 5, no. 2 (June 11, 2020), <https://www.tandfonline.com/doi/abs/10.1080/23738871.2020.1778761>, 285-301. The concept of graceful decomposition emerges with the early ecosystem literature of the 1960s but was truly adopted by the reliability researchers in engineering or computer systems architecture. See, for example, Charles Shelton and Philip Koopman, "Using Architectural Properties to Model and Measure graceful Degradation," in *Architecting Dependable Systems* (Berlin: Springer, 2003), 267-289.
44. John P. Barlow, "A Declaration of the Independence of Cyberspace," *Electronic Freedom Frontier online* (1996). See also as exemplar Rheingold's work, H. Rheingold, *Virtual Communities: Homesteading on the Electronic Frontier* (Reading, UK: Addison Wesley, 1993).
45. Chris C. Demchak, "Cybered Conflict, Hybrid War, and Informatization Wars," in *Handbook of International Cybersecurity*, ed. Eneken Tikk and Mika Kerttunen (New York: Routledge, 2020).
46. Chris C. Demchak, "Cyber Competition to Cybered Conflict," ed. Emily Goldman, Jacqueline Schneider, and Michael Warner, *Ten Years In: Implementing New Strategic Approaches to Cyberspace* (Newport, RI: U.S. Naval War College Press, The Newport Papers, 2020), <https://digital-commons.usnwc.edu/usnwc-newport-papers/45/>, 47-66.
47. Jennifer W Spencer, Thomas P Murtha, and Stefanie Ann Lenway, "How governments matter to new industry creation," *Academy of Management Review* 30, no. 2 (2005), 321-37.
48. See <https://www.ncsc.gov.uk/>, Note the struggle to decide on the form and location of the NCSC was not a foregone conclusion. See, for example, the interesting analysis of how things stood before the NCSC was created, Francesca Spidaleri, Melissa Hathaway, Chris Demchak, James Kerben, and Jennifer McArdle, *United Kingdom Cyber Readiness at a Glance* (Washington, D.C.: Potomac Institute for Policy Studies Press, October 2016), https://www.potomac institute.org/images/CRI/CRI_UK_Profile_PIPSI.pdf.
49. See https://www.gov.il/en/departments/israel_national_cyber_directorate. Jasper Frei, *Israel's National Cybersecurity and Cyberdefense Posture*, Center for Security Studies, ETH Zurich (September 7 2020), <https://css.ethz.ch/en/services/digital-library/publications/publication.html/e7ad9067-e6f9-422d-a633-5665b9327ba3>. For an extended discussion of the rationale and process behind the INCD, Dmitry Adamsky, "The Israeli Odyssey toward Its National Cyber Security Strategy," *The Washington Quarterly* 40, no. 2 (2017), 113-27. See also Lior Tabansky, *Cybersecurity in Israel*, vol. 598 (Berlin: Springer, 2015).
50. For a discussion of how the INCD in particular works with the military, see the following: Lior Tabansky, "Israel Defense Forces and National Cyber Defense," *Connections* 19, no. 1 (2020), <https://www.pfp-consortium.org/connections-journals/national-cyber-defence-policies-winter-2020>, 45-62.
51. For information on the National Cyber Security Centre (NCSC) of the Netherlands, see <https://english.ncsc.nl/about-the-ncsc>. For a mid-2010s view of the cyber readiness posture of the Netherlands, see Francesca Spidaleri, Melissa Hathaway, Chris Demchak, James Kerben, and Jennifer McArdle, *Netherlands Cyber Readiness at a Glance* (Washington, D.C.: Potomac Institute for Policy Studies Press, May 2017), <https://www.potomac institute.org/images/CRI/FinalCRI20NetherlandsWeb.pdf>. See also R.W. Miedema, "Public-private partnerships for cyber security in the Netherlands" (Executive Master Cyber Security The Hague University of Applied Sciences, 2019).
52. Francesca Spidaleri, Melissa Hathaway, Chris Demchak, James Kerben, and Jennifer McArdle, *France Cyber Readiness at a Glance* (Washington, D.C.: Potomac Institute for Policy Studies Press, September 2016), https://www.potomac institute.org/images/CRI/CRI_France_Profile_PIPS.pdf.
53. Notably among these fragmented nations are the US and Japan. Despite increasing concerns about cyber and the adversary, even in the US case going so far as to ban IT state champions from China, a wide variety of actors still operates independently and discordantly in service of the cyber security of the nation. See Francesca Spidaleri, Melissa Hathaway, Chris Demchak, James Kerben, and Jennifer McArdle, *United States Cyber Readiness at a Glance* (Washington, D.C.: Potomac Institute for Policy Studies Press, 2016), https://www.potomac institute.org/images/CRI/CRI_US_Profile_Web.pdf. See also Francesca Spidaleri, Melissa Hathaway, Chris Demchak, James Kerben, and Jennifer McArdle, *Japan Cyber Readiness at a Glance*, (Washington, D.C.: Potomac Institute for Policy Studies Press, 2016), https://www.potomac institute.org/images/CRI/CRI_Japan_Profile_PIPS.pdf.

NOTES

54. Kevin Kohler, *Estonia's National Cybersecurity and Cyberdefense Posture*, Center for Security Studies (CSS) at ETH Zurich (September 7, 2020), <https://css.ethz.ch/en/services/digital-library/publications/publication.html/2d-d8caf3-6741-435b-8b4d-a4df92e67bcb>.
55. Friedman, "The New Concept Everyone in Washington Is Talking About: How exactly did *great-power competition* go from being an "arcane term" a few years ago to "approaching a cliché"?" <https://www.theatlantic.com/politics/archive/2019/08/what-genesis-great-power-competition/595405/>.
56. Demchak, "Cyber Competition to Cybered Conflict."
57. Ibid.
58. This material is taken from the author's 2017 public testimony before the U.S.-China Economic and Security Review Commission Hearing on China's Information Controls, Global Media Influence, and Cyber Warfare Strategy, May 4, 2017, <https://www.uscc.gov/hearings/chinas-information-controls-global-media-influence-and-cyber-warfare-strategy>.
59. The key values of transparency, tolerance, and trust now include privacy – all four need to be ensured in the transformed and secure new cyberspace substrate to be created by the CORA. For a discussion about why to defend transparency in particular, see the following: Jan Kallberg et al., "Defending the Democratic Open Society in the Cyber Age—Open Data as Democratic Enabler and Attack Vector," *The Cyber Defense Review* 2, no. 3 (2017), 129-138.
60. Sam Fleming, Jim Brunsten, and Michael Peel, "EU pitches new post-Trump alliance with US in face of China challenge: Brussels draft plan seeks to rebuild ties with common fronts on tech, Covid-19 and democratic interests," *Financial Times*, November 29, 2020, <https://www.ft.com/content/e8e5cf90-7448-459e-8b9f-6f34f03ab77a>.

Unleash the Dragon: China's Strategic Narrative during the COVID-19 Pandemic

Mark Bryan Manantan^[1]

ABSTRACT

This article argues that the disruption of the coronavirus was a critical opportunity among states to draw compelling narratives and consequently negotiate their power status and level of influence based on their management of the outbreak. This argument will be explored through the Chinese Communist Party (CCP) at the height of the pandemic. The article investigates the evolution of the CCP's information warfare as an asymmetric capability from its early days of technological inferiority towards its ascendancy to great power status. It highlights the breakthrough of Chinese app TikTok in the US-dominated social media landscape and its potential impact in expanding China's strategic narrative. Using the proposed analytical tools—assets, tactics, and narratives—this article examines the whole of CCP approach aimed to shape the narrative in China's favor following the global outcry from its lack of transparency during the early stages of the pandemic set against the backdrop of its deepening strategic rivalry with the US. It concludes that the CCP will continue to capitalize on information warfare to promote the superiority of the Chinese model amid the eruption of unexpected global crises while depicting the decline of the Western-centric order.

INTRODUCTION

In the aftermath of the US Presidential Elections in 2016, an abrupt change in the cybersecurity policy community transpired. From the heavily focused debate about integrating 'deterrence' in cyberspace, the aperture shifted into combatting the increasing threats from the online environment caused by information warfare.^[2] Overnight, social media companies like Facebook, Twitter, and Google found themselves under greater



Mark Bryan Manantan is currently the Lloyd and Lilian Vasey fellow at the Pacific Forum and concurrently, a non-resident fellow at the Center for Southeast Asian Studies at the National Chengchi University in Taiwan. Recently he was based at the Center for Rule-Making Strategies at Tama University in Tokyo, Japan, and the East-West Center in Washington DC as a 2020 US-Japan-Southeast Asia Partnership in a Dynamic Asia Fellow.

scrutiny for being weaponized by Russian sponsored hackers and troll operators to tamper US elections.^[3] Four years after the Russian interference in American election, open and liberal societies are still grappling with the effects of information warfare only to be confronted with an unexpected global health crisis that will test the online information environment into a whole new level. Despite existing efforts like fact-checking or policing against coordinated and inauthentic behaviors in social media platforms,^[4] the uncertainty brought by the COVID-19 pandemic served as the perfect catalyst which afforded authoritarian states like Russia and China to achieve a forward advantage in the online environment by launching information warfare to cause psychological distress. The disruptive effects of the current pandemic facilitated the acceleration of information warfare to win the battle for strategic narrative and ultimately expand influence while continuing to undermine trust among open and liberal societies across the globe.

This article examines the salience of information warfare as the weapon of choice during the unprecedented global pandemic among authoritarian countries. It argues that information warfare was instrumental to propel a strategic agenda, influence the prevailing debates, and even aggravate existing divisions to promote a state's own interests in international politics and undermining adversaries as majority of the international community strive to cope with the devastating impacts of COVID-19. This argument is explored through the Chinese Communist Party (CCP) and its sophisticated efforts to amplify its strategic narrative following the global fallout from its mismanagement of the coronavirus at the early onset of the pandemic, and, more broadly, to advance its interests on its on-going great power contest with the US. The CCP is no stranger in conducting covert operations to promote its strategic narrative as seen in Hong Kong and Taiwan, however, the COVID-19 pandemic has immensely threatened the

Party's international standing and credibility, thereby, this accelerated information warfare as the crux of its strategic response. An international survey revealed a rising anti-China sentiment since the Tiananmen massacre in 1989.^[5] To arrest this, China employed a whole-of-CCP approach to distract the international community from focusing on China's lack of transparency and accountability and to exploit the inherent political and socio-economic divisions in international politics to assert its increasing influence amid a declining US hegemony.

Russia is the most prominent state actor using information warfare to achieve its political and strategic goals as shown during its extensive interference in the US Presidential elections, and the BREXIT referendum in 2016.^[6] Trailing behind Russia is China which is increasingly becoming a central actor in the information warfare space, primarily asserting its influence as a rising power in the emerging post-liberal order. On the surface, it is convenient to assume that China could just be borrowing pages from Russia's information warfare playbook.^[7] However, this paper contends that CCP's information warfare is more sophisticated than Russia influenced by its new-found great power status which demonstrates its dual identity in international politics as a disruptor and as a collaborator. Compared to Russia, which is beset with debilitating challenges primarily from its stagnant economy and regime instability, China's re-emergence is backed by its increasing political and economic power. China's increasing competitiveness in the emerging technological landscape makes it a formidable peer competitor of the US. This makes China a well-resourced state actor capable of launching information warfare that is even more sophisticated, potent, and pervasive than Russia's. China no longer relies solely on the established tech titans—Facebook, Twitter, YouTube, and Google—to conduct its information warfare. Instead it has successfully penetrated the US-dominated global social media landscape with its own rising digital native platforms like TikTok. As a true marker of its ambition to shape the contours of the Fourth Industrial Revolution, China has nurtured and developed its own tech platforms to capture a global audience. This provides the CCP with a myriad of possible options for experimentation on different information campaigns using various assets. On one hand, the CCP could utilize US social media apps to sow its strategic narrative and counter its critics, on the other hand, it can now employ TikTok and other rising Chinese apps for its information warfare operations and conduct censorship on content which does not align to the CCP's agenda.

This article develops a comprehensive analysis on China's unrelenting quest to advance its strategic narrative through information warfare by exploiting US and Chinese social media platforms. It also examines China's evolving information warfare tactics through its two-pronged approach of seeding and amplifying its strategic narrative while simultaneously conducting censorship in the context of the coronavirus pandemic. Data-gathering for this paper relied on desktop research and open-source information, particularly from policy papers and online articles that were published by various think-tanks and international media outlets which covered China's information warfare during the pandemic. To better explicate China's approach to its strategic narrative, the paper proposes three analytical tools namely: (1) assets, (2) tactics, and (3) narrative.

This entire article unfolds as follows: after this introductory section, the paper proceeds with a conceptual discussion on strategic narrative in the context of the brewing contestation in international affairs between the US and China, particularly the systemic challenges presented by the emerging post-liberal order to the current status quo supported by the US-led international rules-based order. It then dives deeper into the role of information warfare as the critical vehicle which allow states to drive discourse surrounding their respective strategic narrative in the online environment. The article moves to explain the CCP's unique approach on information warfare and the evolution of such capability in the context of its ascendancy to great power status to propel a narrative that serves its global interests. The next to last section explains the defining hallmarks of the CCP's strategic narrative playbook using empirical data by drawing from the proposed triad of analytical tools—assets, tactics, and narratives— as seen throughout the course of the pandemic. The final section offers the conclusion.

Understanding Strategic Narrative

Strategic narratives are tools that are used by political actors to construct (reconstruct) their political realities, extend influence, manage expectations, change discursive environments in which they operate and advance their cause to domestic and international audiences.^[8] Examining the “strategy and intent of the communicating actor” and the aspects of “convergence or divergence” will illuminate how and where audience draw their understanding of international politics.^[9] It is necessary to focus on the interlinked process of strategic narratives at all stages—formation, projection, and reception^[10]—and its various constitutive elements of character/actors; setting/environment; conflict/action; to resolution/solution.^[11] These elements form the raw materials that state actors use to craft a narrative to drive discourse.^[12]

In international relations, strategic narrative emerges as an intellectual project which aims to examine the relationship of communication, persuasion and influence in global politics.^[13] Rather than subscribing to ‘soft power’ in explaining how states influence or persuade others, shifting the focus on strategic narratives and its “interactive, dialogic, and relational properties” provides more explanatory power to assess the political dynamics within and between states.^[14] States use narratives *strategically* not only to persuade their target audience but also to contest and even contradict others. Compelling narratives can be sources of power as they illustrate “the formation, projection and diffusion of ideas in the international system.”^[15] Such formation and projection of strategic narratives along with its reception and interpretation evoke a sense-making, order-making and path-making process where engagement, persuasion, and contestation of ideas and information are located, experienced, and examined.^[16]

By analyzing narratives, scholars and policymakers could arrive at a more compelling explanation on power and influence as it demonstrates how “political actors strategically shape and are shaped by narratives.” Strategic narratives could better explain how soft power tools and capabilities such as culture, values, and policies wield influence as they are linked by a causal logic in a communicative fashion.^[17] There are three categories or levels of strategic

narratives—international or systemic, identity or national, and policy or issue-based. At the international level the focus is on the systemic properties, structural dynamics and the major players involved. While at the second level of identity or national narratives, the values, goals, principles, and standards of political actors take centerstage. Lastly, issue or policy-based narratives underline the objectives and the motivation of policies promoted by state actors and how they are implemented.^[18]

As an analytical tool, strategic narrative can illuminate the recent structural shifts in the international system caused by the on-going great power contest. Narratives serve as a window to explicate the relational aspects of the ensuing US-China trade-turned-tech war by shedding light on issues related to the perception and recognition on the rise of China and the decline of the US hegemony. The current reordering in the international system emanating from the US-China competition highlights a rivalry of strategic narratives. The former being the vanguard of the international rules-based order and the latter expressing its dissatisfaction with the status quo which it seeks to challenge or innovate to suit its interests.^[19]

Several scholars have noted that the hegemony of the liberal order which was developed under the US leadership in the post-Second World War that inspired the fundamental basis for international law, free trade, human rights within the multilateral system is already over. The fading traction of liberal norms and values has given rise to some forms of illiberalism.^[20] In ascertaining this transition into the ‘new world order’, three key dimensions comes to mind—power, values, and institutional dynamics.^[21] Power is shifting horizontally and vertically, where transnational dynamics challenge conventional notions of sovereignty, and states are no-longer the central entity in international politics given the rise of non-state actors. The universality of liberal values underpinned by democracy and human rights has diminished as calls for their relativity and even abandonment becomes increasingly palpable.^[22] While the rules-based multilateral system, comprised mainly of the US-led Bretton Wood institutions is also under extreme pressure to reform itself as western-dominated institutions to reflect the rise of other emerging powers.

Applied in the context of this paper, China’s strategic narrative which it aims to propagate in the midst of the pandemic lies within its deep contestation on the preponderance of the US-led order. The COVID-19 pandemic highlights the systemic changes which are underway in the international system. It has become a critical flashpoint for both superpowers to draw compelling narratives and consequently negotiate their power status and level of influence based on their management of the outbreak. China has been capitalizing on the pandemic to prove the strength and endurance of the Chinese authoritarian model vis-à-vis the US international rules-based order. Its narrative has centered on its ability to quickly recover, resume its economy, and return to normalcy to depict a level of legitimacy as the rising superpower. By appearing unscathed from the pandemic, China attempts to cement its claims of legitimacy of great power status.^[23] It positions itself in stark contrast to the underperformance of the US to control the outbreak—a symptom of its declining status. China’s claims of superiority over the

US is further exacerbated by President Trump's threats of withdrawal from the World Health Assembly. The absence of US leadership provides a vacuum which China has been willing to fill in. At the World Health Assembly last May, China pledged \$2 billion for coronavirus response—an amount which is twice more than what the US has provided the global health agency.^[24] But how does China's strategic narratives get diffused to instigate discourse and reach its target audience? The discussion in the proceeding section establishes the linkage between strategic narrative and information warfare in the current era of hyperconnectivity where the latter acts as the critical driving force to stimulate discourse on the former at the regional and international level.

Information Warfare: Pushing the Strategic Narrative Discourse

The rise of social media and the internet more broadly have become important avenues for states to propel their strategic narrative in today's highly connected digital society. The new multimedia environment has become an integral platform for states to construct strategic narratives that favor their foreign policy goals and to counter those that are opposed to their interests.^[25] The upward trend in the adoption of Information and Communications Technology (ICT) has shifted the process on how states produce their own strategic narratives. More so, the instantaneous nature of Internet accelerated the dissemination as well as the contradiction of narratives between rival states, setting the stage for the emergence of threats related to information warfare.^[26]

Information warfare and its related term influence operations is defined as the “deliberate use of information by one party on an adversary to confuse, mislead, and ultimately to influence the choices and decisions that the adversary makes”.^[27] It is a series of strategic narratives espoused by states which are spread online geared towards winning local and global opinion.^[28] And in the evolving threat landscape, elements of information warfare have become increasingly integrated in launching cyber operations.^[29] Throughout this paper, the term information warfare will be used more loosely to refer to the methodology or the approach used by the state to drive its strategic narrative and expand its influence.

The information environment is considered the battleground for information warfare. Competition in this environment occurs within the physical, informational, and cognitive/emotional domain in three distinct forms: propaganda operations, leak operations, and chaos-producing operations.^[30] These three categorizations are not mutually exclusive and could reinforce each other to achieve the overall objectives of the strategic narrative. Social media plays a central role through social networking, propaganda as well as (fake) news and (dis)information sharing.^[31] Information warfare is executed by building on existing narratives which are amplified through the network of bots to force the algorithm of the social media platform to make the elements that comprised the larger strategic narrative a trending topic.^[32] Coercion and persuasion are often used as the decisive factors or key indicators to measure the impact and reach of information warfare.^[33]

Initially, information warfare was conceived as a technology-oriented tactic deployed to gain information dominance, however, overtime, information transformed to become both the weapon as well as the target—making influence a critical aspect in the conduct of conflict.^[34] In this setting, manipulation of information and its intended result of deception have become the centerpiece of the information warfare equation.^[35] It is worth noting that human psyche plays a fundamental role to achieve the desired effects of information warfare. The interdependence that humans have built around the Internet can be leveraged to exploit their cognitive and affective biases, making them susceptible to misinformation and deception.^[36] This makes information warfare a distinct type of warfare as it requires the exploitation of ICT systems and the vulnerabilities associated to political, economic and social discord particularly in free and democratic societies. Without the permissibility of political or socio-economic crisis, the deliberate use of information warfare lends itself ineffective to achieve psychological manipulation against adversaries.

China's Evolving Information Warfare

This section briefly surveys the transformation of China's approach to its information warfare from its early conception up until its newfound status as a rising power.

China has initially developed information warfare as an asymmetric weapon used by the People's Liberation Army (PLA) for longer-range power projection in response to its technological inferiority with the US in the aftermath of the Cold War.^[37] Information warfare has been regarded as the neuro-system of the PLA which encompasses Command and Control, Communications, Computing, Intelligence, Surveillance, and Reconnaissance (C4ISR) even up to electronic and network warfare.^[38] Strategic thinkers in the PLA have regarded information warfare as a fundamental aspect of the Revolution in Military Affairs. Rather than attempting to match the US strength in conventional military forces, the use of information warfare affords the PLA with a milieu of tactics which are deceptive, surprising, and decisive by design.^[39] Its fundamental goal is information dominance—the ability to defend one's own network, while exploiting the vulnerabilities of the adversary.^[40]

A clear distinction must be drawn when using information warfare in the context of US and China. While majority of US military experts view it as a way of fighting, Chinese experts on the other hand consider it as the fight itself.^[41] General Wang Pufeng stated that “information war refers to a kind of war and a kind of war pattern, while information warfare refers to a kind of operation and operational pattern.”^[42] This primary distinction becomes obvious in the scope of application and limitation of these concepts in the strategic and operational context. Unlike the US military which only applies information warfare during conflict or crisis, the Chinese military considers it as an on-going pursuit.^[43] The impact of such a distinction renders it as an “unconventional weapon and not a battlefield force multiplier,” putting China at a strategic advantage to win information campaign without any need for military action.^[44] This is rooted from the Chinese thinking of omnipresent struggle, a Maoist-Marxist-Leninist paradigm which

depicts China's enduring clash with the West which makes no clear distinction on wartime or peacetime.^[45]

Chinese experts see conflict from violent and non-violent perspectives. The former occurs in the battlefield and is characterized as limited in scale, while the latter known as deterrence war takes up the majority of the space and time.^[46] PLA analysts contend that the enemy is most vulnerable during the early phases of war, and thus, necessitates the effective launch of pre-emptive strikes. The notion of deterrence war which occupies the majority of space and time calls for the implementation of a preemptive strategy prior to the actual breakout of conflict.^[47] The aegis of information warfare in the PLA's strategic doctrine as a pre-emptive strategy and asymmetric capability affirm its limited material capabilities to challenge the US dominance in the military domain in the aftermath of the Gulf War. It was a period that showcased the US technological superiority, standing in stark contrast to China's weak warfighting capabilities at that time. Although, there was momentum within the PLA to further develop its information warfare, China did not possess the adequate resources for research and development and the technological infrastructure to fully experiment and develop such capabilities.^[48]

But nearly three decades later, China is now in the precipice of achieving great power status. It has emerged to become the second-largest economy in the world, inching closer to match the US in the world stage by all measure. Through its China model, the CCP has begun to highlight its unique path to development supported by its track-record of lifting millions of its population out of poverty. Relatedly, China's increasing competitiveness in the area of Artificial Intelligence, 5G, and other emerging technologies has made it a formidable rival against the US technological supremacy. These developments now afford China the capability to reinvigorate its information warfare capabilities.

Under the leadership of Xi Jinping the role of information warfare has become integral as the CCP views the challenges posed by cybersecurity and the flow of information against the regime's continuing existence and survival.^[49] Xi views the internet as an ideological battlefield which strengthened his resolve to devote more resources to conduct "online public opinion work". During a Party conference in 2016 on public opinion work, Xi emphasized the urgency for China to construct an external discourse system that enhances its power status on the world stage.^[50] For instance, the active promotion of China's model was viewed as an attempt by the CCP to challenge the hegemony of universal values.^[51] In the present information age, the PLA has rapidly integrated psychological warfare, cyber warfare, and electronic warfare to influence the opponent's psychological behavior which could permeate all aspects from politics, economics, religion, culture, society to science and technology.^[52] Winning without fighting has been the centerpiece of the PLA's ongoing work on discourse power, which requires the integration of the three types of warfare—public opinion, legal, and psychological—to complement and/or reinforce existing political and diplomatic struggle or in the advent of future wars.^[53]

Strategic Narrative with Chinese Characteristics

China's renewed political, economic, and military strength in the world stage has enabled it to refashion its Information Warfare capabilities and drive its strategic narrative as a rising power centered around the promotion of the post-liberal order on multiple fronts at varying degrees. This section unpacks China's strategic narrative playbook with Chinese characteristics. Throughout the COVID-19 pandemic, China is exploiting the information environment across the physical, information, and cognitive domains. To systematically assess China's overall approach on its information warfare to spark international, domestic and policy discourse, the paper proposes three analytical tools: asset, tactics, and narrative.

Assets include the social media platforms that are used by China to conduct information warfare and promote its strategic narrative. As briefly mentioned, China's ability to exploit well-established American social media apps and the meteoritic rise of its own social media natives like TikTok affords it with more resources to undermine liberal values in open and democratic societies and promote its own agenda.

Tactics underscore the trends, patterns and techniques used to operationalize China's information warfare. Similar to cyber or network operations, the covert nature of information warfare complicates the process of attribution. Despite the active policies adopted by Facebook, Twitter, and Google to ban coordinated and inauthentic behaviors, well-resourced threat actor like China continue to adapt and experiment to minimize detection and achieve a level of legitimacy.

Lastly, *Narratives* probe the salient topics and themes that are injected through the information warfare tactics at the international, domestic, and issue-based level. Focusing on the elements of the strategic narrative underscores China's covert operations to leverage on the vulnerabilities that are present in the physical, informational and cognitive aspects of the on-line information environment.

Assets

China's current information warfare has become a sophisticated asymmetric capability with acquired potency and stealth due to its untethered potential to dominate the Fourth Industrial Revolution. China has developed its homegrown tech champions like Baidu, TenCent, Huawei, and Alibaba which in recent years has continued to gain traction as possible rivals to the US tech giants like Apple, Google, Facebook, Amazon, and Microsoft. However, the tipping point for China's information warfare came in 2019 following the breakthrough of TikTok, a social media app owned by Chinese company ByteDance.

A growing body of research has examined how Chinese-linked hackers and troll farms use Facebook, Twitter, YouTube, WhatsApp and Telegram as part of its information warfare to achieve its pursuit of National Rejuvenation towards Hong Kong, Taiwan, and in the territorial disputes in the South China Sea.^[54] But the game-changer was China's successful penetration

of the US dominated social media landscape through its crown jewel—TikTok, a short video-sharing social media app that has gained global followers, especially in the US.

While majority of Western social media apps are still banned in China, TikTok has expanded beyond Chinese borders and captured a global market of 700 million users as of July, 2020.^[55] As the first major international social media platform with Chinese roots, TikTok is becoming a powerful political actor capable of covertly controlling information flows across geographies and culture.^[56] Due to its growing influence, the Trump administration viewed TikTok as a threat to the US national security due to its linkage with ByteDance.^[57] The US alleges that TikTok can be used by China for espionage purposes given its access to millions of personal user data. President Trump has issued various executive orders demanding the divestment of the app's operation from its parent company and to find a suitable US partner if it aims to continue its operations.^[58]

Amidst the perceived overreaction on the Trump administration's efforts to ban the app, a closer look at TikTok's operations reveals that such moves are warranted. The core algorithm that runs TikTok is mandated under the Chinese law to propagate the CCP's propaganda.^[59] Having such extensive reach provides the CCP with a heavy hand to shape TikTok's global content moderation. ByteDance CEO Zhang Yiming has confirmed that the company's product and business lines are designed to promote CCP's agenda, including manipulating TikTok's core algorithm to reflect the party line and promote socialist core values.^[60]

Tactics

Fundamental to understanding the execution of Chinese-linked information warfare are the tactics or techniques it has deployed to maximize various social media platforms. Over the course of the pandemic Facebook, Twitter, and YouTube were the major social media assets that were instrumental in China's information warfare to push for its favorable strategic narrative among foreign audiences. Meanwhile, TikTok has also started to gain traction. China was able to leverage on Facebook, Twitter, and YouTube for its information warfare to amplify its strategic narrative, while it facilitates censorship on TikTok to silence narratives that do not align with the CCP's broader agenda. China has used all of the identified social media apps to fan social unrest particularly in the US and other parts in the Indo-Pacific region to divert scrutiny away from the CCP's lack of transparency during the early onset of the pandemic.

Much of the information warfare tactics and techniques conducted by Chinese-linked trolls have morphed, and now rely not only on bots but also on personal accounts that exude a veneer of legitimacy. Clearly, inauthentic coordinated networks are still driven by networks of automatic bots, but the rise of pro-China patriotic trolls on social media platforms have also made it challenging to make a direct attribution of various information warfare campaigns.^[61] There is a growing cross-posting strategy from Facebook to Twitter that uses repurposed accounts. While China's campaign operators are purchasing the bulk of user accounts in Facebook and Twitter that were based in Bangladesh, Russia, Indonesia, and France,^[62] but it

was also observed that there is a growing propensity to use Facebook pages rather than individual user accounts which is a new type of asset experimentation. Although Facebook fan pages could result into more traction, it will most likely be mixed with individual accounts to maintain a degree of diversity.^[63]

Aside from Facebook and Twitter, YouTube has also become a critical tool in ramping up China's information warfare. A pro-Chinese political spam network called *Spamouflage dragon* was spreading English-language videos that were critical of the Trump administration's tit-for-tat policies against China.^[64] The network was initially spotted in 2019 focusing on the Hong Kong protests and by early 2020 it has started to post videos which are critical of the US government's inadequate response to the coronavirus pandemic.^[65]

China's information warfare extends beyond the digital realm and, includes all the other available tools—political, economic, and diplomatic—at its disposal to inculcate the major themes and key elements of its strategic narrative.^[66] In light of the global backlash following its mismanagement of the virus, the Chinese Academy of Sciences has crafted a coordinated and coherent messaging strategy among Chinese diplomats and state-owned media which offers a wide range of responses. This include aggressive media monitoring and rapid response; promoting the use of diverse sources; supporting Chinese social media like Weibo, WeChat, and Douyin; targeting specific audiences through enhanced means of communication; and cultivating foreign talents.^[67] Although there is a general consensus that Western social media platforms are central elements of Chinese information warfare, CCP's potential control of TikTok's global content policies equips the Chinese government an unrestricted apparatus to boost and complement its strategic narrative.

Narrative

China's information warfare has evolved throughout the course of the pandemic. Although the strategic narrative has initially focused in containing the global backlash it has received, it has immediately shifted gears by painting itself as a responsible stakeholder through its cooperation with the World Health Organization (WHO). China eagerly established the credibility of its approach in the early stages of the pandemic by highlighting its sacrifices during the initial lockdown as the model for the world to emulate to contain the outbreak.^[68] Chinese diplomatic and state-owned media's online accounts boosted this narrative about China's upbeat performance against COVID-19 and compared it to the lackluster response made by the US and Europe, and even highlighted its ongoing cooperation with regional groupings such as ASEAN, Arab League, and the African Union.^[69] China's top diplomats Lijian Zhao and Hua Chunying also exploited the mounting criticisms levied by the US against the WHO. For instance, while the US President Donald Trump's threatened to defund and even pull out from the WHO, Hua Chunying asserted China's commitment and its level of transparency with the WHO.^[70] The specific tweet from the Chinese Ministry of Foreign Affairs was also amplified by state-run media CGTN and Xinhua. Additionally, Chinese-linked accounts also constructed a narrative

that accused the US behavior as 'selfish, foolish, and destructive', compared to China's good behavior in supporting international cooperation through WHO.^[71]

China has also used the COVID-19 pandemic to reaffirm its One China principle and downplay Taiwan's impressive performance to contain the virus. A coordinated anti-Taiwan trolling emerged following Dr. Tedros Adhamon, the WHO Director-General, accused Taiwan of racial attacks. There were 65 accounts pretending to be Taiwanese netizens who offered apologies to Tedros with the hashtag #saysrytoTedros.^[72] A network analysis of the accounts revealed a cluster of commonly followed accounts which were classified as inauthentic. Taiwan's Investigation Bureau Cybersecurity Head Chang Yu-jen confirmed that Chinese trolls were behind the fake posts aimed to put Taiwan as the culprit behind the coordinated racist abuse against Dr. Tedros.^[73] The Twitter accounts that were fomenting the racism spat with the WHO chief were also discovered to be part of a larger campaign that has begun in early 2020.^[74] Most of these accounts mimicked or trolled Western media outlets to mislead readers and harass real accounts by responding with abusive replies or asserting that the troll account was authentic.^[75]

Throughout the pandemic, China has been relentless in undermining the US' reputation and credibility amidst their ongoing strategic rivalry. There were 62 identified accounts on Facebook and 200-300 Twitter users who posted, shared and retweeted similar narratives which started as early as February 2020.^[76] The inauthentic, cross-platform campaigns were believed to be conducted by Chinese-affiliated actors, which targeted Western and US-based audiences to drive divisive or negative narratives against the US, primarily the Trump administration's COVID-19 response, and the spiraling tension in the US-China relations. A further investigation on Facebook and YouTube revealed on-going inauthentic activities with similar themes that centered around the Trump administration's mishandling of the outbreak, threats to ban TikTok in the US,^[77] increasing tension from the Black Lives Matter protests, and the heightened anticipation of the US presidential elections.^[78] Google's Threat Analysis Group has removed a total of more than 2,000 channels that exhibited coordinated influence operations that were tracked back to China.^[79] According to William Evina, Director of the National Counterintelligence and Security Center, China expanded its influence efforts ahead of the US elections by emphasizing the Trump administration failures in managing the pandemic.^[80] The Chinese narrative mirrored the commentaries of Western-liberal media against President Trump's mismanagement of the coronavirus in the US. However, the information warfare component is based on the coordinated and inauthentic tactics that were used to amplify the content. Key issues central to the narratives accused President Trump's denial about the severity of the virus and manipulation on the real statistics on the spread of the virus that led to hundreds of thousands of deaths.^[81] Indeed, the impact of Trump's disastrous performance in managing the outbreak was also a frequent theme discussed or promoted online.^[82]

Some campaigns were also attempting to ignite conspiracy theories on the origin of the virus. An article that circulated on Twitter purports the Fort Detrick theory, which asserts that the coronavirus originated from the Fort Detrick Lab in Maryland, and resembles the same China-state apparatus conspiracy talking points.^[83] TikTok was under fire for circulating baseless assertions regarding the public health crisis. For instance, some users were claiming that Microsoft CEO Bill Gates and his non-profit organization at the Pirbright Institute based in the UK were connected to the coronavirus outbreak.^[84]

Chinese-linked trolls were also actively stoking racial divisions after the viral news surrounding the death of George Floyd by amplifying the eruption of Black Lives Matter protests in the US. Content showing a black protester resisting a white counter-protester were shared excessively over in Facebook and Twitter to exacerbate racial divide.^[85] In contrast, TikTok was engaged in censoring content that are related to the George Floyd protests that used the hashtag #acab, which stands for “all cops are bastards”.^[86] Following a public outcry on its censorship, TikTok immediately restored the hashtags related to the protests. But a few months later, TikTok continued to ban anti-racism and anti-police brutality protests after a surge on social media activity spiked. Following the police shooting of Jacob Blake, the hashtag #acab was once again censored.^[87]

China's Strategic Narrative in the New Normal

Despite China's rapid emergence to great power status marked by its rapid accumulation of conventional military capabilities across all domains, the role of asymmetric capabilities remains a centerpiece in the CCP's regime survival and triumph. Three decades after China's early conception of information warfare as an asymmetric capability, the PLA continues to see its indispensable value against the technologically capable US. As it rapidly becomes a well-resourced state actor, China has been relentless in refining the force-multiplier effect of such capability to be more sophisticated and highly suited in today's hyperconnected world.

In this article, the analysis of China's information warfare throughout the pandemic unveils its unique approach in promoting its strategic narrative that echoes its global ambition as a new superpower. The fallout from its lack of transparency at the onset of the pandemic served as the impetus for China to employ its information warfare at such unprecedented level, unleashing a whole-of-CCP approach, which was orchestrated by its large networks of automated bots, paid campaign operators, the Chinese diplomatic community, and state-owned media all working in unison. The CCP aimed to shift the ire of blame by promoting instead its narrative of triumph against the coronavirus. It was able to capitalize on such a vulnerable spot to project its China model worth emulating in the ongoing public health crisis by juxtaposing it to the US' lackluster performance.

The whole-of-CCP approach will be fundamental to China's emerging strategic narrative in the new normal designed to achieve two-fold: first, to mitigate the impact of worsening

international perception given the uncertainty in the post-COVID-19 era especially as China prepares for a protracted war with the US in the coming decades. Second, to consistently capitalize on the eruption of unexpected crises in the international landscape to advance and highlight the superiority of its Chinese model. The CCP will continue to advance elements of the post-liberal order to depict the decline of a Western-centric order which is incapable of withstanding the disruptive effects of black swan events in international politics. And fundamental to the future of China's information warfare is the stratified approach to propagating its strategic discourse across international, domestic and policy-oriented narratives. Chinese experts will continue to experiment on their tactics and themes including the integration of cyber or network operations and information warfare with emerging technologies to achieve more sophisticated outcomes.

The current trends assessed in this article surrounding China's information warfare points to its future trajectory as it becomes even more vital and stealthy in nature. The breakthrough of TikTok into the mainstream and global social media arena that is largely dominated by Facebook and Twitter provides the CCP with a new platform to elevate its information warfare to a different level. China's revised export control law which covers the Algorithms and AI embedded on TikTok demonstrates the centrality of the app and other emerging Chinese-tech towards winning the global public opinion and reaching its ambition for national rejuvenation in the years to come. Having such unprecedented control over TikTok, China can now directly export its strategic narrative with lesser constraints across the world. It will aim to normalize censorship against narratives that are inimical to the CCP's authoritarian ideals which sets a dangerous precedent in threatening the core notion of 'free speech' in open and democratic societies. As more countries raise concerns on Facebook, Twitter and YouTube's community guidelines, TikTok could be a viable alternative. TikTok's content moderation policies that are synonymous to censorship might be appealing among developing countries that lean towards censoring content and/or anemic to the universal application of free speech.

The future of the Internet appears to be bleak. As countries like China and the US push their respective strategic narratives, a China- or US-approved Internet might eventually be established in the years ahead. If this transpires, China's vision for a post-liberal society will materialize and contradicts the very same ideals upon which the Internet was founded on—openness, transparency, and collaboration. Thus, the key to combatting the increasing prevalence of information warfare as it becomes part of the new normal lies in these same virtues. Encouraging transparency across all social media platforms whether on their community guidelines and policies, content moderation and algorithms is imperative. Social media and tech companies must regularly disclose any information warfare campaigns prevailing in their networks and systems to raise public awareness and resilience among social media users against potential manipulation or deception. Lastly, combatting information warfare

must be a collaborative venture, enjoining government agencies, tech companies, academia, and civil society organizations to create an information warfare-proof Internet based on accountability frameworks through periodic assessments that could safeguard user-data privacy and protection.🛡️

NOTES

1. Mark Bryan Manantan is the Lloyd and Lilian Vasey Fellow at the Pacific Forum, and concurrently a non-resident fellow at the Center for Southeast Asian Studies, National Chengchi University in Taiwan. You can reach him at brymanmedia@gmail.com.
2. Max Smeets and Stefan Soesanto, "Cyber Deterrence Is Dead. Long Live Cyber Deterrence!" Council on Foreign Relations, last modified February 18, 2020, https://biblioteca.fba.up.pt/form_utilizadores/Purdue_OWL_Chicago.pdf.
3. Alexander Spangher, Gireeja Ranade, Besmira Nushi, Adam Fourney, Eric Horvitz, "Analysis of Strategy and Spread of Russia-sponsored Content in the US in 2017," *Social and Information Networks*, last modified October 23, 2018, <https://arxiv.org/abs/1810.10033>; Scott Shane, "The Fake Americans Russia Created to Influence the Election," *New York Times*, last modified September 7, 2017, http://cs.brown.edu/people/jsavage/VotingProject/2017_09_07_NYT_TheFakeAmericansRussiaCreatedToInfluenceTheElection.pdf; Tom McCarthy, "Facebook, Google and Twitter grilled over Russian meddling—as it happened," *The Guardian*, last modified October 31, 2017, <https://www.theguardian.com/technology/live/2017/oct/31/facebook-google-twitter-congress-russian-election-meddling-live>.
4. Foo Yan Chee, "Google, Facebook, Twitter have to do more fight fake news: EU," *Reuters*, last modified last April 23, 2019, <https://www.reuters.com/article/us-eu-tech-fakenews-idUSKCNIRZ0WU>.
5. Laura Silver, Kat Delvin, and Christine Huang, "Unfavorable Views of China Reach Historic Highs in Many Countries," Pew Research, last modified October 6, 2020. <https://www.pewresearch.org/global/2020/10/06/unfavorable-views-of-china-reach-historic-highs-in-many-countries/>.
6. Robert Mueller III, "Report on the Investigation into Russian interference in the 2016 President Election," *US Department of Justice*, March 2019, <https://www.justice.gov/storage/report.pdf>; "Government response to the Intelligence and Security Committee of Parliament report 'Russia'," *Intelligence and Security Commitment*, July 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/902342/HMG_Russia_Response_web_accessible.pdf.
7. Jessica Brand and Torrey Taussig, "The Kremlin's disinformation playbook goes to Beijing," *Brookings*, last modified May 19, 2020, <https://www.brookings.edu/blog/order-from-chaos/2020/05/19/the-kremlins-disinformation-playbook-goes-to-beijing/>.
8. Alister Miskimmon, Ben O'Loughlin, and Laura Roselle. *Strategic Narratives: Communication Power and the New World Order*. (New York: Routledge, 2017), 2; Alice Ba, "China's 'Belt and Road' in Southeast Asia: Constructing the Strategic Narrative in Singapore," *Asian Perspective* 43 (2019): 253. <https://doi.org/10.1353/apr.2019.0010>.
9. Natalia Chaban, Alister Miskimmon, and Ben O'Loughlin, "The EU's Peace and Security Narrative: Views from EU Strategic Partners in Asia," *Journal of Common Market Studies* 55 (2017): 1274. doi:10.1111/jcms.12569.;
10. Chaban et al., "The EU's Peace and Security Narrative," 1274.
11. Laura Roselle, Alister Miskimmon, and Ben O'Loughlin, "Strategic narrative: A means to understand soft power," *Media, War and Conflict*, 7 (2014): 12, doi:10.1177/1750635213516696.
12. Miskimmon et. al, *Strategic Narratives: Communication Power and the New World Order*, 12.
13. Roselle, et. al, Strategic narrative: A means to understand soft power," 77.
14. Alice Ba, "China's 'Belt and Road' in Southeast Asia: Constructing the Strategic Narrative in Singapore," 252.
15. Roselle, et al., Strategic narrative: A means to understand soft power," 74.
16. Ibid., 75.
17. Ibid., 74.
18. Ibid., 76.
19. Caitlin Byrne, "Securing the 'Rules-Based Order' in the Indo-Pacific," *Institute for Regional Security*, 16 (2020), <https://www.jstor.org/stable/10.2307/26924333>.
20. Fareed Zakaria, "The Rise of Illiberal Democracy" *Foreign Affairs* 76 (1997).
21. Andre Barrinha and Thomas Renard, "Power and diplomacy in the post-liberal cyberspace," 4.
22. Ibid., 6.
23. Andrew Jacobs, Michael Shear, and Edward Wong, "US-China Feud Over Coronavirus Erupts at World Health Assembly," *New York Times*, last modified May 18, 2020, <https://www.nytimes.com/2020/05/18/health/coronavirus-who-china-trump.html>.
24. Ibid.

NOTES

25. Kalathmika Natarajan, "Digital Public Diplomacy and a Strategic Narrative for India," *Strategic Analysis* 38 (2014), <https://www.tandfonline.com/doi/abs/10.1080/09700161.2014.863478>.
26. Martin Libicki, "The Convergence of Information Warfare" *Strategic Studies Quarterly* 11 (2017), <https://www.jstor.org/stable/pdf/26271590.pdf?refreqid=excelsior%3Af342323547ec27f92fcd6c3eb5839946>.
27. Herbert Lin and Jaclyn Kerr, "On Cyber-Enabled Information Warfare and Information Operations", SSRN, (2019), 4, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3015680&download=yes.
28. Yeygeniy Golovchenko, Mareike Hartmann, and Rebecca Adler-Nissen, "State media and civil society in the information warfare over Ukraine: citizen curators of digital disinformation," *International Affairs* 94 (2018), <https://academic.oup.com/ia/article/94/5/975/5092080>.
29. Martin Libicki, "The Convergence of Information Warfare."
30. Herbert Lin and Jaclyn Kerr, "On Cyber-Enabled Information Warfare and Information Operations."
31. Jarred Prier, "Commanding the Trend: Social Media as Information Warfare," *Strategic Studies Quarterly* 11 (2017), https://www.jstor.org/stable/26271634?seq=1#metadata_info_tab_contents.
32. Jarred Prier, "Commanding the Trend: Social Media as Information Warfare."
33. Ibid.
34. William Hutchinson, "Information Warfare and Deception," *Informing Science*, 2006, <http://inform.nu/Articles/Vol9/v9p213-223Hutchinson64.pdf?q=deception>.
35. William Hutchinson, "Information Warfare and Deception."
36. Miguel Alberto Gomez, "Cyber-Enabled Information Warfare and Influence Operations. A revolution in Technique?" *Information Warfare in the Age of Cyber Conflict*, ed., Christopher Whyte et al., (New York: Routledge, 2020), 133.
37. James Mulvenon, "The PLA and Information Warfare," in *The People's Liberation Army in the Information Age*, ed. James C. Mulvenon and Richard Yang, (Santa Monica, CA: RAND Corporation, 1999), 176.
38. Chris Wu, "An Overview of the Research and Development of Information Warfare in China," in *Cyberwar, Netwar and the Revolution in Military Affairs*, ed. Edward Halpin, et.al., (London: Palgrave MacMillan, 2006). https://link.springer.com/chapter/10.1057%2F9780230625839_11.
39. Vincent Wei-Cheng Wang, "Asymmetric War? Implications for China's Information Warfare Strategies," Ithaca College (2002), https://digitalcommons.ithaca.edu/cgi/viewcontent.cgi?article=1015&context=politics_faculty_pubs.
40. James Mulvenon. "The PLA and Information Warfare," 180.
41. Barrington Barrett, Jr., "Information Warfare: China's Response to U.S. Technological Advantages," *International Journal of Intelligence and CounterIntelligence* 18 (2006), 684.
42. Barrington Barrett Jr., "Information Warfare: China's Response to U.S. Technological Advantages," 684.
43. Ibid., 685.
44. James Mulvenon. "The PLA and Information Warfare," in *The People's Liberation Army in the Information Age*, 183.
45. Mark Bryan Manantan, "The People's Republic of China's Cyber coercion: Taiwan, Hong Kong, and the South China Sea," *Issues and Studies* 56 (2020), <https://doi.org/10.1142/S1013251120400135>.
46. Barrington Barrett, Jr., "Information Warfare: China's Response to U.S. Technological Advantages," 685.
47. James Mulvenon. "The PLA and Information Warfare," in *The People's Liberation Army in the Information Age*, 183-184.
48. Chris Wu, "An Overview of the Research and Development of Information Warfare in China."
49. Elsa Kania, "The Ideological battlefield: China's approach to political warfare and propaganda in an age of cyber conflict", in *Information Warfare in the Age of Cyber Conflict*, ed. Christopher Whyte et al., (New York: Routledge, 2020).
50. Elsa Kania, "Ideological Battlefield".
51. Ibid.
52. Ibid.
53. Ibid.
54. Mark Bryan Manantan, "The People's Republic of China's Cyber Coercion: Taiwan, Hong Kong, and the South China Sea."
55. Fergus Ryan, Audrey Fritz, and Daria Impiombato, "TikTok and WeChat," *Australian Strategic Policy Institute*, last modified September 8, 2020, <https://www.aspi.org.au/report/tiktok-wechat>, 3.

NOTES

56. Fergus Ryan, Audrey Fritz, and Daria Impiombato, "TikTok and WeChat," 3-4.
57. Justin Sherman, "Unpacking TikTok, Mobile Apps and National Security" *Lawfare*, last modified April 2, 2020, <https://www.lawfareblog.com/unpacking-tiktok-mobile-apps-and-national-security-risks>.
58. Nikki Carvajal and Caroline Kelly, "Trump issues order banning TikTok and WeChat from operating in 45 days if they are not sold by Chinese parent companies," CNN, last modified August 7, 2020, <https://edition.cnn.com/2020/08/06/politics/trump-executive-order-tiktok/index.html>
59. Fergus Ryan, Audrey Fritz, and Daria Impiombato, "TikTok and WeChat," 18.
60. Ibid., 18-19.
61. Jake Wallis, Tom Uren, Elise Thomas, Albert Zhang, Dr. Samantha Hoffman, Lin Li, Alex Pascoe, and Danielle Cave, "Retweeting through the great firewall," *Australian Strategic Policy Institute*, last modified June 11, 2020. <https://www.aspi.org.au/report/retweeting-through-great-firewall>, 19.
62. Jake Wallis, Tom Uren, Elise Thomas, Albert Zhang, Dr. Samantha Hoffman, Lin Li, Alex Pascoe, and Danielle Cave, "Retweeting through the great firewall," 22-23.
63. Ibid.
64. Ben Nimmo, Camille Francois, C. Shawn Eib and Lea Ronzaud, "Spamouflage Goes to America," *Graphika*, last modified August 2020, https://public-assets.graphika.com/reports/graphika_report_spamouflage_goes_to_america.pdf, 1-2.
65. Ben Nimmo, Camille Francois, C. Shawn Eib and Lea Ronzaud, "Spamouflage Goes to America," 3-11.
66. Mark Bryan Manantan, "The People's Republic of China's Cyber Coercion: Taiwan, Hong Kong, and the South China Sea."
67. Wallis, et al, "Retweeting through the great firewall," 5.
68. "Covid-19 disinformation and social media manipulation trends," 3.
69. Ibid.
70. "Covid-19 disinformation and social media manipulation trends," *Australian Strategic Policy Institute*, last modified April 15, 2020, https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-04/COVID-19%20Disinformation%20%26%20Social%20Media%20Manipulation%20Trends%208-15%20April.pdf?LK2mqz3gNQjFRxA21oroH998enBW__5W=, 2.
71. Elise Thomas, Albert Zhang, and Dr. Jake Wallis, "Viral Videos: Covid-19, China, and inauthentic influence on Facebook," *Australian Strategic Policy Institute*, last modified September 29, 2020, https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-09/Viral%20videos.pdf?oRBhvSURmY5drwKr_EbnIZq6eu_87CKh=, 14.
72. "Covid-19 disinformation and social media manipulation trends," *Australian Strategic Policy Institute*, 2.
73. Samson Ellis, "Taiwan Accuses Chinese Trolls of Fomenting Racism Spat with WHO," *Bloomberg*, last modified April 10, 2020, <https://www.bloomberg.com/news/articles/2020-04-10/taiwan-accuses-chinese-trolls-of-fomenting-racism-spat-with-who>.
74. Elise Thomas and Albert Zhang, "COVID-19 Attacks Patriotic Troll Campaigns in Support of China's Geopolitical Interests," *Australian Strategic Policy Institute*, last modified June 11, 2020, https://s3-ap-southeast-2.amazonaws.com/ad-aspi/202004/Patriotic%20Troll%20Campaigns%20Report_ASPI%20Cyber.pdf?3UM1P9V4gVpAacBYaf7zxRM9HM-la_twV=, 3
75. Elise Thomas and Albert Zhang, "COVID-19 Attacks Patriotic Troll Campaigns in Support of China's Geopolitical Interests," 2.63
76. Elise Thomas, Albert Zhang, and Dr. Jake Wallis, "Automating Influence on COVID-19," *Australian Strategic Policy Institute*, last modified August 24, 2020, https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-08/Automating%20influence%20on%20Covid-19.pdf?DxaB4psM9BvTNrhNQNTpu_jWNWmqPGXg=.
77. Elise Thomas, Albert Zhang, and Dr. Jake Wallis, "Viral Videos: Covid-19, China, and inauthentic influence on Facebook," *Australian Strategic Policy Institute*, last modified September 29, 2020, https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-09/Viral%20videos.pdf?oRBhvSURmY5drwKr_EbnIZq6eu_87CKh= .
78. Thomas, et al., "Automating Influence on COVID-19," 6-10.
79. Thomas, et al., "Viral Videos: Covid-19, China, and inauthentic influence on Facebook".
80. Office of the Director of National Intelligence, "Statement by NCSC Director William Evanina: Election Threat Update for the American Public," *Press Release*, August 7, 2020, <https://www.dni.gov/index.php/newsroom/press-releases/item/2139-statement-by-ncsc-director-william-evanina-election-threat-update-for-the-american-public>

NOTES

81. Thomas, et al., “Viral Videos: Covid-19, China, and inauthentic influence on Facebook,” 12-14.
82. Ibid.
83. Thomas, et al., “Automating Influence on COVID-19,” 6-7.
84. Dawn Chmielewski, “TikTok Used To Spread Misinformation About The Coronavirus,” *Forbes*, last modified January 28, 2020, <https://www.forbes.com/sites/dawnchmielewski/2020/01/28/tiktok-used-to-spread-misinformation-about-the-coronavirus/#5ed32ac916d6>.
85. Thomas, et al., “Automating Influence on COVID-19,” 3; Thomas, et al., “Viral Videos: Covid-19, China, and inauthentic influence on Facebook”.
86. Fergus Ryan, Audrey Fritz, and Daria Impiombato, “TikTok and WeChat,” 9.
87. Ibid.

THE CYBER DEFENSE REVIEW

◆ NON-COVID-19 RESEARCH ARTICLES ◆

Homefront to Battlefield: Why the U.S. Military Should Care About Biomedical Cybersecurity

Nataliya D. Brantly

ABSTRACT

Immunity to the cybersecurity risks and potential hazards presented using biomedical devices. US Military and civilian personnel use these devices on the Homefront and battlefield. As the use of biomedical devices increases with time and blurs the lines between private and professional, more attention is required of the U.S. Department of Defense (DoD) to understand the strategic importance of securing biomedical devices. This work provides a better understanding of biomedical devices and analyzes current use of biomedical devices within DoD. It also provides recommendations on actions DoD can undertake to safeguard its workforce today and in the near future. This article examines the significance of cybersecurity for biomedical devices within the context of US national security and demonstrates the important role biomedical cybersecurity plays for DoD.

Keywords: Biomedical, cybersecurity, military, defense, DoD, policy, threat

INTRODUCTION

The importance of cybersecurity to society and national security is growing as technology increasingly pervades all areas of our lives. This is true not only in business, travel and communications, but also in the provision of healthcare, in the sharing of medical records and the treatment of health conditions. Advances in computer science and biomedical engineering have enabled the collection of health data via a multitude of biomedical devices. Such devices offer new lifesaving solutions and enable proximate and non-proximate monitoring of a number of physiological conditions including sleep patterns, heart rate, exercise, blood glucose levels and many other measurements on a daily basis without the direct involvement of a healthcare professional.

© 2021 Nataliya D. Brantly



Nataliya D. Brantly is a Doctoral Student in the Science and Technology Studies (STS) program as well as a graduate student in the Master of Public Health program at the Virginia Polytechnic Institute and State University. Her research interests are broadly in the areas of biomedical security, global health, medicine, and technology.

A number of life-sustaining and lifesaving biomedical devices are in use by the general public and U.S. Department of Defense (DoD) personnel ranging from heart monitoring devices to insulin pumps to implantable cardioverter defibrillators (ICDs). These technologies, while remarkable in their lifesaving abilities, also carry with them the potential for negative health outcomes at the hands of malicious actors. With the expanded use of biomedical devices by active duty and civilian personnel, such devices are becoming an increasing part of the DoD. As a result, the cybersecurity implications of these devices should be taken into consideration in vulnerability assessments and risk prevention programs.

As medical care becomes increasingly infused with technology unique challenges arise including: the potential loss of information, unauthorized intrusion, or manipulation of health-related data from associated biomedical devices or other manipulations, and degradations of equipment that might result in life threatening consequences. There are numerous academic and popular articles describing the multitude of medical devices.^[1] Similarly, there are a number of articles examining hacks performed against biomedical devices. Those include attacks against wearable devices to disable them, obtain collected data, take advantage of the connection between the wireless device and a personal computer,^[2] data breaches and theft of medical records,^[3] to name just a few. In addition to potential risks to the general population, the US military is also vulnerable to novel threats in an increasingly digitally connected world. This applies not only to the growing connectivity of troops around the world but also to the wearable and medical devices used by US military personnel and their families worldwide, and also to point of care locations using medical devices to care for soldiers, their families, and veterans.

Recently, the DoD has emphasized the strategic importance of critical infrastructure cybersecurity, collaboration with international and domes-

tic partners to promote cybersecurity,^[4] the security of federal information systems and national security systems (e.g., SIPRNet and NIPRNet), supply chain cybersecurity, combating cyber espionage, or protection of intellectual property and the development of a robust cybersecurity workforce.^[5] Healthcare, medical, and biomedical cybersecurity have not been explicitly articulated as items of strategic importance for the DoD. The Command Vision for U.S. Cyber Command does not mention biomedical security, nor does it list it as an area of concern. Data presented in this article aims to demonstrate the significance and relevance of biomedical cybersecurity to the DoD and present it as an essential component of the nation's overall cybersecurity strategy.

Biomedical cybersecurity differs from general cybersecurity in a number of ways. First, the benefits received from biomedical devices can be directly lifesaving or life sustaining. Often the benefits of such technology outweigh the risks. However, there is a delicate balance between providing needed biomedical technology to assist with a health issue in a timely manner versus offering timely introduction to the market of needed technology. The key is offering functionality and convenience of use while ensuring the technology is not easily vulnerable to malicious actors. Second, the data collected via cybersecurity breaches is physiological, and include personally identifiable information (PII) derived from biomedical devices. Third, the severity and consequences of potential direct cybersecurity manipulations differ. Biomedical device manipulations can result in lethal outcomes as many devices in use are essential to maintain life or provide critical information to clinicians when making healthcare decisions for a patient.

Biomedical cybersecurity is the protection of biomedical devices from unauthorized intrusion to retrieve or modify information or affect the functionality of such devices. Biomedical cyber threats affect the health, wellbeing, and safety of the US military, through the degradation of the accuracy of clinical decisions adversely affecting the operation of the devices, and impacting the timely recovery and return of military personnel to duty. Moreover, intrusions into DoD biomedical systems can also affect DoD reputation and trust, disclose physical locations on the battlefield, and cause critical mission disruptions. It is essential for US military to stay operational and at full strength on the battlefield and on the Homefront. Biomedical cybersecurity is an important component in overall cybersecurity and should be an important consideration for the DoD to keep military and civilian personnel operational. Biomedical security, awareness of potential disruptions as well as acquisition of skills in preventing and mitigating such disruptions can make the difference between mission success and mission failure.

This article is divided into four sections to address US military biomedical cybersecurity considerations. Section 1 offers a general introduction to biomedical devices. Section 2 reviews biomedical devices in use by US military now and planned use in the near future. Section 3 analyzes threats in cybersecurity of biomedical devices for US military. Section 4 concludes by discussing the importance of biomedical cybersecurity for US military and draws parallels between military biomedical security and general population biomedical security.

The Basics of Biomedical Devices

Advances in biomedical engineering, computer science and modern medicine enabled the development and the introduction to the market a number of medical devices that offer health monitoring, drug delivery, life maintaining and lifesaving functionality to individuals. Healthcare is being revolutionized by digital technology, mobile medical applications and by software and hardware-based products that help clinicians make decisions daily. Such biomedical engineering is defined as “the application of engineering principles, practices, and technologies to the fields of medicine and biology especially in solving problems and improving care (as in the design of medical devices and diagnostic equipment or the creation of biomaterials and pharmaceuticals).”^[6] In the field of biomedical engineering scientists and engineers design hardware and software products to address problems within the fields of medicine, public health and related fields to resolve health issues and improve health outcomes.

The main authority responsible for implementing and enforcing regulations pertaining to medical devices in the US is the U.S. Food and Drug Administration’s (FDA) Center for Devices and Radiological Health (CDRH).^[7] The CDRH works to establish regulatory standards for the safety and efficacy of medical devices, and it places emphasis on rigorous science so that American patients are assured a reasonable degree of quality, reliability and effectiveness of healthcare.^[18] The primary mission of CDRH is to protect and promote public health to “assure that patients and providers have timely and continued access to safe, effective, and high-quality medical devices and safe radiation-emitting products.”^[9]

The FDA groups medical devices into three classes based on risk and the ability to ensure safety and effectiveness of the device.^[10] Class I devices are low-risk and include non-electronic medical devices such as bandages, tongue depressors, stethoscopes, examination gloves, handheld surgical instruments etc. Such devices are not intended to sustain life, support life or prevent disability. Class II devices have intermediate or moderate risk and include devices such as infusion pumps for intravenous medications, powered wheelchairs, and computed tomography (CT) scanners to name a few. They are intended to support or sustain human life. Class III devices are high-risk and crucial to maintain health and sustain life. Among those are artificial pacemakers, insulin pumps and deep-brain stimulators. Such devices are important in preventing impairment of human health and pose a potential risk of illness or injury if the device fails.

Biomedical devices analyzed in this paper exclude Class I devices as they are not a cybersecurity risk. Class II and Class III devices containing a central processing unit (CPU), electronic devices with wireless or wired connectivity to other devices or networks are considered in this paper. It is also important to consider other digital health products such as software for medical devices. Further discussion of biomedical devices will encompass considerations of both hardware and software.

This article groups biomedical devices into three main categories that will be further discussed in more detail and summarized in the table below. The first category is wearable devices (wearable trackers, clothing, health assist devices, infusion devices, implanted devices, ingestibles). The second category is healthcare medical devices (diagnostic devices, monitoring devices, treatment devices). The third category is software health products (health recordkeeping and sharing products, mobile apps).

1. Wearable Devices

Wearable devices (wearables) are electronic networked devices that contain sensors and microchips,^[11] can collect physiological data, can be worn on the user's body and can execute a variety of actions based on user's needs and device capabilities. Wearables can be further subdivided into six groups based on function and impact. Wearable trackers (a.k.a. fitness trackers or activity trackers) are widely used in US with increasing popularity. Wearable trackers continuously track general health and wellness with outputs such as heart rate, step count, sleep patterns, exercise, and calorie consumption, as well as GPS tracking. Wearable activity trackers are the most widely used wearables within an ever-increasing segment of the US consumer market.^[12]

Clothing, as biomedical technology, is gaining traction as a subset of wearable devices. This is possible through the development of novel fabrics (conductive and touch sensitive materials), "smart" accessories (e.g., buttons, belts, embroidery), and ways to integrate technology into the clothing through fabric-based sensors and electrodes.^[13] Biomedical clothing has the capability to "monitor physiological, neurological, and body kinematic parameters"^[14] such as Electrocardiograms (ECGs), Electromyogram (EMG), pulmonary activity, skin Ph, blood pressure, temperature, body position, comprehensive sleep patterns and impact detection. Biomedical clothing is used in gaming industry, professional sports and fitness, health, medicine,^[15] and the military.^[16]

Among health assist and monitoring devices are small wearable devices that help individual patients with a particular health need or issue. Among such devices are hearing aids, electronic contact lenses^[17] or glasses as well as continuous glucose monitoring (CGM) systems and mobile ECG monitors. Additional health monitoring devices are wrist bands to detect elderly falls,^[18] blood pressure monitors^[19] and ultrasound scanners connected to smart phones.^[20] Infusion devices are wearable biomedical devices designed to deliver medication to individual patients. Examples of such devices are injectable technologies to treat a number of health issues in oncology, cardiovascular and diabetes care, autoimmune disorders and infectious diseases. Insulin pumps are one of most widely used infusion devices that are customized to user's needs and provide lifesaving solutions to the patient. Implanted devices are essential for an individual's life. Examples of implanted devices include implantable cardioverter defibrillators (ICDs), heart pacemakers and ventricular assist devices (VADs). Ingestible devices include

consumable pills used to monitor the gastrointestinal tract, evaluate how the patient is affected by prescribed medication and to assess medication adherence. Capsule ultrasound (CUS) device, a small ingestible disposable wireless imaging sensor based on ultrasound technology, is an example of ingestible device that provides a new method of diagnosing gastrointestinal diseases.^[21] Another example is Proteus Discover, ingestible sensor that provide information about patient's health patterns and the effectiveness of medical treatment resulting in more informed healthcare.^[22] Proteus Discover was first used commercially in 2012 in the UK and in 2016 in the US^[23] with subsequent expansion to eight health systems in US by June 2017.^[24]

2. Healthcare Medical Devices

Healthcare medical devices are primarily used at the point of care locations such as hospitals, clinics, urgent care facilities, group medical practices and with individual providers. Such entities collect, store and exchange significant amounts of medical data generated by diagnostic, monitoring and treatment biomedical devices. Diagnostic biomedical devices are used to conduct testing and diagnose health conditions. Examples of diagnostic devices are ophthalmoscopes, ultrasound, digital medical laboratory equipment, radiological and imaging radiological equipment (computed tomography (CT), magnetic resonance imaging (MRI), mammography, positron emission tomography (PET), radiography, fluoroscopy). Monitoring biomedical devices are used to continuously collect health data to monitor patient's vital signs. Among such devices are digital sphygmomanometers (blood pressure monitors), ECG (electrical signal evaluation in the heart) and electroencephalogram (EEG—electrical activity evaluation in the brain). Treatment biomedical devices are used for the treatment of health conditions for the support of life. Examples are drug dosing and delivery equipment such as infusion pumps, life support equipment such as cardiopulmonary bypass (CB) devices, medical ventilators, dialysis machines and neonatal incubators.

3. Software Health Products

Software health products include a large number of software products used by healthcare providers, software used on personal computers and mobile phones in the form of mobile medical applications. A variety of software products are designed to provide a health benefit for patients and provide health management solutions for healthcare providers to diagnose, treat, predict risk and treatment response.^[25]

Electronic health recordkeeping systems and exchanges for health-related data are used by health care providers, hospitals, health information technology developers, patients, testing laboratories, manufacturers of medical devices (public and private entities) engaged in the evaluation of health information technology performance and other entities or individuals.^[26] The severity of threats coming from such systems depend on the interoperability of biomedical devices with the systems, which security features have been implemented, and the ease of submitting, accessing and exchanging health data. Threats to health records from cybersecurity arise from a wide range of unauthorized system access types including the retrieval,

modification or manipulation of health records. Consequences of such breaches range from patient inconvenience, data and monetary losses to inaccurate diagnosis and death.

Large numbers of individuals can be affected simultaneously via cybersecurity breaches at point of care entities. This can lead to significant data losses as exemplified by Community Health Systems' cyber-attack and theft of 4.5 million patient records.^[27] Such entities are targeted for the volume and diversity of data collected, stored and exchanged.^[28] Hackers target medical entities for the theft of records because of the high profitability of such records.^[29] In 2018 IBM sponsored "The Cost of a Data Breach" study conducted independently by Ponemon Institute. This study identified \$408.00 to be the average global cost per lost or stolen record for healthcare industry compared to \$148.00 per stolen record of personal or sensitive information in other industries.^[30] The breach of healthcare industry and biomedical cybersecurity is a lucrative business for cyber criminals.^[31] After a credit card breach, one can relatively easily recover by closing the account or changing a bank.^[32] On the other hand, a medical records breach offers limited options for individual remediation due to insurance restrictions and limited provider availability.^[33] Threats to biomedical devices or their support systems affect not only the individual, but also the healthcare entities suffering significant financial losses.

Biomedical Devices Used or Planned for the Military

The US military uses numerous biomedical devices, both at home and on the battlefield. These include devices such as wearable trackers, biomedical clothing, health assist devices, infusion devices and implanted devices as outlined below. On the Homefront such wearable devices are used for personal fitness or health needs on a daily basis and for conducting training missions in preparation for the battlefield. Wearable biomedical devices on the battlefield are used to monitor vital signs for combat troops. The use of wearable biosensors can detect dehydration and other performance and health metrics to provide accurate assessments of these aspects of force readiness in real-time.^[46] Biomedical clothing devices used by Soldiers can detect impact wounds from a bullet or shrapnel penetration, sense chemical, thermal, and physical attacks, and other battlefield hazards so that appropriate medical care or tactical awareness is provided. Such systems offer the potential for real-time non-invasive health monitoring.^[47] For example, U.S. Army Research Institute of Environmental Medicine (USARIEM) conducted "field studies using wearable physiological monitors" to understand "how low core temperatures went in metabolically challenged Ranger School students, and how high they went during Marine patrolling activities in Iraq and Afghanistan."^[48]

Wearable biomedical devices used by the military during training and field studies provide useful information about an individual's vital signs, health condition and stress management thus improving training outcome and reducing the time to reach desired goals. The U.S. Army uses wireless and wired monitoring systems in vehicles to monitor performance and safety in real-time, the introduction of comparable systems for Soldiers has been in research and development for over 50 years.^[49] A real-time wireless physiological status monitoring system was

WHY THE U.S. MILITARY SHOULD CARE ABOUT BIOMEDICAL CYBERSECURITY

Table 1. Description of biomedical devices types with examples and associated risk assessment summary.

Biomedical Device Type	Examples	Risk Assessment
Wearable Devices		
Wearable Trackers	Apple Watch, Microsoft Band, Fitbit bands, CGM, Garmin VivoSport	Data theft, location disclosure, unauthorized tracking, espionage, identity theft
Biomedical Clothing	AIO smart sleeve, Owlet Smart Sock, E-Skin ^{*(34)} , GT Wearable Motherboard ^{*(35)} , NFC smart suit ⁽³⁶⁾ , Smart Pajamas ^{*(37)} , Hexoskin ⁽³⁸⁾ , BioSscarf ⁽³⁹⁾	Overheating, data theft, espionage
Health Assist and Monitoring Devices	Hearing aids, electronic contact lenses ^{*(40)} or glasses ⁽⁴¹⁾ , CGM, ECG, Muse ⁽⁴²⁾ , EEG, BodyGuardian Heart ⁽⁴³⁾	Disabled device, data manipulation, modification and theft
Infusion Devices	Insulin Pump, continuous drug delivery devices	Data theft, device manipulation, overdose, hospitalization, death
Implanted Devices	Pacemakers, ICDs, VADs	Data manipulation, modification and theft,
Ingestibles	Proteus Discover, Capsule Ultrasound ^{†*(44)} , PillCam ⁽⁴⁵⁾	Data manipulation, modification and theft
Healthcare Medical Devices		
Diagnostic Devices	Ophthalmoscopes, ultrasound, digital medical laboratory equipment, radiological and imaging radiological equipment (CT, MRI, PET, DEXA scan, x-ray, nuclear medicine)	Data manipulation, modification and theft, inaccurate diagnosis, internal threats, espionage, death
Monitoring Devices	Digital sphygmomanometers, ECG, ICU equipment	Data theft, data spoofing, prolonged recovery, internal threats, espionage, prolonged recovery, death
Treatment Devices	Drug dosing systems, infusion pumps, cardiopulmonary bypass (CB) devices, medical ventilators, dialysis machine and neonatal incubators	Data manipulation, modification and theft, inaccurate diagnosis, drug overdose, internal threats, espionage, prolonged recovery, death
Software Health Products		
Software Health Products	Mobile apps, health Recordkeeping and Exchange, Health Databases, medical billing software, patient medical portals	Data manipulation, modification and theft, identity theft, clinical-billing-insurance multipoint data transfer breaches, financial loss, internal threats, outdated software/operating system, espionage, supply-chain attack method, identity theft, inaccurate diagnosis, mistreatment, death

**Biomedical devices in development*

used to monitor thermal work-strain during Marine Corps training at Camp Geiger, NC, which identified trainees could be challenged more to reach a higher fitness level.^[50] Such systems are able to provide individual data so that training can be tailored more effectively to reach

higher output. In 2018 the Pentagon restricted the use of wearable trackers and apps that rely on geolocation for deployed service members at sensitive locations.^[51] However, such devices and apps are still used by US military members and civilian employees on military installation and other locations not designated as operational areas.^[52]

Biosensor development and use by US military is used to “provide combat casualty care and is targeted towards Soldiers and support personnel on battlefields.”^[53] The US military is investing resources into biomedical research. For example, the U.S. Air Force Office of Scientific Research is supporting research in “smart” pajamas, biomedical clothing that can monitor sleep patterns, heartrate, movement, pressure changes and posture.^[54] Researchers and military personnel realize the importance of sleep in productivity, stress management, disease prevention, mental agility and improvement of decision-making skills through better sleep habits.^[55] Additionally a large number of military members suffer from hearing loss, tinnitus and other hearing disabilities therefore hearing aids or prosthetic devices are widely used.^[56]

US military personnel also use to wearable devices for personal medical needs. There are a number of medical conditions that can disqualify an individual from joining the military;^[57] however, if health conditions were diagnosed during the military service an individual might be allowed to continue serving. For example, Diabetes Mellitus of any type is listed as a disqualifying condition, but an active duty military member diagnosed with Type 1 Diabetes Mellitus (T1DM) is more likely to continue service with reliance on biomedical devices and telemedicine for remote locations.^[58] A Soldier with T1DM has the same health needs, the same access to biomedical devices and the same vulnerabilities associated with such devices as non-military patients.

Medical devices to diagnose, monitor and treat individuals are available via multiple health-care providers. Generally, biomedical devices whether on the Homefront or on the battlefield suffer from same cybersecurity vulnerabilities. However, some remote locations might have less availability for such devices thus reducing the associated cybersecurity threat. The DoD has worked to bridge the gap and provide needed medical care to soldiers in remote locations. Teleradiology is an example of such an effort. The US military has pioneered the implementation of teleradiology to provide access to needed services in remote locations around the world.^[59] Teleradiology has enabled cost and travel time reductions, increased safety, and saved resources for the US military.^[60]

Software health products, health recordkeeping and sharing systems remain vulnerable regardless of the location of soldiers since such records are in an electronic format and often stored in the cloud. Software health products also have multiple points of vulnerability as medical records and patient’s PII are transferred between doctor’s offices, billing services, insurance companies for reimbursement, etc.

Threats in Cybersecurity of Biomedical Devices for the Military

Biomedical device cybersecurity failures on the Homefront or battlefield can lead to serious consequences, not only for individual Soldier's health and wellbeing, but also for the overall mission success. Such threats can be grouped into three risk categories based on severity of consequences: low, moderate, and high. It is also important to highlight that the threat levels of biomedical device cybersecurity differ depending whether it is used on the Homefront or the battlefield.

This article defines low-risk threats as those with little effect on human life and mission success. Among low-risk threats on the Homefront are wearable activity trackers, from activity bands to "smart" watches. The nature of the information collected by such devices is not likely to cause injury or to affect mission. However, threats that would generally be considered low risk on the Homefront, such as the use of fitness wearables and potential loss of information collected by such technology, can have a different effect when considered in terms of battlefield effects. As most wearables today have integrated GPS capabilities, a threat of location disclosure for US forces can lead to mission failure and potentially to loss of life.

In 2017, Strava's disclosure of the heat map data visualization of its user's activities and the early 2018 uncovering of military personnel activity tracking are examples of such an operational security breach.^[61] Strava is a fitness app and a self-described "social network for athletes," such as runners and cyclists, to track, analyze and share a number of workout metrics. Strava's heat map disclosed the locations of remote military bases, individual's exercise routines on base and "the identities of soldiers based there."^[62] Additionally, data collected by the Polar app, another application used for exercise tracking, revealed service members' names, home addresses, deployment history locations, "soldiers' movements in hotspots like the Crimea, Baghdad, and Guantanamo" to name a few.^[63] The Pentagon's subsequent restriction of wearable trackers and apps that rely on geolocation for deployed service members at sensitive locations, does not apply to US military members and civilian employees on military installations and other locations not designated as operational areas.^[64]

In Ukraine, Russian information warfare units utilized the devices of individual soldiers to engage in location tracking, propaganda and disinformation, and for direct and indirect fires targeting.^[65] The battlefield use of devices such as Strava, Polar, or others is no longer abstract, the tracking of military members in the field has been achieved with deadly effect.^[66] All indications are that barriers to infiltrating, manipulating, tracking or otherwise harnessing personal devices used for biomedical or similar uses are rapidly disappearing as adversary nations are developing the skills to utilize our own devices against us.^[67]

Moderate risk threats might have a significant effect on an individual's wellbeing and can have an effect on the mission. Hospital diagnostic equipment or software assisting clinicians with a diagnosis can cause inaccurate treatment or diagnosis, causing prolonged treatment,

worsening of a health condition, mistreatment, prescription of incorrect medications, overdose and/or potentially a loss of life.

The threat of hacking a biomedical device that individuals rely on for diagnosis and treatment is particularly worrisome. And this is just not a possibility; it is a reality today. Edited medical records or malware enabled modified radiological images with removal or addition of cancerous nodules can lead to misdiagnosis and mistreatment for patients that need critical and timely care.^[68] The removal of cancerous growth from X-ray images in patients with cancer led to 94% rate of misdiagnosis of such patients as being healthy.^[69] The 2018 reports of malware infected computers that support biomedical devices such as MRIs and X-Rays machines demonstrated the reality of such threat.^[70]

High risk threats are those that will lead to loss of life and/or complete mission failure. Devices that support or sustain life have the highest chance of causing lethal effects if compromised. Among these are implanted devices such as insulin pumps that, if compromised, can administer lethal dose of insulin. The above-mentioned risks apply to both Homefront and the battlefield. The risks of such threats on the battlefield can have larger consequences. Even if a single individual is affected during a critical mission, the consequences of such threat can lead to the whole team to be affected. Every individual on the team plays a role; hence, having even a single service member out can lead to insufficiency of resources for the mission, lack of critical skill or lack of leadership.

Researchers demonstrated unauthorized access to an implantable cardiac defibrillator and were able to retrieve name, date of birth and diagnosis, switch off saved settings, thereby leaving the device unresponsive to emergencies, remotely causing it to emit a shock.^[71] Modern implantable pacemakers are also equipped with wireless connectivity and transmit data to and from the device.^[72] In 2007, the cardiologist for Vice President Dick Cheney disabled the wireless functionality of the Vice President's pacemaker because of the cybersecurity risks posed by the device.^[73] In 2012, researcher at Black Hat security conference demonstrated how a deadly 830-volt shock can be delivered by a pacemaker through hacking vulnerabilities in the device using a laptop computer from distance of 50-feet away from a potential victim.^[74] Insulin pumps have similarly been found to have cybersecurity risks, and studies show how easy it is to gain unauthorized access to the device to disable it, cause delivery of modified amount of insulin or empty the content of the pump into the patient to deliver a lethal dose of the medication.^[75]

The increased connectivity of multiple devices poses additional challenges. Synchronization of biomedical devices with smartphones, computers and other non-biomedical technology by design is becoming a use-driven demand from industry and consumers. A Wireless Body Area Network (WBAN) is a "sensor network that enables various medical sensors located inside or outside the human body to communicate seamlessly with one another, and integrate automatically with existing devices, such as smartphones".^[76] There are challenges in securing WBAN

not only because of the connectivity among multiple devices, but also because the individual is often on the move along with the network.

The DoD should also start thinking beyond visible wearable devices. The FDA has started regulating precision medical devices such as next generation sequencing (NGS) technology that can now examine genomic variances of a large number of individuals at the same time to determine if an individual has certain health conditions or is at a risk of a disease.^[77] The DoD should take note of such technology and how it can affect US military. In particular, the potential of NGS technology to quickly detect health conditions and target individuals should be of great concern.

CONCLUSION

The DoD is investing significant resources both in financial and intellectual capital to improve soldier survivability on the battlefield to ensure mission success. Using biomedical technology and the development of lighter, more efficient toolkits, the DoD is preparing warfighters for technologically advanced conflicts. To outsmart the other side, the US military must be aware of and capable at battling cyber espionage, cybercrime, and other cyber threats. Biomedical technologies are becoming increasingly essential tools in modern conflict. Consequently, the cybersecurity threats to such technologies cannot be ignored. It is important to prepare US military personnel for the biomedical cybersecurity threats of today as well as proactively analyze and address critical threats that will arise in the future. The DoD should consider biomedical security from the micro to the macro scale, from the vantage point of an individual, team, DoD, and the nation.

It is important to conduct education, training, active learning and regular reviews of potential cyberthreats to develop awareness on an individual level. Individual awareness of cybersecurity vulnerabilities to biomedical devices and associated systems begins the process of identifying potential risks and threats affecting individual health situations. It is vital to prepare and educate individuals to be conscious of biomedical cyber threats affecting them at the Homefront or the battlefield. One individual's actions can significantly affect a mission, the safety of a team and the security of the nation. The DoD would benefit from adopting the Patient Centric Cybersecurity Framework as a tool to empower the workforce and foster trust, effective communication, and more accurate data flows to enhance decision-making processes.^[78]

Every US military unit and team should take stock of biomedical devices in use on and off duty to ensure awareness, be proactive in assessing potential threats, and determine how to avoid or correct issues. The DoD should elevate the security of biomedical devices in use by the military to a level of strategic importance. This does not only apply to combat biomedical devices, but also to biomedical devices for personal use. The DoD should effectively regulate such devices via policy to ensure the fidelity of medical devices, and should raise awareness via

workforce education, research, internal reviews as well as cooperation and teamwork against cyber-criminal networks exploiting biomedical devices. These efforts should span multiple levels with the intent of fostering best practices and creating synergies better able to detect and combat malicious behaviors. Biomedical devices used by the general population are also used by military personnel. The device ecosystems are deeply intertwined and vulnerabilities within biomedical devices within either the military or the civilian sectors of biomedical devices, are unlikely to stay segregated from one another. The result is that both are exposed to increased levels of risk.

Finally, US military and the Department of Veterans Affairs acquisitions within the broader landscape of the US healthcare market are large and expanding. While the arbitrary implementation of wide-ranging regulation should be avoided, the DoD's directed and conscientious effort to provide better implementation of cybersecurity for biomedical devices will be a significant factor in future conflicts. Moreover, DoD innovations in biomedical cybersecurity will assure better outcomes for the nation as a whole.🛡️

NOTES

1. Jamin Casselman, Nicholas Onopa, and Lara Khansa, "Wearable healthcare: Lessons from the past and a peek into the future," *Telematics and Informatics*, 34, no. 7 (2017): 1011-1023, <https://doi.org/10.1016/j.tele.2017.04.011>.
2. Matteo Langone, Roberto Setola, Javier Lopez, "Cybersecurity of Wearable Devices: An Experimental Analysis and a Vulnerability Assessment Method," *IEEE 41st Annual Computer Software and Applications Conference (COMPSAC)* (2017): 304-309, doi: 10.1109/COMPSAC.2017.96.
3. "The Cost of a Data Breach," *Briefings on HIPAA*, Health Services Administration: USA, 16, no.11 (2016): 4-7.
4. "Cybersecurity Reference and Resource Guide," U.S. Department of Defense (2019), updated February 2020, https://dodcio.defense.gov/Portals/0/Documents/Cyber/2019%20Cybersecurity%20Resource%20and%20Reference%20Guide_DoD-CIO_Final_2020FEB07.pdf.
5. "National Cyber Strategy of the United States of America," National Cyber Strategy, The White House, Washington, D.C. (2018), <https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>.
6. "Definition of biomedical engineering", *Merriam-Webster Dictionary*, accessed February 25, 2021, <https://www.merriam-webster.com/dictionary/biomedical%20engineering>.
7. "Digital Health Innovation Action Plan," U.S. Food and Drug Administration (2017), accessed February 25, 2021, <https://www.fda.gov/media/106331/download>.
8. "CDRH Mission, Vision and Shared Values," U.S. Food Drug Administration (2017), accessed February 25, 2021, <https://www.fda.gov/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/ucm300639.htm>
9. "2018-2020 Strategic Priorities, Center for Devices and Radiological Health," U.S. Food and Drug Administration (2018), accessed February 25, 2021, <https://www.fda.gov/downloads/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/CDRHVisionandMission/UCM592693.pdf>.
10. "Code of Federal Regulations – Title 21 – Food and Drugs", USCODE-2010 – Title 2 – Chapter 9 – subchapter V – Part A – Section 360c, Classification of Devices Intended for Human Use (2018), accessed February 25, 2021, <https://www.govinfo.gov/content/pkg/USCODE-2010-title21/pdf/USCODE-2010-title21-chap9-subchapV-partA-sec360c.pdf>.
11. Adam Thierer, "The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation," *Richmond Journal of Law & Technology*, 21, no.2 (2015), <http://dx.doi.org/10.2139/ssrn.2494382>.
12. Sara Shahrimi, "Wearing Your Data on Your Sleeve: Wearables, the FTC, and the Privacy Implications of This New Technology," *Texas Review of Entertainment Sports Law*, 18, no.1 (2017): 1-25.
13. Gilsoo Cho, Seungsin Lee, and Jayoung Cho, "Review and Reappraisal of Smart Clothing," in *Smart Clothing: Technology and Applications*, ed. Gilsoo Cho, (CRC Press, 2009).
14. Ibid.
15. Andreas Lymberis and Silas Olsson, "Intelligent Biomedical Clothing for Personal Health and Disease Management: State of the Art and Future Vision," *Telemedicine Journal and e-Health*, 9, no. 4 (2004), <http://doi.org/10.1089/153056203772744716>.
16. C.A. Winterhalter et al., "Development of electronic textiles to support networks, communications, and medical applications in future U.S. Military protective clothing systems," *IEEE Transactions on Information Technology in Biomedicine*, 9, no. 3 (2005): 402-406, doi: 10.1109/TITB.2005.854508.
17. Jihun Park et al., "Soft, smart contact lenses with integrations of wireless circuits, glucose sensors, and display," *AAAS, Science Advances*, 4, no. 1 (2018) doi: 10.1126/sciadv.aap9841.
18. T. Elakkiya, "Wearable safety wristband device for elderly health monitoring with fall detect and heart attack alarm," *IEEE 2017 Third International Conference on Science Technology Engineering & Management* (2017): 1018-1022, doi: 10.1109/ICONSTEM.2017.8261318.
19. Jim Li and Yukiya Sawanoi, "The History and Innovation of Home Blood Pressure Monitors," *2017 IEEE History of Electro-technology Conference* (2017): 82-86, doi: 10.1109/HISTELCON.2017.8535736.
20. Hatice Koydemir and Aydogan Ozcan, "Smartphones Democratize Advanced Biomedical Instruments and Foster Innovation", *Clinical Pharmacology & Therapeutics Development*, 104, no. 1 (2018), <https://doi.org/10.1002/cpt.1081>.
21. Junyi Wang et al., "Capsule Ultrasound Device: Characterization and Testing Results," *IEEE International Ultrasonics Symposium* (2017): 1-4, doi: 10.1109/ULTSYM.2017.8092071.
22. "Proteus digital health" (2020), accessed May 21, 2020, <https://www.proteus.com/discover/>.

NOTES

23. Jonah Comstock, "California hospital becomes first in US to prescribe ingestible sensors from Proteus," *MobiHealthNews*, (2016), accessed May 21, 2020, <https://www.mobihealthnews.com/content/california-hospital-becomes-first-us-prescribe-ingestible-sensors-proteus>.
24. "Tiny Ingestible Sensor Aids Rush Doctors, Patients," Rush University Medical Center (2017), accessed February 25, 2021, <https://www.rush.edu/news/tiny-ingestible-sensor-aids-rush-doctors-patients>.
25. "Final Document: Software as a Medical Device (SaMD): Clinical Evaluation," International Medical Device Regulators Forum (IMDRF), Software as a Medical Device Working Group (2017), http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-170921-samd-n41-clinical-evaluation_1.pdf.
26. "21st Century Cures Act," PUBLIC LAW 114-255, 114th Congress (2016), <https://www.congress.gov/114/plaws/publ255/PLAW-114publ255.pdf>.
27. Dan Munro, "Cyber Attack Nets 4.5 Million Records from Large Hospital System," *Forbes* (2014), accessed May 21, 2020, <https://www.forbes.com/sites/danmunro/2014/08/18/cyber-attack-nets-4-5-million-records-from-large-hospital-system/#69647ff77f07>.
28. Daniel Nigrin, "When 'Hacktivists' Target Your Hospital," *New England Journal of Medicine*, 371, no. 5 (2014): 393-395, doi: 10.1056/NEJMp1407326.
29. "2018 Cost of Data Breach Study: Impact of Business Continuity Management," Ponemon Institute (2018), accessed February 25, 2021, <https://www.ibm.com/downloads/cas/AEJYPWA>.
30. Ibid.
31. Ibid.
32. Ibid.
33. "The Cost of a Data Breach," Briefings on HIPAA, Health Services Administration: USA, 16, no. 11 (2016): 4-7.
34. Takao Someya, "Bionic Skin for a Cyborg You," *IEEE Spectrum* (2013), accessed February 25, 2021, <https://spectrum.ieee.org/biomedical/bionics/bionic-skin-for-a-cyborg-you>.
35. "Georgia Tech Wearable Motherboard™: The Intelligent Garment for the 21st Century," Georgia Tech, accessed May 21, 2020, <http://www.smartshirt.gatech.edu>.
36. "CES 2016: NFC-Enabled Wearables, IoT Home Systems, And Sunburn Sensors," NFC Forum (2016), <https://nfc-forum.org/ces-2016-nfc-enabled-wearables-iot-home-systems-and-sunburn-sensors/>.
37. "Smart sleepwear: Introducing 'phyjama,' a physiological-sensing pajama," *Science Daily*, source: University of Massachusetts at Amherst (2019), accessed February 25, 2021, <https://www.sciencedaily.com/releases/2019/09/190912162528.htm>.
38. "HEXOSKIN Health Sensors and AI," *HEXOSKIN* Smart Garments Specifications, accessed May 21, 2020, <https://www.hexoskin.com>.
39. "The 1st scarf with air pollution, allergy, cold & flu protection built right in!" *BioScarf*, accessed May 21, 2020, <https://www.bioscarf.com>.
40. "Electronic Contact Lenses for Better Vision," *Med Gadget* (2008), accessed May 21, 2020, https://www.medgadget.com/2008/01/electronic_contact_lenses.html.
41. "Top 5 Electronic Glasses for the Blind and Visually Impaired," IrisVision, accessed May 21, 2020, <https://irisvision.com/electronic-glasses-for-the-blind-and-visually-impaired/>.
42. "EEG-Powered Sleep: Tracking & Meditation," *Muse*, accessed May 21, 2020, <https://choosemuse.com>.
43. "Listen to the Beat," *BodyGuardian Heart*, accessed May 21, 2020, <https://www.preventivesolutions.com/patients/body-guardian-heart>.
44. Benjamin Cox et al., "Ultrasound capsule endoscopy: sounding out the future," *Annals of Translational Medicine*, 5, no. 9 (2017), <https://doi.org/10.21037/atm.2017.04.21>.
45. "PILLCAM™ SB 3 SYSTEM," Medtronic, accessed May 21, 2020, <https://www.medtronic.com/covidien/en-us/products/capsule-endoscopy/pillcam-sb-3-system.html>.
46. "Wearable sensors could leverage biotechnology to monitor personal, environmental data," CCDC Army Research Laboratory Public Affairs (2019), accessed May 21, 2020, <https://www.army.mil/article/221184>.
47. Gilsoo Cho, Seungsin Lee, and Jayoung Cho, "Review and Reappraisal of Smart Clothing," in *Smart Clothing: Technology and Applications*, ed. Gilsoo Cho (Boca Raton, FL: CRC Press, 2009).

NOTES

48. Reed Hoyt, Karl Friedl, "The future of wearable tech," U.S. Army (2016), accessed May 21, 2020, https://www.army.mil/article/161761/the_future_of_wearable_tech.
49. Ibid.
50. Ibid.
51. Tara Copp, "Fitbits and fitness-tracking devices banned for deployed troops," *Military Times* (2018), accessed May 21, 2020, <https://www.militarytimes.com/news/your-military/2018/08/06/devices-and-apps-that-rely-on-geolocation-restricted-for-deployed-troops/>.
52. "Use of Geolocation-Capable Devices, Applications, and Services," Deputy Secretary of Defense, Memorandum (2018), accessed May 21, 2020, https://partner-mco-archive.s3.amazonaws.com/client_files/1533573228.pdf.
53. Rainee Simons, "Body-Sensor Networks for Space and Military Applications," in *Antennas and Propagation for Body-Centric Wireless Communications*, 2nd ed. Peter Hall, Yang Hao (New York: Artech House, Inc., 2012), 271-290.
54. "'Smart' pajamas could monitor and help improve sleep," American Chemical Society (2019), accessed May 21, 2020, <https://www.acs.org/content/acs/en/pressroom/newsreleases/2019/april/smart-pajamas-could-monitor-and-help-improve-sleep-video.html>.
55. Ibid.
56. Larry Humes, Lois Joellenbeck, and Jane Durch, eds., *Noise and Military Service: Implications for Hearing Loss and Tinnitus*, Institute of Medicine (Washington, D.C.: The National Academies Press, 2006), <https://doi.org/10.17226/11443>.
57. "Join the Military: Eligibility Requirements. Medical Conditions That Can Keep You From Joining the Military," *Military.com*, accessed May 21, 2020, <https://www.military.com/join-armed-forces/disqualifiers-medical-conditions.html>.
58. Sammy Choi and Jon Cucura, "US Army Soldiers With Type 1 Diabetes Mellitus," *Journal of Diabetes Science and Technology*, 12, no. 4 (2018), 854-858, <https://doi.org/10.1177/1932296818767700>.
59. E.R. Ranschaert and Barneveld Binkhuysen, "Teleradiology: Evolution and Concepts," *European Journal of Radiology*, 78 no. 2 (Elsevier Ireland Ltd, 2011), 205-209, doi:10.1016/j.ejrad.2010.08.027.
60. M.R. Brumage, S. Chinn, and K. Cho, "Teleradiology in a Military Training Area," *Journal of Telemedicine and Telecare*, 7, no. 6 (2001), 348-52, doi:10.1258/1357633011936994.
61. Katelyn Newman, "Fitness App Strava Reveals Military Security Oversight," *USNews.com* (2018,) accessed May 5, 2019, Gale General OneFile, https://link.gale.com/apps/doc/A525573438/ITOF?u=viva_vpi&sid=ITOF&xid=ca0fc22a.
62. "How Strava's Heat Map Uncovers Military Bases," *NYTimes.com Video Collection*, World History in Context (2018), accessed May 5, 2019, https://link.gale.com/apps/doc/CT526718358/WHIC?u=viva_vpi&sid=WHIC&xid=0cbe492f.
63. "After Strava, fitness app Polar exposes location history of soldiers and spies," *Media Nama* (2018), Computer Database, accessed May 5, 2019, https://link.gale.com/apps/doc/A545911140/CDB?u=viva_vpi&sid=CDB&xid=71107de7.
64. Tara Copp, "Fitbits and fitness-tracking devices banned for deployed troops," *Military Times* (2018), accessed May 21, 2020, <https://www.militarytimes.com/news/your-military/2018/08/06/devices-and-apps-that-rely-on-geolocation-restricted-for-deployed-troops/>.
65. Aaron F. Brantly, Nerea Cal, and Devlin Winkelstein, "Defending the Borderland: Ukrainian Military Experiences with IO, Cyber, and EW," *The Cyber Defense Review* (2017), <https://cyberdefensereview.army.mil/Portals/6/Documents/UA%20Report%20Final%20AB.pdf>.
66. Jeff Roberts, "How Russia Used a Poisoned App to Spy on Ukraine's Military," *Fortune* (2016), accessed February 25, 2021, <https://fortune.com/2016/12/22/russia-ukraine-app/>.
67. Aaron F. Brantly and Liam Collins, "A Bear of a Problem: Russian Special Forces Perfecting Their Cyber Capabilities," *Army Magazine*, 68, no. 12 (2018).
68. Kim Zetter, "Hospital viruses: Fake cancerous nodes in CT scans, created by malware, trick radiologists," *The Washington Post* (April 3, 2019), accessed May 21, 2020, https://www.washingtonpost.com/technology/2019/04/03/hospital-virus-fake-cancerous-nodes-ct-scans-created-by-malware-trick-radiologists/?noredirect=on&utm_term=.5elb44764063.
69. Michael Kan, "Scary Hacking Threat: Editing X-Ray Images to Add or Remove Cancer," *PCmag* (2019), accessed May 21, 2020, <https://www.pcmag.com/news/367598/scary-hacking-threat-editing-x-ray-images-to-add-or-remove>.
70. Ibid.

NOTES

71. Neal Leavitt, "Researchers Fight to Keep Implanted Medical Devices Safe from Hackers," *Computer*, 43, no. 8 (Washington, D.C.: IEEE Computer Society Press, 2010), 11-14, doi: <https://doi.org/10.1109/MC.2010.237>.
72. Aaron F. Brantly, "The Violence of Hacking: State Violence and Cyberspace," *The Cyber Defense Review* (2017), 73-92, doi:10.2307/26267402.
73. Daniel Clery, "Could your pacemaker be hackable?" *Science*, 347, no. 6221, (AAAS, 2015): 499, <https://science.sciencemag.org/content/sci/347/6221/499.full.pdf>.
74. Mandeep Khera, "Think Like a Hacker," *Journal of Diabetes Science and Technology*, 11, no. 2, (2016): 207-212, doi:10.1177/1932296816677576.
75. David Klonoff, "Cybersecurity for Connected Diabetes Devices," *Journal of Diabetes Science and Technology*, 9, no. 5 (2015): 1143-1147, <https://doi.org/10.1177/1932296815583334>.
76. Jamin Casselman, Nicholas Onopa, and Lara Khansa, "Wearable healthcare: Lessons from the past and a peek into the future," *Telematics and Informatics*, 34, no. 7 (2017): 1011-1023, <https://doi.org/10.1016/j.tele.2017.04.011>.
77. "FDA Advances Precision Medicine Initiative by Issuing Draft Guidances on Next Generation Sequencing-Based Tests," U.S. Food and Drug Administration, (2016), accessed February 25, 2021, <https://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm509814.htm>.
78. Aaron F. Brantly and Nataliya D. Brantly, "Patient-centric cybersecurity," *Journal of Cyber Policy*, 5, no.3 (2020): 372-391, <https://doi.org/10.1080/23738871.2020.1856902>.

Factors That Motivate State-Sponsored Cyberattacks

Lance Y. Hunter, Ph.D.

Craig Douglas Albert, Ph.D.

Eric Garrett

ABSTRACT

The study of the factors involved in the initiation of violent interstate conflicts has been well documented within international relations. However, scholars have yet to analyze the factors associated with the initiation of international state-sponsored cyberattacks due to the lack of available data. This study is a first attempt to address this limitation. This project examines the political, economic, and military factors associated with the initiation of state-sponsored cyberattacks from 2005–2012, using a unique dataset that incorporates author-collected political, economic, and military data, along with cyber data on known state-sponsored cyberattacks extracted from the Council on Foreign Relations (CFR) Cyber Operations Tracker Dataset. With this unique dataset, we seek to better understand those states most likely to cyberattack other states.

INTRODUCTION

Cyber conflict is an emerging topic within the field of international relations. Every nation has been affected in some form by illegal cyber operations deployed by other nations or groups.^[1] Sixty percent of senior internet technology officials predict that the severity of nation-state attacks against governments and corporations will continue to increase over time and even lead to all out cyber-war.^[2] Observers note: “In the future, wars will not be fought by guns or with planes that drop bombs. They will also be fought with the click of a mouse a half a world away that unleashes carefully weaponized computer programs that disrupt or destroy critical industries like utilities, transportation, communications and energy.”^[3] Scholars such as Kello contend: “[t]he implications for international security are potentially serious: according to [calculated ambiguity], a

© 2021 Dr. Lance Y. Hunter, Dr. Craig Douglas Albert, Eric Garrett



Lance Y. Hunter, Ph.D., is an Associate Professor of International Relations at Augusta University. His research focuses on how terrorist attacks influence politics in democratic countries and how political decisions within countries affect conflicts worldwide. His work has appeared in journals such as: *Journal of Peace Research*, *Terrorism and Political Violence*, *Party Politics*, *Studies in Conflict and Terrorism*, *Armed Forces and Society*, *Conflict, Security and Development*, *European Political Science*, and *Global Policy*.

cyber event can occur that does not meet the traditional definition of war but nevertheless elicits a reprisal of commensurate severity.”^[4]

While the threat of cyberconflict is ever-present, the systematic study of the factors involved in the initiation of state-sponsored cyberconflict is in its infancy stages. Factors that lead to military conflicts between nation-states has been exhaustively researched, but far less is known about the factors that precipitate cyberconflicts cross-nationally. Relatively speaking, this project is therefore one of earlier attempts to examine the political, economic, and military factors associated with the initiation of state sponsored cyberattacks, and focuses on the years 2005-12. Our dataset includes political, economic, and military data on 143 states, and on known state-sponsored cyberattacks collected from the Council on Foreign Relations (CFR) Cyber Operations Tracker Dataset (COTD). In analyzing this unique dataset, we attempt to better understand what states are more or less likely to cyberattack other states.

Here, we seek to identify those variables most important in influencing which states are most likely to initiate cyberattacks, and factors that would influence the frequency of such cyberattacks. We also include a complementary descriptive analysis of factors associated with cyberattacks by analyzing the political, economic, and military features of cyberattacking states as compared to cyberattack victim states. This descriptive analysis complements our statistical analysis to better understand the factors key to motivating state-sponsored cyberattacks. The descriptive analysis is from 2005-16.

We first examine the factors traditionally associated with military conflict between states, and then turn to how, per existing literature, such factors themselves may influence cyberconflict. We next proceed to empirical analysis, discussing first our statistical analysis and results, followed by our descriptive analysis and findings. Lastly, we present our conclusions and their implications.



Craig Douglas Albert, Ph.D., is an Associate Professor of Political Science and the Graduate Director of the Master of Arts in Intelligence and Security Studies at Augusta University, with concentrations focused on international relations, ethnic conflict, cyberterrorism and cyberwar, and the scholarship of teaching and learning. He is widely published, including articles in the *Journal of Political Science Education*; *Iran and the Caucasus*; *Politics*; *East European Politics*; *Chicago-Kent Law Review*; *Middle Grades Review*; *The Journal of International Social Studies*. Dr. Albert testified before the U.S. Congress' joint subcommittee of the House Foreign Affairs Committee concerning the Boston Bombings. You can follow him on social media @DrCraigDALbert.

Power

A large body of research within international relations links economic and military power to the initiation of military conflicts, as more powerful states tend to have a greater number of interests to protect so are more likely to initiate military conflicts in the protection of those geopolitical interests.^[5] Thus, an appropriate question to ask is, does economic and military power similarly affect the initiation of cyberconflicts?

Many scholars consider cyberpower as equal to military power projection in the physical domain and should be conceptualized and studied similarly.^[6] As such, power allows an actor to dominate other states leading the more powerful state to achieve one's interests.^[7] Additionally, it can be argued that deploying offensive cyber capabilities is less effective in projecting power than traditional kinetic military weapons because the lesser chance of palpably injuring the enemy, especially from an unsophisticated cyberattack such as a Computer Network Attack (CNA).^[8] A sophisticated cyberattack however, could yield more force projection or damage depending on the scope of the attack. Conversely, executing such an attack requires a substantial reserve of power projection capability because such an attack requires strength in technological sophistication, skill, ingenuity, reconnaissance, social engineering and sophisticated knowledge of network vulnerabilities.^[9] In other words, cyber capability is a corollary of relative power generally. However, one cannot rest assured on the strategy of deterrence to work in cyberspace. Offense holds the competitive advantage concerning the cyber offense-defense balance as, due to the difficulty of attribution, deterrence can be undermined. As Lindsay notes, "weaker actors can attack the control systems of superior adversaries to achieve levels of physical disruption possible previously only through kinetic bombing."^[10] Thus, one could argue that weaker powers are more prone to be cyber-attackers than great powers.



Eric Garrett is a recent graduate of Augusta University's Master of Arts in Intelligence and Security Studies program, holds numerous professional cybersecurity certifications in penetration testing, incident response, host and network forensics, and network and systems security monitoring.

But the flip side of this argument must also be considered. First is the fact that the flexible nature of cyber weapons render them vulnerable to be “captured, manipulated, and turned against their creators”.^[11] Also, the first-mover advantage might be more modest in the cyber domain if attacks are mitigated or otherwise rendered ineffective by a victim who responds at will, possibly even using a variant of the weapon of its attacker. If hiding the cyber weapon is key to its efficacy, offensive dominance can be easily neutralized by premature disclosure of capabilities. Asymmetric effects may only be present as disproportionate costs as weaker states can attempt to rebalance an asymmetric relationship with a more powerful state by using inexpensive tools and methods to inflict heavy victim expenses on the targeted state. Yet success of this strategy may be offset by limitations inherent to the first mover's cyber domain advantage.

Some experts explain that cyberattacks that fall short of qualifying as a coercive tool, may nevertheless be expressions of brute force as a “means of forcible accomplishments.”^[12] Cyber operations are also considered well-suited as an asymmetric warfare component that complements rather than replaces conventional operations. A cyber-plus attack describes a scenario where a computer network attack is used as a non-violent precursor to other actions to achieve direct political or military objectives.^[13] Rather than achieving a one-and-done attack or a cyber-Pearl Harbor, this could maximize conventional effects and also reduce the risk of play-back of the cyber weapons against their creators, or other collateral damage. Mazanec points to Russian cyberattacks used against the Georgian government and command and control networks as a progression of cyber tools being used “as a force multiplier to conventional military operations” causing “tangible disruption and effects beyond CNE [computer network exploitation]-style espionage.”^[14] Furthermore, these otherwise

unsophisticated attacks were ineffective unless focused on interfering with the Georgian government's ability to communicate by denying, degrading, and disrupting command and control systems.^[15]

Cyberattacks facilitate the use of non-violent means to achieve interests, whether by militarized effects or through sabotage. Complicating validation of their impact as a means of power projection is that cyberattacks generally are better suited for stealthy actions that may remain secret in both their capabilities, use, and effects.^[16] On the other hand, cyber tools used can equate to cyber tools lost, potentially giving defensive postures an advantage as costly cyber tools have a limited time in which they can reveal defensive vulnerabilities and illuminate system weaknesses that can be repaired. This also reduces the ability for coercion as the more offensive a deployed tool is, the less credibility it has when defensive postures are adjusted to defeat the exploits. A defensive mindset benefiting from greater awareness of vulnerabilities and weaknesses also drives up the costs and required level of sophistication to preserve offensive cyber weapons effectiveness.

Complicating the issue is that cyberpower, like other forms of power, can be used as hard power (i.e., a Critical Infrastructure Systems attack) or soft power through information warfare or social media weaponization designed for intelligence operations.^[17] As to weaker states, even if a regime has major cyber capabilities, if it lacks corresponding economic and/or military prowess, it may refrain from carrying out cyberattacks for fear of kinetic response. Executing a cyberattack would be too costly to risk conflict escalation and spillover effects from cyberspace to physical territory. But smaller states that can effectively carry out a sophisticated and undetectable cyberattack may view the rewards as outweighing the costs, and act more offensively in the cyber realm. As Gartzke and Lindsay write, "Cyber operations alone lack the insurance policy of hard military power, so their success depends on the success of deception."^[18] However, cyberattacks will seldom go unnoticed, particularly if attribution is intended and necessary to demonstrate power, so the balance between weaker and stronger states could rely on the known threat of disproportionate costs and the need to back up fragile capabilities with hard military power.^[19] This could form a basis of deterrence based on restraint derived from risk assessment and by considering the complementary threats and vulnerabilities of both adversary and friendly systems.

Based on the information discussed above, we present two competing hypotheses regarding the impact of power on the initiation of state-sponsored cyberattacks. The first hypothesis is that states with greater power are more likely to initiate cyberattacks due to their power advantage, which would correspond to literature on power and military conflict that finds more powerful states are more likely to initiate military disputes.

- ◆ **Hypothesis 1:** More powerful states (i.e., states with greater economic and military power) are more likely to initiate cyberattacks than weaker states.

Our second hypothesis is in respect to the notion that state-sponsored cyberattacks are often a tool used by weaker states due to the possibility of deception and the potential need for less resources (economic and military) to execute a cyberattack compared with more traditional forms of conflict.

- ◆ **Hypothesis 2:** Less powerful states (i.e., states with less economic and military power) are more likely to initiate cyberattacks than powerful states.

We now turn to examining the literature pertaining to regime type and conflict.

Regime Type

Many researchers have investigated the relationship between regime type and military conflict. This area of research has considered how the presence or absence of democratic institutions affects conflict. While research has largely confirmed that democracies generally have peaceful relations with each other,^[20] another strand of research has investigated the extent that regime type influences conflict in general,^[21] though this line of research has produced mixed results. Some research has found that democracies are as equally conflict prone as authoritarian states^[22] while other research has found that the level and type of democratic institutions within states can have pacifying effects on the likelihood of conflict.^[23] Lastly, other scholars have found that democratic and authoritarian states select into different types of conflicts due to their disparate political institutions.^[24]

While exhaustive research exists in regards to the relationship between democratization and war and the correlation between democratic regimes and peace, research examining the impact of regime type on cyberspace and how regime type influences the initiation of cyberattacks is quite limited. Yet it is reasonable to assume that states with more aggressive domestic exploitation of cyberspace are likely to have the same framework when considering cyber foreign policy. For instance, MacKinnon argues that although many hoped, especially in the technology corporate sector, that the internet would help democratize and open spaces within authoritarian regimes, cyberspace has actually had the opposite effect.^[25] MacKinnon calls this new regime space, networked authoritarianism, where the government controls netizens through internet capabilities.^[26] The author alarmingly notes that, “[s]trong governments in weak or new democracies are using second-and third-generation Internet controls in ways that contribute to the erosion of democracy and slippage back toward authoritarianism.”^[27] Stateless packet inspection, falling into the category of first-generation Internet controls, includes simple filtering methods based on metadata found within traffic headers such as machine addresses or ports and protocols. In contrast, second and third-generation Internet controls apply increasingly complex algorithms based on higher levels of traffic content, through stateful or deep packet inspection, to shape or deny traffic while maintaining awareness of context. More advanced Internet controls falling under the next-generation label increasingly seek to apply machine learning and artificial intelligence concepts to increase data tracking and awareness.^[28]

These controls may also lead to establishing behavioral norms, compliance, and imposing rules rather than hardware and software operations.^[29] With increased capabilities to examine Internet traffic, next-generation controls also collide with privacy and governance issues.

Deibert notes that authoritarian regimes are actually shaping cyberspace to their own strategic advantage, utilizing technological, legal, extralegal, and other target information controls.^[30] Generally, these measures have had “the effect of strengthening the state at the expense of human rights and civil society.”^[31] Most relevant to the present paper is Deibert’s analysis of third-generation controls, which are active offensive measures involving surveillance, targeted espionage, and other methods of covert disruptions in cyberspace.^[32] These third-generation controls target human-rights, prodemocracy, and independent movements outside the state in which the controls are launched.^[33]

Dr. Jan Kallberg argues that cyberattacks work best, according to strategic cyberwar theory against weak regimes or, “the theory’s predictive power is strongest when applied to targeting theocracies, authoritarian regimes, and dysfunctional experimental democracies, because the common tenet is weak institutions.”^[34] Kallberg further notes that fully functioning democracies have a strategic advantage in cyberwar because of their institutional stability and accepted institutions.^[35] Thus, it is reasonable to assume that democracies will not engage in cyberwarfare against one another, but are likely to engage in cyberconflict against non-democracies, or anocracies (i.e., hybrid regimes). Kallberg explains that “[a]n attack will fail to destabilize the targeted society if the institutions are intact after the attack....Therefore it is important to ensure that the attack is of the magnitude that it pushes the targeted society over the threshold to entropy.”^[36]

Based on the existing literature, we present two additional competing hypotheses regarding the relationship between regime type and the initiation of cyberattacks. The third hypothesis engages with the notion that democratic states should be less likely to initiate cyberattacks due to their domestic norms and membership in specific types of international institutions that encourage more cooperative behavior in foreign policy. This hypothesis aligns with literature that finds democratic states are more dovish compared with authoritarian regimes due to their domestic norms, which may be transferred to the international arena, along with their membership in specific international institutions that serve to moderate aggressive foreign policy behavior and promote cooperation.

♦ **Hypothesis 3:** Democratic states are less likely to initiate cyberattacks than authoritarian states.

An opposing hypothesis is that democratic states may be more likely to initiate cyberattacks as cyberattacks could be an alternative tool to actual military engagement. This proposition views democracies as more likely to advance cyberattacks because they are the less costly alternative to traditional military conflict.

- ◆ **Hypothesis 4:** Democratic states are more likely to initiate cyberattacks than authoritarian states.

Research Design: Statistical Analysis

To test our hypotheses, we include data on 143 countries from 2005-12 (all data that is available) in our statistical analysis of the relationship among state power, regime type, and the initiation of cyberattacks. The cyberattack data are taken from the Council on Foreign Relations (CFR) Cyber Operations Tracker Dataset (COTD),^[37] and includes data on cyberattacks that occurred during that time. The state-sponsored cyber activities included are as follows: “The data exclusively tracks incidents and threat actors engaged in denial-of-service attacks, espionage, defacement, destruction of data, sabotage, and doxing.”^[38] One limitation in the dataset, which exists in all cyberconflict datasets, is not all cyberattacks that occurred during the time period are included due to limited information as to the full universe of cyberattacks that transpired during the time span. Thus, the attacks included in the CFR COTD pertain to verified attacks where information was largely known regarding both the attacker and the targeted victim states. The primary dependent variable from the CFR COTD we generate is the measure Cyberattack Count. The Cyberattack count variable captures the number of cyberattacks initiated by a given state for the year observed.

State Power

To measure the level of power for each state we use the Composite Index of National Capabilities (CINC) measure taken from the Correlates of War Dataset,^[39] which is one of the most widely used measures of state power in international relations.^[40] The CINC score gauges the level of power each state has relative to all other states, and is generated by calculating a state’s total score based on six core components: iron and steel production (thousands of tons), military expenditures, military personnel, energy consumption, total population (thousands) and urban population. CINC score increases for any state indicates an increase in power relative to all other states, and is measured on a continuous 0 to 1 scale.^[41]

Regime Type

The primary measure we use to assess whether a state is democratic or authoritarian is the widely recognized Polity2 measure for the Polity IV Database.^[42] The Polity2 measure is widely used in international relations and is considered to be a valid and reliable measure of regime type.^[43] The Polity2 measure captures the level of democracy or authoritarianism within states and ranges from -10 to 10. Higher values indicate a state is more democratic. Lower values indicate a state is more authoritarian. Political rights and civil liberties are two additional variables that are related to regime type included in our analysis. Political rights and civil liberties capture different aspects of the nature of governance within states that differ from what Polity2 measures. We use the political rights and civil liberties measures from the Freedom House

database to capture the extent that political rights and civil liberties of each states.^[44] Political rights measure one's freedom to participate in the political process by voting for elected leaders in free and fair elections, running for political office, and joining political organizations. The political rights measure is coded on an ordinal seven-point scale. The higher to value (here, 7) the lower political rights, with (1) depicting the widest possible range of political rights. The civil liberties measure gages one's right to openly express political beliefs, or belong to political and civil organizations, or have personal privacy and autonomy protected, and the rule of law. The civil liberties measure is coded on the same ordinal seven-point scale described above, with the lower value being the greatest civil liberties. The highest value (7) indicates a state has few or no civil liberties, and (1) indicates a state enjoys a wide range of civil liberties. Thus, higher values equate to a state having fewer civil liberties.

Control Variables

Our statistical analysis includes the variables discussed above, along with a number of other variables traditionally used to explain conflict initiation in order to attempt to identify those factors more closely associated with initiation of cyberattacks. These measures include economic variables that past studies often link to conflict (Inflation and Trade).^[45] To control for the effects of any potential ongoing conflicts on the initiation of cyberattacks we also include another standard measure in conflict/terrorism literature, i.e., the number of battlefield deaths within a state for any given year, both military and civilian. The data for the three variables (Inflation, Trade, Battlefield Deaths) are from the World Development Indicators.^[46]

Estimation Procedure

We conducted a cross-national time series analysis that examines how our economic and political variables influence the initiation of state-sponsored cyberattacks. For our primary measure, Cyberattack Count, we employ a random effect, time-series regression with a lagged dependent variable to control for autocorrelation. We used this estimation procedure based on the nature of our data, and since we are interested in the between-state variation in our sample. Our unit of analysis is state year.

Results

Table 1 (Model 1) displays the results that includes Cyberattack Count as the dependent variable. The CINC measure proved to have a positive and statistically significant relationship with the Cyberattack Count dependent variable.^[47] Thus, an increase in CINC score corresponds to a statistically significant greater number of cyberattacks. None of the other remaining political and economic variables reflected statistical significance in our models. Thus, state power appears to be the most influential factor regarding cyberattack initiation.

When examining the real-world implications of state power (CINC Score) on the number of cyberattacks initiated by states it is important to examine the predictive margins pertaining to state power's effect on cyberattack initiation. The predictive margins indicate the effects changes in the primary independent variable (CINC Score) have on the dependent variable when all other variables are held constant at their mean values. In Table 2 (Model 2), and Figure (1), we observe the expected number of initiated cyberattacks based on changes in levels of relative power as the CINC measure increases in increments of .10 (i.e., an increase in 10% relative power). When analyzing the predictive margins, we observe that when the CINC score is at the minimum level of relative power (0) the expected number of cyberattacks initiated is .0025, and when the CINC Score is at the maximum level of relative power (1) the expected number of cyberattacks initiated is 7.37. Thus, as the percentage of relative power increases states initiate a greater number of cyberattacks, and the increase is statistically significant. We now turn to discussing the findings in our descriptive analysis.

Table 1: DV
Number of Initiated Cyber Attacks

Variables	Model 1 DV: Cyber Attack Count
CINC	7.264 (0.538)***
Polity2	0.000 (0.003)
Political Rights	0.012 (0.014)
Civil Liberties	0.002 (0.014)
Inflation	-0.000 (0.000)
Trade	0.000 (0.000)
Battlefield Deaths	-0.000 (0.000)
Lagged DV	0.641 (0.026)***
Observations	944
r2	.9497
Prob. > X2	.0000**

*p <.10; **p<.05; ***p<.01; standard errors in parentheses.

Table 2: Predictive Margins
Expected Number of Initiated Cyber Attacks

Independent Variable CINC ScorDV: Cyber Attack Count	Model 2 DV: Cyber Attack Count
.0	.0032 (.0092)
.1	.7296 (.0508)***
.2	1.4560 (.1042)***
.3	2.1824 (.1579)***
.4	2.9088 (.2116)***
.5	3.6352 (.2653)***
.6	4.3616 (.3191)***
.7	5.0881 (.3728)***
.8	5.8145 (.4266)***
.9	6.5409 (.4803)***
1	7.2673 (.5341)***
N	944

$p < .10$; ** $p < .05$; *** $p < .01$; standard errors in parentheses

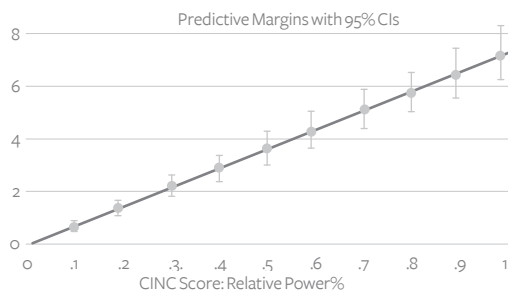


Figure 1: Expected Number of Initiated Cyberattacks

Descriptive Analysis

The descriptive analysis seeks to better understand those factors that affect a state's propensity to cyberattack when considered in the context of the political, economic, and military aspects of the respective attacking and targeted states.^[48] This descriptive analysis complements our statistical analysis and includes data on known cyber incidents taken from the CFR COTD from 2005-16 that meet the same criteria used for the statistical analysis. The dataset records

include both cyber attacker and cyberattacked states, and these two categories may not be equal given the multiple players in many of these events. The descriptive analysis includes a total of 102 states.^[49] The factors we examine are similar to the factors mentioned in our statistical analysis (State Power and Regime Type) along with State Wealth (Gross Domestic Product: GDP) and two additional conflict measures. We include the two additional measures (Dyadic Conflict and Monadic Conflict) to assess if cyberconflict-involved states are simultaneously involved in traditional forms of military conflicts. We first code whether such Dyadic Conflict refers to states engaged in a crisis/conflict with their cyberconflict counterpart. Monadic Conflict refers to when cyberconflict-involved states are also involved in any other international crises/conflicts. A crisis/conflict includes any event that “leads decision-makers to perceive a threat to basic values, time pressure for response and heightened probability of involvement in military hostilities.”^[50] The data on military crises/disputes and conflicts were collected from the International Crisis Behavior (ICB) dataset.

Descriptive Results

Several trends emerge when examining the findings from the descriptive analysis. Table 3 of the descriptive results confirms that relative power is a key factor that influences initiation of cyberattacks. The average CINC score for attacking states is .0434, and the average CINC score of targeted states is .0209. Thus, on average, attacking states have twice the amount of relative power than targeted states. In addition, the GDP for attacking states averages 20% higher than that of the targeted state. Attacking states thus generally have greater overall levels of both military and economic power. We conduct a two-sample t-test comparing the mean values of attacking states and targeted states for the relative power measures (CINC and GDP) and in each test the mean values were statistically different at the 99% level.

Table 3: Descriptive Measures

Variables	Mean	Standard Dev.	Minimum	Maximum	Observations
CINC Attacker	.0437295	.0802805	0	.2181166	188
CINC Target	.0209757	.0469934	0	.185799	155
Polity2 Attacker	-2.760638	5.530774	-10	10	188
Polity2 Target	4.877248	4.847779	-10	10	155
Political Rights Attacker	4.710106	2.964542	0	7	188
Political Rights Target	1.909962	1.804903	0	7	155
Civil Liberties Attacker	4.329787	2.736711	0	7	188
Civil Liberties Target	1.901613	1.710458	0	7	155
GDP Attacker	3.86e+12	4.47e+12	0	1.86e+13	188
GDP Target	7.88e+11	1.60e+12	0	9.28e+12	155

Regime type also influences a state's propensity to initiate cyberattacks. Table 3 displays the average Polity2 score of attacking states as -2.7, and 4.8 as the average for targeted states, leaving an average delta of 7.5. The average political rights score for attacking states is 4.71, and 1.9 for targeted states. Similarly, the average civil rights score for attacking states is 4.32 versus 1.90 for targeted states. These findings thus indicate that attacking states have lower overall levels of political rights and civil liberties than targeted states. Further, the Polity2 measure indicates that attacking states are generally more authoritarian than targeted states. Also, we conduct a two-sample t-test comparing the mean values of attacking states and targeted states for the regime type variables (Polity2, Political Rights, and Civil Liberties) and in each test the mean values were statistically different at the 99% level.

Lastly, as to the Dyadic Conflict measure, in 8.17% of cases the attacking state was involved in a crises/conflict with the cyber targeted state(s). In 7.69% of the cases the targeted state was involved in a crisis/conflict with the specific state that it was targeted by in the cyberattack.^[51] The Monadic Conflict measure confirmed that the attacking state was involved 16.35% of the time in at least one military crises/conflict with another state when it cyberattacked. Conversely, the targeted state was involved in at least one military crises/conflict with another state in 25.73% of cases when the cyberattack occurred. We conducted a two-sample t-test comparing the mean value of the Monadic Conflict variable for attacking states and targeted states and the results were statistically insignificant. Thus, the difference in mean values for the monadic conflict variable for attacking states and targeted states were not statistically significant.

In summary, in reviewing our descriptive analysis results, relative power, state wealth, and lower levels of democracy appear to increase the propensity to initiate state-sponsored cyberattacks. Cyber aggressors are more likely to have greater levels of power, both militarily and economically, be less democratic, and have weaker political rights and civil liberties. It also appears cyberattacks coincide with military crisis/conflict only in 7%-8% of our cases.

Overall, while regime type (i.e., overall levels of democracy, political rights, and civil liberties) is a factor in a state's propensity to initiate or be targeted by cyberattacks, these political variables are statistically insignificant. Thus, while regime type may be associated with the initiation of cyberattacks (i.e., authoritarian states are more likely to initiate cyberattacks), this effect is not pronounced enough in our sample to have a meaningful effect in our statistical analysis. Rather, state power is the predominant factor that influences cyberaggression in both our statistical analysis and descriptive results. More powerful states are more likely to initiate cyberattacks. These results track findings by scholars that states with greater power initiate more military conflicts than their less powerful counterparts.^[52] As with traditional forms of military conflict, power appears to play an important role in influencing state behavior in the cyber realm.

CONCLUSION

This article has considered the relative significance (and insignificance) of a number of factors and their impact on a state's propensity to engage in cyberattacks. We conclude that more powerful and authoritarian states are most likely to initiate cyberattacks. Regime type and state power (both military and economic) are associated with the initiation of cyberattacks. Our statistical analysis also confirms the notion that state power is associated with cyberattack initiation. Here we find that states are more likely to initiate cyberattacks as their relative power increases in the international system. As is true with kinetic military operations, our study confirms that more powerful states are more prone to initiate cyberattacks. Furthermore, in both the statistical analysis and descriptive results, greater power disparity significantly increases the odds of an attack by the stronger on the weaker. These findings further track what we know not only about relative military power but relative economic power as well as it relates to foreign policy behavior.

While this study is a first attempt to examine the factors associated with the initiation of state-sponsored cyberattacks cross-nationally, there is much room for further exploration. For example, which factors influence the severity of cyberattacks, and what is the impact of relative technological sophistication of both attacking and targeted states? Currently, comparative data on the cross-national measures of cyber capabilities of states, is uncharted territory. As this data becomes available, these variables should also be evaluated insofar as how they are influencing cyber conflict. Future research should also analyze what (other than raw power) motivates cyberattacks and why states choose cyberattacks over other alternatives, and how regime type and governance impact this decision, as our descriptive results suggest. This article hopefully has opened the door; more research is now needed to determine precisely how regime type affects cyberconflict.🔒

NOTES

1. P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar* (New York: Oxford, 2014).
2. Gil Press, "60 Cybersecurity Predictions for 2018" *Forbes*, November 26, 2017, <https://www.forbes.com/sites/gilpress/2017/11/26/60-cybersecurity-predictions-for-2018/#7087bb4073ff>.
3. Singer and Friedman, *Cybersecurity and Cyberwar*, 4.
4. Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," *International Security* 38, no. 2 (2013): 26.
5. Palmer and Morgan, *A Theory of Foreign Policy*.
6. Ragnhild Endresen Siedler, "Hard Power in Cyberspace: CNA as a Political Means," 2016 8th *International Conference on Cyber Conflict (Cycon): Cyber Power*, ed., N. Pissanidis, H. Rõigas, and M. Veenendaal, 23-36, (Tallinn: NATO CCDCOE Publications, 2016), 26.
7. Siedler, "Hard Power in Cyberspace."
8. Ibid.
9. Ibid.
10. Jon R. Lindsay and Lucas Kello, "Correspondence: A Cyber Disagreement," *International Security* 39, no. 2 (2014): 29.
11. Daniel Hughes and Andrew M. Colarik, "Predicting the Proliferation of Cyber Weapons into Small States," *Joint Force Quarterly* 83, no. 4, 21.
12. Siedler, "Hard Power in Cyberspace."
13. Adam P. Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War." *Journal of Strategic Studies* 35, no. 3 (2012): 401-428.
14. Brian M. Mazanec, *The Evolution of Cyber War: International Norms for Emerging-Weapons Technology* (Lincoln, NE: Potomac Books, 2015).
15. Siedler 2016; Fred Kaplan, *Dark Territory - The Secret History of Cyber War* (New York: Simon & Schuster, 2016).
16. Thomas Rid, *Cyber War Will Not Take Place* (New York: Oxford University Press, 2016).
17. P.W. Singer and Emerson T. Brooking, *LikeWar: The Weaponization of Social Media*. (New York: Houghton Mifflin Harcourt, 2018).
18. Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies* 24 (2015): 335.
19. David C. Gompert and Phillip C. Saunders, *The Paradox of Power: Sino-American Strategic Restraint in an Age of Vulnerability* (Washington, D.C.: National Defense University Press, 2011).
20. Bruce M. Russett, *Grasping the Democratic Peace: Principles for a Post-Cold War World* (Princeton: Princeton University Press, 1993).
21. Bruce Bueno de Mesquita and Randolph Siverson, "War and the Survival of Political Leaders: A Comparative Study of Regime Types and Political Accountability," *American Political Science Review* 89, no. 4 (1995).
22. Steve Chan, "Mirror, Mirror on the Wall ...Are the Freer Countries More Pacific?" *Journal of Conflict Resolution* 28, no. 4 (1984).
23. Dan Reiter and Erik Tillman, "Public, Legislative, and Executive Constraints on the Democratic Initiation of Conflict," *Journal of Politics* 64 no. 3 (2002).
24. Darren Filson and Suzanne Werner, "Bargaining and Fighting: The Impact of Regime Type of War Onset, Duration and Outcomes," *American Journal of Political Science* 48, no. 2 (2004).
25. Rebecca MacKinnon, "Liberation Technology: China's 'Networked Authoritarianism'," *Journal of Democracy* 22, no. 2 (2011).
26. MacKinnon, "Liberation Technology: China's 'Networked Authoritarianism'," 33.
27. Ibid., 44.
28. Ron Deibert and Rafale Rohozinski. (2010), "Control and Subversion in Russian Cyberspace.," In Ronald Deibert, John Palfrey, Rafel Rohozinski, Jonathan Zittrain, and Miklos Haraszti (eds), *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (Cambridge: MIT Press), 15-34.
29. Ron Deibert and Rafale Rohozinski, "Liberation vs. Control: The Future of Cyberspace," *Journal of Democracy*, 21, no. 4 (2010): 50.

NOTES

30. Ron Deibert, "Authoritarianism Goes Global: Cyberspace Under Siege," *Journal of Democracy*, 26, no. 3 (2015): 65.
31. Deibert, "Authoritarianism Goes Global," 65.
32. Ibid., 68.
33. Ibid., 68.
34. Jan Kallberg, "Strategic Cyberwar Theory-A Foundation for Designing Decisive Strategic Cyber Operations," *The Cyber Defense Review* 1, no. 1 (2016): 114.
35. Kallberg, "Strategic Cyberwar Theory", 114.
36. Ibid., 116.
37. Council on Foreign Relations, "Cyber Operations Tracker Dataset" (2018), <https://www.cfr.org/interactive/cyber-operations>, May 11, 2019.
38. See the (CFR 2018) Dataset for more information regarding the data collection methodology.
39. David J. Singer, Stuart Bremer, and John Stuckey (1972), "Capability Distribution, Uncertainty, and Major Power War, 1820-1965;" In Bruce Russett (ed) *Peace, War, and Numbers*, Beverly Hills: Sage, 19-48.
40. Halvard Buhaug, "Dude, Where's My Conflict? LSG, Relative Strength, and the Location of Civil War," *Conflict Management and Peace Science* 27, no. 2 (2010):107-128.
41. J. David Singer, Stuart Bremer, and John Stuckey, "Capability Distribution, Uncertainty, and Major Power War, 1820-1965;" In *Peace, War, and Numbers*, ed. Bruce Russett (Beverly Hills: Sage, 1972).
42. Polity IV Project, *Polity IV data set* (College Park, MD: University of Maryland, Center for International Development and Conflict Management, 2014).
43. Todd L. Allee and Paul K. Huth, "Legitimizing Dispute Settlement: International Legal Rulings as Domestic Political Cover," *American Political Science Review* 100, no. 2 (2006).
44. Freedom House (2014) "About Freedom in the World: An annual study of political rights and civil liberties."
45. The trade variable measures trade as a percentage of annual GDP for each state. The inflation variable captures the percentage of inflation for each state for each year.
46. World Development Indicators (WDI 2014).
47. For more on hypothesis testing please see David F. Groebner, Patrick W Shannon, and Phillip C. Fry, "Business Statistics," 9th Edition, Chapter 7 (London: Pearson, 2013).
48. The variation in the years included in the statistical analysis and descriptive analysis is due to the variation in the years covered (i.e., data availability) for the variables required for the statistical analysis.
49. Only states involved in cyber incidents are included in the descriptive analysis.
50. Michael Brecher and Jonathan Wilkenfeld, *A Study of Crisis* (Ann Arbor, MI: University of Michigan Press, 2000); Michael Brecher et al., *International Crisis Behavior Data Codebook*, Version 12 (2017, 4).
51. Percentages vary for the dyadic conflict measure for attacking and targeted states due to the unequal number of attacking versus targeted states in the sample.
52. Palmer and Morgan, *A Theory of Foreign Policy*.

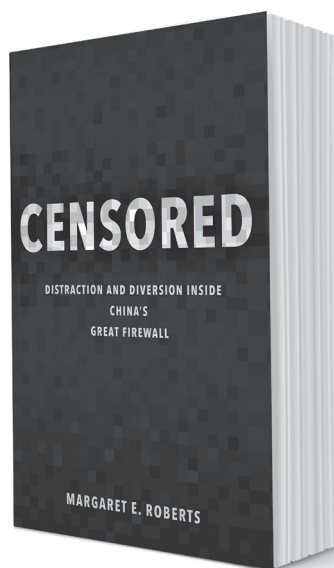
THE CYBER DEFENSE REVIEW

◆ BOOK REVIEW ◆

Censored: Distraction and Diversion Inside China's Great Firewall

By Margaret E. Roberts

Reviewed by Cadet Tommy Hall



EXECUTIVE SUMMARY

This review discusses the content and implications of Margaret E. Roberts' book, *Censored: Distraction and Diversion Inside China's Great Firewall*, (Princeton University Press, April 2018), beginning with the author's background, and followed with a by-chapter breakdown and conclusion. This review also evaluates Roberts' ability to deconstruct false assumptions about authoritarian censorship in the digital age. While information is more widespread and accessible now than ever, it also comes with greater vulnerability to the weaponization of disinformation in the cyber domain. Although some of China's dystopian cyber censorship follow conventional wisdom while other features are radically different from conventional wisdom. Liberal democracy advocates must brace for China's integrated model of "porous censorship" to rapidly proliferate.

REVIEW

Margaret Roberts is best known for her contributions to "How Censorship in China Allows Government Criticism but Silences Collective Expression," co-authored with Gary King and Jennifer Pan, and published in the *American Political Science Review* in 2013. Their study found that China's government is no more likely than other authoritarian governments to censor vitriolic criticism from citizens on the web. Censorship in China instead focuses on forestalling collective action. In *Censored: Distraction and Diversion Inside China's Great Firewall*, Roberts expands upon her previous research, shedding new light on the Chinese Communist Party's (CCP's) censorship strategy.

This is a work of the U.S. Government and is not subject to copyright protection in the United States. Foreign copyrights may apply.



Tommy Hall, a 3rd year Cadet at the United States Military Academy focuses his research on China, including historical conceptions of nationalism, environmental policy, and contemporary US-China relations. His other research interests include writing pedagogy, specifically about access and equity within college writing centers. As a Stamps Scholar and a Chinese language major, Cadet Hall hopes to promote cross-cultural understanding between the citizens of the United States and China in an era of renewed great power competition.

Censored: Distraction and Diversion Inside China's Great Firewall is composed of eight chapters, including an introduction and an appendix. Roberts' intended audience includes all who have a general interest in digital policy, authoritarianism, or Chinese domestic affairs. Her writing is clear and descriptive, allowing non-technical readers to quickly grasp her key concepts and experiments. The introduction guides the reader through the basics of China's "porous censorship" model, breaks down the CCP methods used to distract and divert its population from accessing information the government sees as a threat, identifies how the CCP's methods depart from the conventional wisdom on the nature of censorship in modern authoritarian regimes, and finally, outlines a roadmap for the rest of her book. Subsequent chapters cover a theoretical breakdown of government censorship itself, the evolution of censorship in China's modern history, Chinese citizens' reactions to censorship, the key concepts of "information friction" and "information flooding," and the implications of censorship in the digital landscape for authoritarian and democratic regimes. Roberts concludes with a call to action, highlighting areas and topics for future research.

Critical to Roberts' case study is her observation that Chinese digital censorship is porous, not airtight. Nor is China's Great Firewall an impenetrable digital barrier. Instead, it is routinely jumped or avoided by technologies and user practices, like VPNs or simply waiting longer than usual for censored websites to load. With a little extra time or money, any Chinese citizen can access censored material with few if any consequences. Due to the rapid proliferation and mass availability of information in the Internet Age, the days of authoritarian governments trying to monopolize information flow are long gone. Complete control of information is costly and risky for the CCP to implement at scale. When the greater public discovers an instance of state censorship, the backlash is swift and sometimes too much for

an authoritarian regime to bear. For example, Roberts explains that the discovery of censorship can create anger and reduce public trust in government institutions. Compounded with the economic inefficiency censorship creates, Roberts explains that the potential for unrest and the erosion of regime legitimacy are severe consequences that authoritarian governments must consider before censoring information.

Although Roberts labels Chapter 2 as an overview of censorship theory, this chapter does more, describing each critical concept in-depth and explaining its theoretical underpinnings to establish a roadmap for the key concepts she expands upon in later chapters. She explains that:

1. The CCP has an advanced understanding that most citizens are rationally ignorant about consuming political information. Why enact a blanket application of risky, fear-based censorship tactics when citizens can be routed away from behavior that threatens an authoritarian regime's survival through a small tax on information?
2. Instead of exploiting fear, the CCP more often uses the censorship mechanisms of friction and flooding, which Roberts defines in Chapters 5 and 6. Understanding why friction and flooding work better for the CCP than fear alone requires an understanding as to why China customizes its censorship.
3. Following this logic, Roberts identifies two types of citizens: 1) the masses—citizens who have little interest in politics; and 2) the politically elite—well-educated citizens who desire to become informed about and participate in politics. Roberts shows how, through information friction and flooding, the masses can be easily sedated. A more targeted approach of fear-based mechanisms can then be discreetly enacted with brutal efficiency on members of the elite political class—those citizens most likely to engage in collective action.

Chapters 3 and 4 display Roberts' mastery of multiple disciplines: Chapter 3 offers an impressively researched history, detailing the evolution of censorship in the People's Republic of China, and Chapter 4 rigorously analyzes the methodology Roberts used to carry out her experiments to gauge how China's netizens react to digital censorship. Chapter 4 also identifies several costs authoritarian regimes incur when they enact censorship measures, including the potential to create anger, decrease trust, increase economic inefficiencies, and undermine the government's ability to collect information from the public. Roberts notes that, as the Internet becomes increasingly accessible, censorship costs become more likely and more taxing because, now more than ever, people can express their voices directly to the public via social media platforms and are thus more likely to experience government censorship in a direct and personal manner.

Chapters 5 and 6 define the two mechanisms critical to understanding China's porous censorship strategy: friction and flooding. According to Roberts, information friction deters individuals from accessing threatening information. Google, which is legal in China, provides a

prime example. When the CCP orders Google to be throttled by purposefully slowing search results, the extra load time is enough to divert netizens to alternative search engines, like Baidu. Search filtering, keyword blocking, and denial of service attacks are other common examples of information friction. Information flooding promotes information that aligns with the government's preferred narrative. Flooding is often coordinated and intends to distract the public or compete with other types of information more harmful to the CCP's agenda.

Roberts explains how the digital world has made this form of censorship much less costly to produce. There are two common types of flooding: flooding information directly to the public and flooding the media. When a hashtag, originally intended to criticize a government policy, is applied to pro-government propaganda or irrelevant content, the hashtag is flooded with pro-government sites, comments, and information, burying the negative, anti-government criticism. Another example of flooding is when controversial news stories are pushed deeper into pages of media or Internet search results by pro-government or irrelevant content. Both information friction and flooding allow the CCP to retain plausible deniability. In an age of more access to information than people can consume, small inconveniences and delays often suffice to steer a consumer away from information the CCP does not want them to access.

To summarize, Roberts leaves us with critical implications and areas for future research. Roberts fears a world in which enormous data-collection programs and surveillance are paired, creating personalized friction and flooding. In her discussion of the impact on free speech in democracies, she concludes that "digital media has made the contrast between democracies and autocracies less stark" and argues that democratic countries should look at information prioritization and the algorithms that control what consumers see in their personal news feeds.

CONCLUSION

Censored: Distraction and Diversion Inside China's Great Firewall provides a nuanced explanation of the theory and mechanisms of China's porous censorship and raises important questions for democracies to address in avoiding self-inflicted cyber censorship. This book will greatly benefit readers seeking to understand the specific mechanisms behind the most pervasive digital censorship experiment in modern history. For those with a background in China studies, Roberts' book provides a meticulously detailed description of how digital censorship intersects with China's domestic politics, media, and popular opinion. Readers with highly technical backgrounds should find her efforts to quantify a citizens' probability of speaking out against censorship fascinating. Roberts details her methodology and experimental design before stating her conclusions, allowing readers to draw their conclusions from her findings. Roberts' biggest strength is her ability to capitalize on a mixed-methods approach that qualitatively assesses the history and offers a theory, while quantitatively breaking new ground with innovative and complex empirical work.

While China-focused, a secondary theme of the book is how China's porous censorship relates to the absence of any US cyber policy that would prevent tech corporations and government bureaucracies from adopting similar authoritarian practices. The US today is extremely polarized politically. Flooding techniques, specifically, could drain democratic efficiency. The past two presidential elections confirm that US adversaries are willing to employ coordinated efforts across social media and the Internet to exacerbate political tensions in the US. Burma provides an example, where the military dictatorship has now adopted China's digital censorship playbook, down to friction and flooding techniques that divide the public, deter political organization, and wreak havoc on free expression.

Ultimately, *Censored: Distraction and Diversion Inside China's Great Firewall* is an excellent resource for all seeking to better understand how digital censorship is applied in an age of authoritarian resurgence, and also, how similar mechanisms of digital censorship may emerge in democratic nations. Roberts neatly contextualizes each of her arguments and returns to important points to underscore for her readers the key takeaways. Although packed to the brim with information, Roberts lays her book out in an easily digestible fashion.

Censored: Distraction and Diversion Inside China's Great Firewall is a critical piece to read to understand the fundamental challenges defining 21st Century information warfare. We live in an era when, by merely logging onto a computer, we step onto the battlefield of the future. As with every fight, most often the victors are those with better intelligence and better understanding of how to apply it. Roberts very skillfully explores a pivotal case study in information warfare, and much more work is needed to apply her theories so as to improve the digital information landscape of democracies.♥

Title: ***Censored: Distraction and Diversion Inside China's Great Firewall***

Author: Margaret E. Roberts

Publisher: Princeton University Press; Reprint edition (April 10, 2018)

eBook: 281 pages

Language: English

Price: \$9.99 (eBook)

ISBN: 0691204004

THE CYBER DEFENSE REVIEW


CONTINUE THE CONVERSATION ONLINE

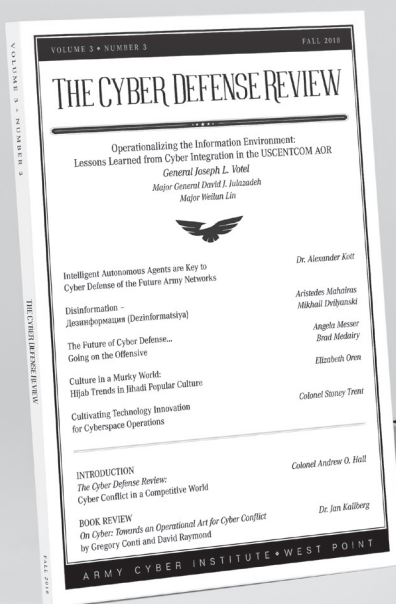
 CyberDefenseReview.Army.mil

AND THROUGH SOCIAL MEDIA

 Facebook [@ArmyCyberInstitute](https://www.facebook.com/ArmyCyberInstitute)

 LinkedIn [@LinkedInGroup](https://www.linkedin.com/company/ArmyCyberInstitute)

 Twitter [@ArmyCyberInst](https://twitter.com/ArmyCyberInst)
[@CyberDefReview](https://twitter.com/CyberDefReview)



ARMY CYBER INSTITUTE ♦ WEST POINT



THE ARMY CYBER INSTITUTE IS A NATIONAL RESOURCE FOR RESEARCH, ADVICE AND EDUCATION IN THE CYBER DOMAIN, ENGAGING ARMY, GOVERNMENT, ACADEMIC AND INDUSTRIAL CYBER COMMUNITIES TO BUILD INTELLECTUAL CAPITAL AND EXPAND THE KNOWLEDGE BASE FOR THE PURPOSE OF ENABLING EFFECTIVE ARMY CYBER DEFENSE AND CYBER OPERATIONS.