VOLUME 7 ◆ NUMBER 4 FALL 2022

THE CYBER DEFENSE REVIEW

Better Anticipating and Managing Today's Growing Cyber Risks
Dr. Daniel Gerstein

Russian Cyber Operations in the Invasion of Ukraine
Dr. Herbert Lin

Tactics and Technicalities Undermining Strategy: Cyber Security is Distracting National Security Communities
Brig. Gen. Martin White

Cyber-Physical Coordinated Attacks:
The Emerging Complexity of Crisis Management
John Checco

The Impending Data Literacy Crisis Among Military Leaders
Lt. Col. Andrew G. Farina

How China's Cyber Operations During the COVID-19 Pandemic Worsened the United States Biodefense and National Security
Lt. Col. Regan F. Lyon

A Military of Influencers: The U.S. Army, Social Media, and Winning Narrative Conflicts
Josh Rutland and Lt. Col. Robert J. Ross

Deterrence Thru Transparent Offensive Cyber Persistence
Lt. Col. Ryan Tate and Col. Chad Bates

Everything Flows: Russian Information Warfare Forms and Tactics in Ukraine and the US Between 2014 and 2020
Samantha Mullaney

INTRODUCTION
The Only Constant is Change... *Col. Jeffrey M. Erickson*

BOOK REVIEW
Cyberspace in Peace and War, 2nd Edition
by Martin C. Libicki *Dr. Mark Grzegorzewski*

ARMY CYBER INSTITUTE ◆ WEST POINT PRESS

The Cyber Defense Review

◆ Fall Edition ◆

THE CYBER DEFENSE REVIEW

A DYNAMIC MULTIDISCIPLINARY DIALOGUE

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.

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.

THE CYBER DEFENSE REVIEW VOL. 7 ◆ NO. 4 ◆ FALL 2022

INTRODUCTION

Col. Jeffrey M. Erickson 9 The Only Constant is Change...

SENIOR LEADER PERSPECTIVE

Dr. Daniel Gerstein 15 Better Anticipating and Managing Today's Growing Cyber Risks

Dr. Herbert Lin 31 Russian Cyber Operations in the Invasion of Ukraine

Brig. Gen. Martin White 47 Tactics and Technicalities Undermining Strategy: Cyber Security is Distracting National Security Communities

PROFESSIONAL COMMENTARY

John Checco 69 Cyber-Physical Coordinated Attacks: The Emerging Complexity of Crisis Management

Lt. Col. Andrew G. Farina 91 The Impending Data Literacy Crisis Among Military Leaders

Maj. Y. Brian Lee, Maj. Dennis Kim, Maj. Wallace Rollins 99 Contract AI Risk Engine (CARE) to Reduce Cyber Contracting Risk

Col. (Ret.) Jeffrey Voice 109 Leveraging the Operational Cyber Mission Stack (OCMS)

RESEARCH ARTICLES

Bart Hogeveen 123 The UN Cyber Norms: How Do TheyGuide the Responsible Development and Use of Offensive Cyber Capabilities?

Alfred D. Hull, Dr. Jim Kyung-Soo Liew, Kristian T. Palaoro, Dr. Mark Grzegorzewski, Dr. Michael Klipstein, Dr. Pablo Breuer, Dr. Michael Spencer 143 Why the United States Must Win the Artificial Intelligence (AI) Race

RESEARCH ARTICLES

Lt. Col. Regan F. Lyon	159	How China's Cyber Operations During the COVID-19 Pandemic Worsened the United States Biodefense and National Security
Lt. Cmdr. Michael McLaughlin	175	Seventh Service: Proposal for the United States Cyber Force
Samantha Mullaney	193	Everything Flows: Russian Information Warfare Forms and Tactics in Ukraine and the US Between 2014 and 2020
Josh Rutland **Lt. Col. Robert J. Ross, Ph.D.**	213	A Military of Influencers: The U.S. Army, Social Media, and Winning Narrative Conflicts
Lt. Col. Ryan Tate **Col. Chad Bates**	227	Deterrence Thru Transparent Offensive Cyber Persistence
2nd Lt. Joseph Zuccarelli **2nd Lt. Nico Manzonelli**	247	Ethical Assessment of Russian Election Interference Using the Framework of Just Information Warfare

RESEARCH NOTE

Andrew Luzzatto	261	Regulating Cyber Warfare through the United Nations

BOOK REVIEW

Dr. Mark Grzegorzewski	273	*Cyberspace in Peace and War*, 2nd Edition By Martin C. Libicki

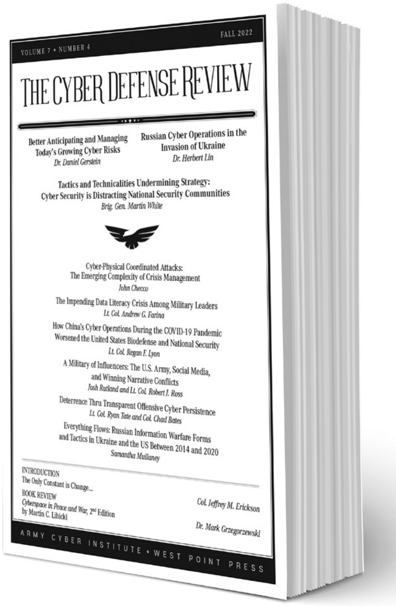
The Cyber Defense Review

Introduction

VOL. 7 ◇ NO. 4

The Only Constant is Change...

Colonel Jeffrey M. Erickson



VOLUME 7 • NUMBER 4

FALL 2022

THE CYBER DEFENSE REVIEW

Better Anticipating and Managing Today's Growing Cyber Risks
Dr. Daniel Gerstein

Russian Cyber Operations in the Invasion of Ukraine
Dr. Herbert Lin

Tactics and Technicalities Undermining Strategy: Cyber Security is Distracting National Security Communities
Brig. Gen. Martin White

Cyber-Physical Coordinated Attacks: The Emerging Complexity of Crisis Management
John Checco

The Impending Data Literacy Crisis Among Military Leaders
Lt. Col. Andrew G. Farina

How China's Cyber Operations During the COVID-19 Pandemic Worsened the United States Biodefense and National Security
Lt. Col. Regan F. Lyon

A Military of Influencers: The U.S. Army, Social Media, and Winning Narrative Conflicts
Josh Rutland and Lt. Col. Robert J. Ross

Deterrence Thru Transparent Offensive Cyber Persistence
Lt. Col. Ryan Tate and Col. Chad Bates

Everything Flows: Russian Information Warfare Forms and Tactics in Ukraine and the US Between 2014 and 2020
Samantha Mullaney

INTRODUCTION
The Only Constant is Change... *Col. Jeffrey M. Erickson*

BOOK REVIEW
Cyberspace in Peace and War, 2nd Edition by Martin C. Libicki *Dr. Mark Grzegorzewski*

ARMY CYBER INSTITUTE • WEST POINT PRESS

The ancient Greek philosopher Heraclitus is credited with the quote "The only constant in life is change." While Heraclitus was certainly not thinking of cyberspace or modern technologies, it occurs to me that he may have been onto something with respect to the larger world of cyber related issues as we have seen continual evolution since the founding of the Army Cyber Institute (ACI) at West Point.

This Fall marks ten years since the creation of the ACI by the Secretary of the Army, John McHugh, and the Chief of Staff of the Army, General Raymond Odierno, in 2012 to serve as "a national resource for research, advice, and education in the cyber domain, engaging military, government, academic, and industrial cyber communities in impactful partnerships to build intellectual capital and expand the knowledge base for the purpose of enabling effective Army cyber defense and cyber operations."

At the time, the Army was trying to figure out the best approach to address the uncertain environment and growing demand for a deeper understanding of the cyberspace environment, as well as its potential positive and negative impacts on the Army, the Department of Defense, and the Nation. In the past decade, the Army's Cyber Community has seen significant changes across many areas. Some of the highlights include:

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.

- The creation of the Cyber Branch in 2014, recognizing the necessity for a dedicated cadre of cyber experts for the Army, and marking the Army's the first new branch since the Special Forces was established in 1987
- The designation of Ft. Gordon from the Signal Center of Excellence to the Cyber Center of Excellence and the creation of the U.S. Army Cyber School in 2014
- ACI published the first issue of *The Cyber Defense Review* in 2016, the first DoD-sponsored cyber-focused journal
- The creation of the Army Futures Command in 2017 to develop future Army readiness
- U.S. Cyber Command's (USCYBERCOM) elevation to a unified combatant command in 2018
- The creation of the 915th Cyber Battalion in 2019 to provide an organic expeditionary capability to Army Cyber Command (ARCYBER)
- The move of ARCYBER from Fort Belvoir to Fort Gordon in 2020 to achieve synergy between the operational and institutional sides of the cyber force

These milestones were steps in the evolution of the Army Cyber Community towards greater capability, a more defined identity/culture, better integration from the tactical to the strategic levels, and a widespread recognition of the necessity for improved cyber capabilities.

A key component of these changes is the open and continuous dialogue and debate among operators, senior leaders, academics, industry leaders, and government officials in analyzing courses of action, making decisions, and implementing plans. The CDR authors continue to add to the dialogue and debate by presenting new and developing perspectives on the challenges of cyberspace.

I thank all our Fall authors for their invaluable contributions and would like to recognize a few for their focus on change:

- **What do leaders need to know to navigate the cyber domain?** LTC Andrew Farina's article ("The Impending Data Literacy Crisis Among Military Leaders") captures key points about leaders struggling to achieve data literacy in understand new technologies and paradigm shifts, in this case related to data literacy.
- **How should we organize to operate in cyber?** LCDR Michael McLaughlin advocates for the creation of a "Seventh Service" for the United States with authorities more akin to the Coast Guard and National Guard.
- **How do we adjust our approach?** In "Tactics and Technicalities Undermining Strategy," Australian Brigadier Martin White argues that the downfall of our current approaches is the focus on analyzing too much information, resulting in an overall weaker posture.
- **How do we change our enemy's perception?** LTC Ryan Tate and COL Chad Bates argue for increased deterrence by being more transparent with operations in their article "Deterrence Thru Transparent Offensive Cyber Persistence."

These authors argue for changes to the people, processes, and technologies we use to see ourselves, our adversaries, and the terrain in cyberspace. As the ACI begins its next decade, expect to see constant changes across the Cyber Force with CDR authors constantly seeking solutions to future problems.

The Cyber Defense Review

⋄ Senior Leader Perspective ⋄

Better Anticipating and Managing Today's Growing Cyber Risks

Daniel M. Gerstein

> Modern man emerged and began using language 1,400 generations ago. Writing was invented 200 generations ago. Books were first printed 20 generations ago. The invention of the computer occurred less than 2 generations ago.[1]

...And Then Came the Cyber Domain

We live in an increasing cyber enabled world where more of our lives are monitored, assessed, and controlled by forces and decisions that function largely in the background and with little appreciation for the risks that we assume as a result. Absent fundamental rethinking as to how we incorporate Information Age technologies into the fabric of our daily lives, we will increasingly find ourselves reaching a point of no return as more complex technologies such as AI and greater ubiquity of cyber technologies inherent in the Internet of Things (IoT) continue to proliferate in cyberspace. To manage these technologies, we still rely on organizations and processes rooted in the 18th century to confront threats that move across the globe in milliseconds. It is no wonder that we find ourselves in a defensive battle and in a position of great disadvantage.

In considering the current state of cybersecurity, we will do so in its broadest sense. We will consider the computers, networks, technology, and the various means employed for operating in the cyber domain. We will also consider the lower-level components of the Internet that form the basis of cyberspace– these include the computers and Internet of Things (IoT) devices that are an inherent part of the network, packet switching and Internet protocols, cloud computing and the various communications means that comprise the cyber domain and contribute to the increasing attack surface. In looking broadly, we

Dr. Daniel Gerstein, a 1980 West Point graduate, served as the Department of Homeland Security Undersecretary (acting) and Deputy Undersecretary in the Science and Technology Directorate from 2011-2014. He has extensive experience in security and defense and has served in uniform, industry, academia, think tanks and as a senior government civilian. He is currently an Adjunct Professor at American University in Washington, D.C. In uniform he served on four continents during combat, peacekeeping, humanitarian, counterterrorism and homeland security including standing up SOUTHCOM's Theater Network Operations and Security Center following 9/11. He served for more than a decade in the Pentagon in various high-level staff assignments, including having served on the Holbrooke Delegation that negotiated the peace settlement in Bosnia. He is a frequent national security contributor and has published numerous books and articles on national and homeland security issues. His latest book—*Tech Wars: Transforming U.S. Technology Development* (Praeger)—was published in September 2022.

will consider the effects on related technologies such as big data, blockchain, encryption, social media and AI. We will also consider how norms, regulations, and laws contribute to or detract from our cyber lives, and how these issues, within a whole-of-society context that ranges from international and national authorities to each and every citizen, will be affected by and in some cases become part of the cyber domain. As we ponder these concepts, considering effects on society in areas such as loss of privacy, human interactions in cyber space, and sensitive data such as security of personal identifiable information (PII) will also be important.

The purpose in looking so broadly is to understand the overall risks associated with this human created cyber domain. In doing so, we hope to better understand and mitigate such risks in the future.

Our approach to date for dealing with cyber risks has been largely reactive as we install intrusion detection systems and internal network monitoring capabilities to prevent intruders from penetrating our networks and look for anomalous behavior within our networks. At the 2022 DEF CON National Cyber Director Chris Inglis asserted this must change and highlighted that "defense is the new offense," and "the way forward for cybersecurity is defense."[2] With each cyber intrusion, ransomware event, theft of intellectual property or attack on critical infrastructure, we seek to understand how the attack occurred and implement specific changes in the form of software patches, calls for hardware refreshes for obsolete systems or incorporating new procedures to protect our cyber networks.[3]

Despite these efforts, evidence abounds that this approach is inadequate. In the first half of 2021, Accenture found a triple digit increase in cyber-attacks. They further identified five industries that comprised more than 60% of the intrusions, including consumer goods and services, industrial, banking, travel and hospitality and insurance. Not surprisingly, the top three nations targeted were the US, UK and Australia, and the top threats are ransomware and extortion.

We also have experienced cyber-attacks targeting critical infrastructure that caused serious property damage. Examples include:

- Saudi Aramco attack (2006)
- Attacks that targeted government facilities in Estonia (2007)
- Polish teenager remotely derailing trains (2008)
- Hacker tampering with a hospital ventilation system in a Texas hospital (2011)
- Yahoo cyber-attack that compromised one billion accounts (2013)
- Russian attack against the Ukrainian power grid (2015)
- WannaCry ransomware attack (2017)
- Saudi Arabia's oil refineries attacked (2017)
- JBS attack (2021)
- Colonial Pipeline attack (2021)

These represent only a small but highly visible subset of attacks.[4,5,6]

The continued increase in the number and variety of devices, users, applications, and data have resulted in growing attack surface problems, i.e., the number of points vulnerable to attack continues to grow. Issues are exacerbated by several intertwined and mutually reinforcing trends: the increasing number of IoT sensors and actuators on the network and associated volumes of retained data, evolving sophistication of global supply chains that rely on the Internet, the mass migration of resources to the cloud, and greater remote work activities (which accelerated in the COVID-19 era).[7]

In short, we have applied a serial approach to a massively parallel problem within a complex network, all further complicated by the fundamentals of the cyber domain. At its core, the Internet—the early instantiation of the cyber domain—was created as an information sharing platform with little regard for security. In fact, security was, and still often is, an afterthought or add on feature rather than a coequal part of the Internet. It is further complicated as some 85% of critical infrastructure, to include the Internet and associated infrastructure, reside in the private sector.[8] Even those parts of the cyber domain that are used by government traditionally have portions of their networks that reside in the broader cyber domain. For example, classified networks normally lease communications systems from Internet service providers and employ secure devices to provide security for their networks and data. We also know that a significant percentage of the cyber insecurities occur at the application layer, where human-computer interface occurs and the user operates—by one estimate, 95% of cyber security breaches are caused by human error.[9]

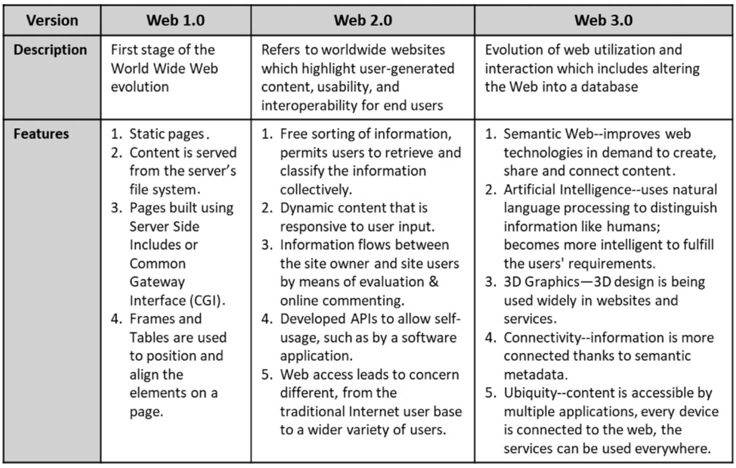
Understanding and Managing Future Cyber Risk

To better manage future cyber risks, we need to better understand them, which requires consideration of two different types of risks. The first are technology risks associated with the development of key cyber enabling technologies. The second set of risks are strategic and occur from lacking the necessary command and control relationships, planning and processes, or failing to take appropriate actions as required to prevent, protect, mitigate, respond, and recover from a cyber event.

The earlier introduction paints a bleak picture of several cyber threats that have materialized in the past and even provides a glimpse of likely future cyber risks. Yet increasing capabilities of Information Age technology could present even greater risks.

To understand how the cyber landscape could evolve, it helps to segment the Internet (and associated World Wide Web or www) into Web 1.0, Web 2.0, and Web 3.0, as described in Table 1 below.[10] Web 1.0 consisted of static pages. Advertisements were banned. Personal users hosted their own web pages on ISP-run websites. Web 2.0 is often called the "participative social web,"[11] which allows for "podcasting, blogging, tagging, curating with RSS, social bookmarking, social networking, social media, and web content voting."[12] It is both enabled by and a product of ubiquitous mobile communications that allow humans to maintain virtually constant contact with the World Wide Web. Web 3.0 would significantly increase Web 2.0 capabilities to allow for "web utilization and interaction, which includes altering the web into a database," thereby optimizing Web 3.0 for "machine conception as opposed to human understanding."[13]

Table 1. Web 1.0, Web 2.0, Web 3.0 Descriptions and Features.



Version	Web 1.0	Web 2.0	Web 3.0
Description	First stage of the World Wide Web evolution	Refers to worldwide websites which highlight user-generated content, usability, and interoperability for end users	Evolution of web utilization and interaction which includes altering the Web into a database
Features	1. Static pages. 2. Content is served from the server's file system. 3. Pages built using Server Side Includes or Common Gateway Interface (CGI). 4. Frames and Tables are used to position and align the elements on a page.	1. Free sorting of information, permits users to retrieve and classify the information collectively. 2. Dynamic content that is responsive to user input. 3. Information flows between the site owner and site users by means of evaluation & online commenting. 4. Developed APIs to allow self-usage, such as by a software application. 5. Web access leads to concern different, from the traditional Internet user base to a wider variety of users.	1. Semantic Web--improves web technologies in demand to create, share and connect content. 2. Artificial Intelligence--uses natural language processing to distinguish information like humans; becomes more intelligent to fulfill the users' requirements. 3. 3D Graphics—3D design is being used widely in websites and services. 4. Connectivity--information is more connected thanks to semantic metadata. 5. Ubiquity--content is accessible by multiple applications, every device is connected to the web, the services can be used everywhere.

This is not to imply that humans will not be important in Web 3.0. Rather, the structure of the data and interactions will enhance machine-to-machine communications and learning. Web 3.0 will transform the World Wide Web with a semantic web that facilitates creating, sharing and connecting content; AI that supports natural language processing and enhanced speed of action; 3-dimensional graphics that improve both human understandings and computer generated graphics; enhanced connectivity and access to information; and ubiquity with billions of other web-attached devices. In short, Web 3.0 will generate data, decision quality information and enhanced timeliness where humans will be challenged to keep up and machine-to-machine interactions will often dominate.

Today we are at Web 2.0 with some early surfacing features that will likely evolve into Web 3.0. For example, there are AI uses on the current web, but in Web 3.0, we should expect that computers would be able to differentiate information as humans do or perhaps even more accurately and efficiently depending on the evolution of this technology.

Transitioning from Web 2.0 to Web 3.0 will require technological development along numerous key areas including AI, communications and cybersecurity, big data, the IoT and the Internet of Bodies (IoB),[14] natural language processing, robotics, pattern recognition, machine learning, object recognition speech recognition and statistical learning, to name a few. Indeed, many Information Age technologies must coevolve for this development to proceed toward Web 3.0.

Internet evolution will be fraught with complexities and uncertainties; new approaches to issues such as the curation and storage of personal data; and ultimately a variety of risks from the system to the strategic levels that will require careful management.

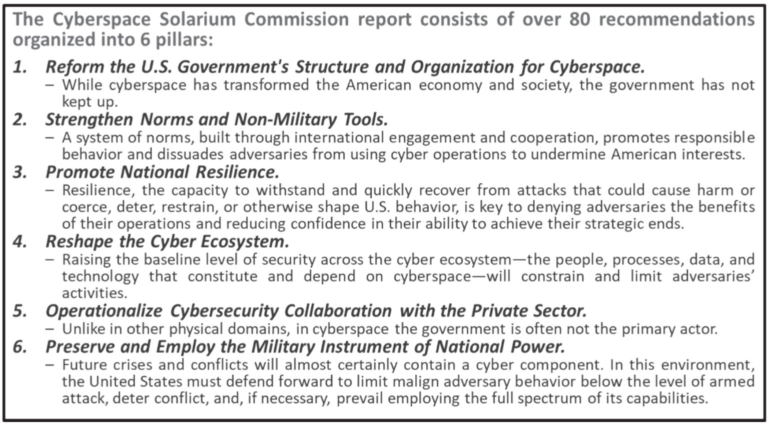
DoD's Defense Innovation Board (DIB) proposed AI Principles for the "design, development, and deployment of AI for both combat and non-combat purposes,"[15] and provides a useful point of departure for considering the implications of managing future cyber technology development risks. The stated goal is to develop technologies that are: responsible, equitable, traceable, reliable, and governable.

Strategic risks associated with lack of necessary governance relationships, inadequate planning and processes, or failure to take necessary actions also must be carefully considered. The DoD 2018 cyber strategy provided a framework with five reinforcing the lines of effort: build a more lethal force; compete and deter in cyberspace; expand alliances and partnerships; reform the Department; and cultivate talent.[16] However, this document focuses exclusively on military cyber domain considerations.

The more recently published Cyberspace Solarium Commission (CSC) report considers federal civilian and military cyber issues as well as non-governmental cyber concerns, and hence is more encompassing. The CSC was established in the National Defense Authorization Act for Fiscal Year 2019 to "develop a consensus on a strategic approach to defending the US in cyberspace against cyber attacks of significant consequences."[17] The bipartisan commission released its July 2020 report that contained over 80 recommendations organized into six pillars. The document was intended to serve as a road map for Congressional legislation to be developed (See Table 2).

The CSC report highlights shortfalls in organizational structures and coordination between federal and non-federal government entities, industry, academia, non-profits and international partners and stakeholders, and recognizes the importance of international norms and robust signaling and deterrence capabilities. It also stresses the importance of preparedness and response capabilities (including resilience) should deterrence fail.

Table 2. Cyberspace Solarium Commission Report Findings (July 2020)



The Cyberspace Solarium Commission report consists of over 80 recommendations organized into 6 pillars:

1. ***Reform the U.S. Government's Structure and Organization for Cyberspace.***
   – While cyberspace has transformed the American economy and society, the government has not kept up.
2. ***Strengthen Norms and Non-Military Tools.***
   – A system of norms, built through international engagement and cooperation, promotes responsible behavior and dissuades adversaries from using cyber operations to undermine American interests.
3. ***Promote National Resilience.***
   – Resilience, the capacity to withstand and quickly recover from attacks that could cause harm or coerce, deter, restrain, or otherwise shape U.S. behavior, is key to denying adversaries the benefits of their operations and reducing confidence in their ability to achieve their strategic ends.
4. ***Reshape the Cyber Ecosystem.***
   – Raising the baseline level of security across the cyber ecosystem—the people, processes, data, and technology that constitute and depend on cyberspace—will constrain and limit adversaries' activities.
5. ***Operationalize Cybersecurity Collaboration with the Private Sector.***
   – Unlike in other physical domains, in cyberspace the government is often not the primary actor.
6. ***Preserve and Employ the Military Instrument of National Power.***
   – Future crises and conflicts will almost certainly contain a cyber component. In this environment, the United States must defend forward to limit malign adversary behavior below the level of armed attack, deter conflict, and, if necessary, prevail employing the full spectrum of its capabilities.

Assessing Future Cyber Risks

Assessing the future cyber risk will require us to examine both the technology development principles identified by the DIB and strategic risks identified by the CSC. Many technology risks will be illuminated by the DoD (DIB) proposed principles for "design, development, and deployment of AI." These stated goals (i.e., responsible, equitable, traceable, reliable and governable) will be key as we develop technologies and transition from Web 2.0 to the more AI-based Web 3.0.

Responsible requires that humans exercise judgment in developing, deploying, using, and arriving at outcomes. Accomplishing this requires humans to embed structures and processes that directly account for and retain human control in the algorithms that enable the functionality of the cyber domain. It also requires keen human judgments in decision-making, a point important to consider more deeply.

Increasingly, we will see cases where computer-developed capabilities far exceed the speed, efficiency, and effectiveness of human-developed capabilities. To reduce the risks associated with these machine-created systems, humans, before embracing these new capabilities, need mechanisms in place that safely validate the new designs. As an example, consider development of an aerial drone chassis using AI technologies. By adding the goals of the design–i.e., the parameters of the system to be developed–the computer can optimize the platform design.[18] But beyond development of the drone, the system needs to be validated through a mix of tests and simulations conducted in both the virtual and real worlds.

While this sounds sensible, there are unfortunate examples where such appropriate care was not taken. Consider the Boeing aircraft company issues with the 737 Max aircraft Maneuvering Characteristics Augmentation System (MCAS) flight control, which through the combination of system design failures, inadequate training of pilots, and failure to alert the airlines to the incorporation of this technology resulted in the death of hundreds of people in two separate crashes.[19] This incident highlights two other painful lessons. The first is the fragility of human computer interfaces. For humans and computers to interoperate in systems, key information flows can become life-and-death essential to safe operation. Second, even if it is an automated system that fails, humans remain responsible for the outcomes. In this case, Boeing was found to have created an unsafe system that required modification and recertification for flight, and otherwise posed liability and crash-related lawsuits.

As capabilities become more complex, cyber community stakeholders will be challenged to establish responsibility without a deliberate focus on this area. As the hardware, software and processes (and algorithms) become less transparent, allocating responsibilities will become even more challenging, as discussed below under “traceability.”

Equity in cyberspace requires concrete measures to avoid bias in developing and deploying cyber-related systems, and to mitigate biases injected by cyber platform users (e.g., social media and deepfakes), to include both deliberate and unintended biases. For example, search engine developers often accord their parent company advantages such as responses to be loaded first and hence more likely to be viewed. In today’s Web 2.0, the greater number of clicks would result in advertisers paying more to preferred sites.

Unintended bias may manifest in search engines that reflect racist, sexist, or anti-Semitic attitudes as well. For example, Google discovered shortly after going public in 2004 that searching the term “Jew” returned hits on anti-Semitic websites.[20] The very concept of search engine usage creates these kinds of unintended issues. Search history is often targeted to identify other websites that might align with a person’s values, thereby opening the door to sites or topic areas perceived to be aligned. This can improve user’ experience, but also can lead to reinforcing biased behaviors through online content.[21] This was recently seen as a contributing cause of COVID-19 vaccine hesitancy.[22]

Facial recognition algorithms have come under scrutiny for their poor performance for certain demographic groups. One study points to “divergent error rates across demographic groups, with the poorest accuracy consistently found for those who are female, Black, and 18-30 years old.”[23] In this 2018 “Gender Shades" project, three facial recognition algorithms were compared for different demographic categories. The findings indicated, “All three algorithms performed the worst on darker-skinned females, with error rates up to 34% higher than for lighter-skinned males.”[24] With such a glaring gap in accuracy across demographic categories, it virtually assures low acceptability of the technology, particularly among disenfranchised groups.

Some of these issues of equity relate to the how the original research was conducted. Initial facial recognition data disproportionately used homogeneous white male populations, making facial recognition outside this grouping far less accurate. To address this issue, the facial recognition algorithms need to be trained on more "diverse and representative datasets." In collecting data, adjusting camera settings to better "capture people with darker skin tones" has been found to be useful. Finally, routinely assessing performance through regular "ethical auditing" should be incorporated to render facial recognition systems more accurate and hence reliable.[25]

Traceability requires understanding the technology, development processes, and methods of operational systems, including having transparent and auditable methodologies, data sources, and design procedures and documentation.[26] It implies having a direct line of sight through the lifecycle of the technology and across all its component parts. It is important to understand that a failure across any part of the system can result in catastrophic failure of the entire system in an operational setting.

Traceability requires validation and verification of the system and its component parts in both test and operational environments. Validation pertains to whether the system functions as intended, according to the customers' requirements. It answers the question, "Am I building the right product," and includes customer acceptance and usability testing. Verification ensures that the product adheres to specifications, and is conducted while the product is still under development, and can be done on individual modules or the complete system. It answers the question, "Am I building the product right," and includes unit, integration, and automated testing. Both validation and verification make use of regression, system, and Beta testing.[27] And, as with our previous facial recognition example, shortfalls in systems development and inadequately robust data hinders traceability of the results.

Self-driving cars illustrate yet another interesting traceability challenge. Self-driving cars depend on three autonomous systems that must function synchronously. The perception module uses cameras, radar, and LiDAR to identify objects in a car's vicinity. The prediction module forecasts the movements of these near neighbors. Finally, the decision module sets the driving policy and acts based on the inputs received from the other two modules. Despite inherent safety benefits of autonomous vehicles and millions of miles in real-world testing, technology concerns persist, and center around two issues: the legal implications of autonomous vehicle accidents and software traceability. To this second point, understanding how changes made affect vehicle functionality is imperative for traceability–ensuring that a digital thread exists that will confirm the software as well and thereby allow for auditing is essential.[28]

Traceability is also central to any debate about lethal autonomous weapon systems (LAWS). Autonomous systems are already employed for defensive purposes–such as the Phalanx close in anti-missile gun on several Navy ships and Israel's Iron Dome counter mortar system that the US has also employed in Iraq and Afghanistan, yet the offensive use of LAWS continues to be debated. The concern arises in the case of an allegedly unjust killing where one philosopher argues "that the autonomy of LAWS makes it impossible to hold anyone accountable for illegitimate killings they commit."[29] Who should be held responsible if the robot acted autonomously? This creates what some have called a "responsibility gap" that some find "morally objectionable and legally infeasible."[30]

A software bill of materials (SBOM) has become a "key building block in software security and software supply chain risk management." SBOM guidance for developing software increases the transparency of products developed, information on SBOM tools that support creators and vendors in classifying their products, and summaries of formats and standards for software development. In short, SBOM enhance the traceability of the software.[31]

Reliability requires an "explicit, well-defined domain of use, and the safety, security, and robustness of such systems should be tested and assured across their entire life cycle within that domain of use."[32] Reliability overlaps with validation and verification discussed under traceability above. Testing at all stages of development should continue throughout a system's lifecycle, from basic and applied research to early-stage development, and throughout fielding and use in operational environments.

It would be comforting to observe the great benefits experienced to date from the cyber domain and the invaluable uses of these technologies. In the same breath, one could confirm explosive growth of the cyber economy with great benefit to those able to incorporate the technology. All true, but the cyber domain also has contributed to instability, both within the US and indeed, worldwide. We have seen conclusive evidence of devastating physical and other damage to critical infrastructure, to say nothing of the adverse effects of tainted information and sources of news which have become no longer trustworthy.

Reliability shortfalls in our hardware, software, networks, and data storage capacity often contribute to the initial breach and the severity of the intrusion. The Office of Personnel Management (OPM) data breach–characterized as the most significant breach of sensitive personnel data to have ever occurred–began in November 2013, but was not discovered until June of 2015.[33] OPM's system was breached with over 20 million SF-86 security clearance adjudication packages exfiltrated over an 18 month period. While China was identified as the perpetrator, even the post-breach period demonstrated a lack of system reliability and resilience coupled with shortfalls in preparedness, response and resilience.[34] This data breach highlighted numerous deficiencies and insecurities ranging from procedural issues and inadequate cyber hygiene to antiquated systems and obsolete methods for storage of sensitive data. The breach was not discovered until government software (Continuous Diagnostics and Monitoring (CDM)) was being installed. The breach highlighted the challenges that "smaller-sized, medium-sized agencies that didn't consider themselves to be [at] such a threat to cyberactivity from data thieves, that they also have this potential [negative] publicity associated with becoming a target and becoming a victim."[35]

More recent cyber breaches such as the Colonial Pipeline ransomware and log4j software vulnerability continue to demonstrate the inadequate security of the Internet and its associated components. To put a fine point on these issues, they have exposed the lack of reliability in our systems. As with other such cyber incidents, the Colonial attack exposed an important human dimension which contributed to the breach as the attackers gained access to the network through an "exposed password for a VPN [virtual private network]."[36] Despite planning, exercises and even simulations of attacks against U.S. infrastructure, we collectively—Colonial, the critical infrastructure sector and nationally—were not prepared when a criminal extortion ring gained control of corporate data and held it for ransom. Colonial Pipeline was left to conclude that their supposed "impermeable wall of protections was easily breached."[37]

The discovery of the log4j vulnerability should give us great cause for concern. U.S. Cybersecurity and Infrastructure Security Agency (CISA) Director Jen Easterly, identified the log4j vulnerability as "the most serious vulnerability I have seen in my decades-long career."[38] Log4j is free "code that helps software applications keep track of their past activities."[39] The vulnerability is created if a line of malicious code is inserted into the software that would allow "bad actors [to] grab control of servers that are running log4j."[40] The ubiquity of this code is cause for great concern. Perhaps more concerning is that the code, and hence this zero-day vulnerability, was in use for years before being discovered in 2021. What does this say about our software assurance capabilities and how many potentially catastrophic log4j-like vulnerabilities are in the offing?

A final note on reliability is in order here. Numerous hacks, attacks, breaches, and insecurities have resulted from legacy systems running obsolete hardware and software components that are generations past their technological prime. Despite security patches and efforts to improve user awareness and procedures, there is only so much that can be done. Eventually obsolete equipment must be replaced. This challenge is magnified as most of the cyberinfrastructure, some 85% of all US-based cyberinfrastructure, is in the private sector and hence requires private sector investments to be made.[41]

By way of a postscript on reliability, Microsoft's report, *Defending Ukraine: Early Lessons from the Cyber War*, illustrates that cyber lessons regarding reliability are being learned in real time. For example, having dispersed and distributed digital operations within and outside of a nation's national borders is critical. A combination of threat intelligence and endpoint protection have mitigated some of the threats that had the potential for devastating consequences. Having a coordinated and comprehensive cyber strategy that includes defenses against "destructive cyberattacks, espionage and influence operations" is essential. As with any conflict, both sides can adapt. This has been reinforced in the Russia-Ukraine war as Russia has increased its network penetration and espionage activities, targeting both Ukraine and allied governments supporting Ukraine.[42] The message is that regardless of the preparations and response capabilities that have been developed, adapting in real time to threats and vulnerabilities is essential to stay ahead of adversaries.

Governable connotes a system "designed and engineered to fulfill their intended function while possessing the ability to detect and avoid unintended harm or disruption and disengage or deactivate deployed systems that demonstrate unintended escalatory or other behavior." Governability significantly overlaps with reliability. Certainly with 85% of critical infrastructure held privately, governance is a huge challenge. Technical challenges also pose governance hurdles—the log4j vulnerability is but one example, which brings to mind the adage, "if you've seen one cyber-attack, you've seen one cyber-attack." This makes governance in cyberspace increasingly more challenging.

Recent experiences illustrate that the magnitude of the intrusion or attack also contributes to the challenges of governing cyberspace. The SolarWinds breach penetrated a number of US government agencies—including the Treasury and Commerce Departments, and unconfirmed reports of the Department of Defense, NASA and the White House—and compromised hundreds of organizations worldwide.[43] *Cybercrime Magazine* estimates that the world will lose $10.5 trillion annually to cybercrime by 2025. Highlighting the implications of this risk, the source identifies cybercrime as "the greatest transfer of economic wealth in history."[44] The numbers illustrate just how pervasive the problem is becoming.

The news is no better for the effects on social media which has been implicated in a variety of ills including manipulated elections, inciting violence, facilitating cyber bullying and cyber abuse, and proliferating offensive and illegal content. After revelations of social media's—in particular Facebook (now Meta)—influence over the 2016 elections, the company announced that it barred all political advertisements the week before the 2020 elections.[45] According to a Pew Research survey, "Many users see social media as an especially negative venue for political discussions," despite its growing user base and continued use for this purpose.[46]

So how should we think about issues of cyber governance? Several key shortfalls underlie the demonstrated inability to govern cyberspace.

First, the tools to appropriately govern cyberspace are lacking. The only true governance on the Internet today are the technical specifications that allow the Internet to function. No one or no single organization is in charge of the Internet. Cyberspace grew up as an organic domain and has continued to evolve to its current state. The Internet was not centrally planned and has truly been built from the ground up. As new concepts and capabilities are incorporated into the Internet, the evolution continues. The horizontal and vertical growth of the Internet tech companies demonstrates this evolution. This puts leaders of large tech firms in the position of governance over large swaths of the Internet which often leads to conflicts of interest, placing shareholder value and public safety interests at odds.[47]

Second, the Internet lacks the ability to sense in real-time when anomalous and potentially dangerous activities are occurring. Here the Internet should be considered in its broadest sense and include governments, industry and the private sector, and individual users. Capabilities are incorporated into the Internet before they are fully understood, with guardrails installed, often after the fact, to address potential vulnerabilities.

Third, we rely on users for too much sophistication. One assessment focusing on the human factor in IT [information technology] security, observes that over half of the companies "believe they are at risk from within" from user carelessness or lack of knowledge.[48] This concern was even more pronounced for smaller corporations. Even for personal use, an expectation of sophistication is inherent. Individual users are expected to understand the threats and vulnerabilities, replace obsolete systems, and routinely patch their systems. These expectations continue despite estimates that "95% of cybersecurity breaches are a result of human error, only 5% of companies' folders are properly protected, only 16% of executives say their organizations are well prepared to deal with cyber risk, and over 77% of organizations do not have a cyber security incident response plan."[49]

STRATEGIC CYBER RISKS

In the previous section we discussed technology development principles for cyberspace technologies. Here we will briefly consider the strategic implications associated with cyberspace. For this purpose, the Cyberspace Solarium Commission provides a useful point of departure. Unlike in the previous section's focus on the individual development principles, reference to the CSC is to remind the reader that the cyber domain is global and overlays the other natural domains (i.e., land, maritime, air, and space).

We must remain mindful that the Solarium Commission's six pillars and 80 recommendations cannot apply solely within the US. Optimally, they must apply to the entire international cyberspace domain. As an example, the first CSC pillar calls for reforming the US structure and organization for cyberspace. That structure must also fit within international structures and organizations. For example, the US cyber structures and organizations should support economic activities, account for societal norms, and also be aligned with international laws and regulations.

Several Solarium Commission recommendations pertain to building capacity to improve security, strengthen norms, and enhance resilience to withstand and recover. These activities should be undertaken with a keen eye toward the five technology development risks discussed in the previous section—cyber domain technologies developed must be: responsible, equitable, traceable, reliable, and governable.

Having internationally accepted cyber domain "rules of the road" going forward is vitally important. Unless these rules effectively police against behavior that is irresponsible, inequitable, untraceable, unreliable or ungovernable, it is difficult to envision how the Internet can continue to serve US interests and values.

As the CSC emphasizes, all stakeholders must be considered and represented, and governments at all levels must meaningfully participate in establishing laws, norms, and regulations. Industry and academia bring the greatest technical knowledge and therefore must be represented when solutions are needed. Private citizens must have input as they will increasingly find the cyberspace dominating important aspects of their lives.

CONCLUDING THOUGHTS

Ideally, transition from Web 2.0 to Web 3.0 should not occur until the technology development and strategic cyber risks have been carefully analyzed and addressed. However, logic may not govern transition to Web 3.0. Already we are witnessing the rapid incorporation of IoT (and soon IoB) devices, wearables, machine learning and AI technologies long before most even realize the rapid transition is occurring.

Moving to Web 3.0—which will rely on greater use of machine-to-machine communications and less human intervention—should evolve deliberatively, and only after adequate assessment and mitigation of risks are fully incorporated into the future cyber domain. Here the DoD (DIB) principles provide a useful framework for understanding these risks and developing approaches to mitigate concerns. In concert greater progress must also be made to address strategic cyber risks.

Continuing to advance before the range of threats, vulnerabilities, and consequences inherent in the future cyber risks of Web 3.0 are fully analyzed and mitigated at each step of our progressive evolution towards Web 3.0 not only would be wrong; it also would be foolhardy.

NOTES

1. Tim Chao, Tuan Pham and Mikhail Seregine, "The Dangers of Technological Progress," Stanford University, https://cs.stanford.edu/people/eroberts/cs201/projects/1999-00/technology-dangers/issues.html, accessed December 6, 2018.
2. Kirsten Errick, "White House Cyber Director: 'Defense is the New Offense' for Cyber," Nextgov, August 14, 2022, https://www.nextgov.com/cybersecurity/2022/08/white-house-cyber-director-defense-new-offense-cyber/375822/.
3. "Triple digit increase in cyberattacks: What next?" Accenture, August 4, 2021, https://www.accenture.com/us-en/blogs/security/triple-digit-increase-cyberattacks.
4. "6 Cyber Attacks that Caused Property Damage," The ALS Group, March 14, 2017. https://info.thealsgroup.com/blog/cyber-attacks-property-damage.
5. "When Cyber threats get Physical," Clyde and Co, May 17, 2021, https://www.clydeco.com/en/insights/2021/05/when-cyber-threats-get-physical.
6. Sama Al-Kurdi, "The 10 Biggest Cyber Attacks In History," *Albawaba*, June 26, 2021, https://www.albawaba.com/business/10-biggest-cyber-attacks-history.
7. "are the jbs and colonial attacks just the beginning?" Silent Breach, https://silentbreach.com/BlogArticles/are-the-jbs-and-colonial-attacks-just-the-beginning/.
8. Paul Rosenzweig "Is It Really 85 Percent?" *Lawfare*, May 11, 2021, https://www.lawfareblog.com/it-really-85-percent.
9. Rob Sobers, "134 Cybersecurity Statistics and Trends for 2021," Varonis, March 16, 2021, https://www.varonis.com/blog/cybersecurity-statistics/.
10. "The Internet is a global network of networks while the Web, also referred formally as World Wide Web (www) is a collection of information that is accessed via the Internet," What's difference between the Internet and the Web? GeeksforGeeks. Last updated November 3, 2021, https://www.geeksforgeeks.org/whats-difference-internet-web/#:~:text=The%20Internet%20is%20a%20global,on%20top%20of%20that%20infrastructure.
11. Ibid.
12. Ibid.
13. Ibid.
14. Bernard Marr, "What Is The Internet Of Bodies? And How Is It Changing Our World?" *Forbes*, December 6, 2019, https://www.forbes.com/sites/bernardmarr/2019/12/06/what-is-the-internet-of-bodies-and-how-is-it-changing-our-world/?sh=421e2dbf68b7
15. AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense by the Defense Innovation Board (Undated), https://media.defense.gov/2019/Oct/31/2002204458/-1/-1/0/DIB_AI_PRINCIPLES_PRIMARY_DOCUMENT.PDF, While this document pertains specifically to ethical use of AI, the categories also related directly to examining the risks.
16. Summary: Department of Defense cyber strategy 2018, U.S. Department of Defense, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.
17. Cyberspace Solarium Commission (CSC), https://www.solarium.gov/.
18. "Drone design artificial intelligence," TEDx, March 1, 2017, https://www.youtube.com/watch?v=odHC-gxJhG4.
19. Darryl Campbell, Redline: The many human errors that brought down the Boeing 737 Max," The Verge, May 2, 2019, https://www.theverge.com/2019/5/2/18518176/boeing-737-max-crash-problems-human-error-mcas-faa.
20. Edward Tenner, "Search Engines May Seem All-Knowing, But They're Not. Here's How to Get More Trustworthy Results" *Time*, June 26, 2018, https://time.com/5318918/search-results-engine-google-bias-trusted-sources/
21. Bias in the machine: Internet algorithms reinforce harmful stereotypes," Princeton University, Department of Computer Science, November 22, 2016, https://www.cs.princeton.edu/news/bias-machine-internet-algorithms-reinforce-harmful-stereotypes.
22. Matthew Daniel, "Fake news, politics, and behavioral biases: A perfect storm for vaccine hesitancy," BenefitsPRO, January 6, 2022, https://www.benefitspro.com/2022/01/06/fake-news-politics-and-behavioral-biases-a-perfect-storm-for-vaccine-hesitancy/?slreturn=20220715112223.
23. Alex Najibi, "Racial Discrimination in Face Recognition Technology," Harvard University: Science in the News. October 24, 2020, https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/
24. Ibid.
25. Ibid.

NOTES

26. AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense by the Defense Innovation Board (Undated), https://media.defense.gov/2019/Oct/31/2002204458/-1/-1/0/DIB_AI_PRINCIPLES_PRIMARY_DOCUMENT.PDF.
27. "Verification vs Validation: Do You know the Difference?" Plutora, November 23, 2020, https://www.plutora.com/blog/verification-vs-validation.
28. Patrick Londa, "Autonomous Vehicles Pose an Unprecedented Software Challenge," *Design News*, August 28, 2018, https://www.designnews.com/automotive/autonomous-vehicles-pose-unprecedented-software-challenge.
29. Matthew Anzarouth, "Robots that Kill: The Case for Banning Lethal Autonomous Weapon Systems," *Harvard Political Review*, December 2, 2021, https://harvardpolitics.com/robots-that-kill-the-case-for-banning-lethal-autonomous-weapon-systems/.
30. Ibid.
31. Software Bill of Materials, Department of Commerce, National Telecommunications and Information Administration, Accessed March 7, 2022. https://ntia.gov/SBOM.
32. AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense by the Defense Innovation Board, October 31, 2019, https://media.defense.gov/2019/Oct/31/2002204458/-1/-1/0/DIB_AI_PRINCIPLES_PRIMARY_DOCUMENT.PDF.
33. Michael Adams, "Why the OPM Hack Is Far Worse Than You Imagine," *Lawfare,* Friday, March 11, 2016, https://www.lawfareblog.com/why-opm-hack-far-worse-you-imagine.
34. Ian Smith, "Bolton Confirms China was Behind OPM Data Breaches." FedSmith. September 21, 2018, https://www.fedsmith.com/2018/09/21/bolton-confirms-china-behind-opm-data-breaches/.
35. Brian Naylor, "One Year After OPM Data Breach, What Has The Government Learned? *NPR*, June 6, 2016, https://www.npr.org/sections/alltechconsidered/2016/06/06/480968999/one-year-after-opm-data-breach-what-has-the-government-learned.
36. Sean Michael Kerner, "Colonial Pipeline hack explained: Everything you need to know." Tech Target: WhatIs.com, April 26, 2022, https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know#:~:text=What%20was%20the%20root%20cause,Homeland%20Security%20on%20June%208.
37. David E. Sanger and Nicole Perlroth, "Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity," *The New York Times*, May 14, 2021, updated June 8, 2021, https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html.
38. Tatum Hunter and Gerrit De Vynck, "The 'most serious' security breach ever is unfolding right now. Here's what you need to know." The Washington Post, December 20, 2021, updated December 20, 2021, https://www.washingtonpost.com/technology/2021/12/20/log4j-hack-vulnerability-java/
39. Ibid.
40. Ibid.
41. Paul Rosenzweig, "Is It Really 85 Percent?" *Lawfare*, May 11, 2021, https://www.lawfareblog.com/it-really-85-percent.
42. Brad Smith, "Defending Ukraine: Early Lessons from the Cyber War," Microsoft, June 22, 2022, https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/.
43. "are the jbs and colonial attacks just the beginning?" Silent Breach, https://silentbreach.com/BlogArticles/are-the-jbs-and-colonial-attacks-just-the-beginning/.
44. Steven Morgan, "Cybercrime To Cost The World $10.5 Trillion Annually By 2025," *Cybercrime Magazine,* November 13, 2020, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.
45. Michael Baldassaro and David Carroll, "It's time for Congress to regulate political advertising on social media," *The Hill*, October 7, 2020, It's time for Congress to regulate political advertising on social media | TheHill.
46. Lee Rainie, "Americans' complicated feelings about social media in an era of privacy concerns," Pew Research Center, March 27, 2018, How Americans feel about social media and privacy | Pew Research Center
47. Craig Timberg, "Net of Insecurity: A Flaw in the Design." *The Washington Post*, May 30, 2015. https://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/.
48. "The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within," *Kaspersky Daily*, https://www.kaspersky.com/blog/the-human-factor-in-it-security/.
49. "15 Cybersecurity Statistics in 2021," TitanFil, https://www.titanfile.com/blog/15-important-cybersecurity-statistics-in-2021/.

Russian Cyber Operations in the Invasion of Ukraine

Dr. Herbert Lin

INTRODUCTION

In March 2021, Russia began to deploy large numbers of troops and armaments near the Russia-Ukraine border in what Western observers believed posed an invasion threat to Ukraine, which Russia strongly denied. An intense debate in the West ensued over whether the troops were being deployed to pressure Ukraine into making political concessions or to conduct an actual invasion.

Noting previous Russian offensive cyber operations against Ukraine starting as early as 2014, many cyber analysts and scholars predicted that an invasion would be accompanied by significant cyberattacks on Ukraine and possibly on Western nations supporting Ukraine, including particularly the US. For example, Maggie Miller wrote in *Politico* that "in a full-scale cyber assault [on Ukraine], Russia could take down the power grid, turn the heat off in the middle of winter and shut down Ukraine's military command centers and cellular communications systems."[1] Samuel Charap of the RAND Corporation thought the most likely Russian response to Western economic sanctions would be a cyber operation that temporarily shut down some major Western banks.[2]

Russia launched its invasion of Ukraine on February 24, 2022. Since then, many cyber analysts and scholars have observed that Russian offensive cyber operations have played a relatively small role compared to its kinetic operations. For example, in explaining why Russian cyber operations had yet to play an important tactical role in its invasion, Nadiya

Dr. Herbert Lin is senior research scholar for cyber policy and security at the Center for International Security and Cooperation and Hank J. Holland Fellow in Cyber Policy and Security at the Hoover Institution, both at Stanford University. His research interests relate broadly to policy-related dimensions of cybersecurity and cyberspace, with particular focus on the use of offensive operations in cyberspace as instruments of national policy and security dimensions of information warfare and influence operations on national security. He is also Chief Scientist Emeritus for the Computer Science and Telecommunications Board, National Research Council (NRC) of the National Academies, where he served (1990-2014) as study director of major projects on public policy and information technology, and Adjunct Senior Research Scholar and Senior Fellow in Cybersecurity (not in residence) at the Saltzman Institute for War and Peace Studies in the School for International and Public Affairs at Columbia University. In 2016, he served on President Obama's Commission on Enhancing National Cybersecurity.

Kostyuk and Erik Gartzke argued that that such operations were best suited for pursuing informational goals, such as gathering intelligence, stealing technology, or winning public opinion or diplomatic debates, whereas kinetic military operations occupy territory, capture resources, diminish the military capability of opponents, and terrorize populations.[3] Writing with Lennart Maschmeyer,[4] Kostyuk poses an important question: If cyber operations offer effective and potent instruments for coercion, why did Russia go to the effort and expense of mobilizing its troops? Their conclusion is that cyber operations do not in fact provide such instruments.

On April 12, 2022, the Ukrainian Computer Emergency Response Team (CERT-UA) and the Slovakian cybersecurity firm ESET issued advisories that the Sandworm hacker group, confirmed to be Unit 74455 of Russia's military intelligence agency, the GRU, had conducted cyberattacks against high-voltage electrical substations in Ukraine,[5] which reportedly were thwarted but could possibly have hit two million Ukrainians with lost power. (An earlier, private advisory from CERT-UA reported that power to nine electrical substations had been temporarily switched off, but this later was disavowed by Victor Zhora, Ukraine's deputy head of the State Special Service for Digital Development, characterizing the private report as "preliminary," and a "mistake."[6])

Russia was not entirely inactive on the cyber front. For example, on the first day of the invasion, a Russian cyberattack on tens of thousands of satellite modems in Ukraine and elsewhere in Europe disabled Internet service for many in those regions. Going beyond a simple denial-of-service attack, this attack also destroyed key data on these modems, rendering them permanently inoperative. A Ukrainian cyber official said the attack led to "a really huge loss in communications in the very beginning of the war,"[7] although one more recent report indicates that this official's comments regarding the magnitude of the impact were misunderstood at the time.[8] Other cyberattacks conducted contemporaneously with or just prior to the invasion include the following:

- Ukrainian websites across multiple sectors were subjected to Russian distributed denial-of-service (DDoS) attacks in mid-February, including one on the Ukrainian Ministry of Defense on February 15.[10]
- Russian wiper malware programs appeared in Ukrainian systems; to date, a number of distinct variants have been identified. These programs erase user data, programs, and hard drives.[11] Wiper malware-affected Ukrainian government, financial, information technology, and energy sectors also spread to systems in other European countries.
- Ukrainian Internet services were temporarily disrupted in targeted attacks on telecommunications providers Triolan on March 9, Vinasterisk on March 13, and Ukrtelecom on March 28.[12]
- A month into the invasion, Russia launched cyberattacks against Starlink terminals, which SpaceX had deployed into Ukraine to augment its satellite communications capability. These attacks reportedly succeeded for several hours, until SpaceX updated software to resist such attacks.[13]
- Western social media companies identified several disinformation campaigns. These campaigns have included coordinated inauthentic behavior on social media, brief takeovers of media channels, and attempts to compromise social media accounts.[14] On March 28, the Security Service of Ukraine announced that it had shut down five disinformation-spreading bot farms operating over 100,000 social media accounts since the invasion began.[15]

Implicitly building on these examples, David Cattler and Daniel Black, Assistant Secretary General for Intelligence and Security and Principal Analyst in the Cyber Threat Analysis Branch at NATO, respectively, wrote in *Foreign Affairs* that “the magnitude of Moscow’s pre-kinetic destructive cyber-operations was unprecedented” and that on February 24, 2022, “Russian cyber-units successfully deployed more destructive malware—including against conventional military targets such as civilian communications infrastructure and military command and control centers—than the rest of the world’s cyberpowers combined typically use in a given year.” They assert that, contrary to assessments that Russian cyber operations were ineffective, Russia’s invasion strategy “failed to capitalize on the full capabilities and numerous operational successes of its cyber-units.” They further argue that “cyber operations have been Russia’s biggest military success to date in the war in Ukraine,” and that “they will continue to provide Moscow a flexible tool capable of hitting a range of targets in Ukraine and beyond.”[16]

Microsoft has compiled the most complete inventory of cyberattacks against Ukraine to date,[17] reporting that “the cyber operations so far have been consistent with actions to degrade, disrupt, or discredit Ukrainian government, military, and economic functions, secure footholds in critical infrastructure, and to reduce the Ukrainian public’s access to information.” Microsoft observed that "cyber and kinetic military operations appeared to be directed toward similar military objectives. Threat activity groups often targeted the same sectors or geographic locations around the same time as kinetic military events." However, it was unclear "if there was coordination, centralized tasking or merely a common set of understood priorities driving the correlation."

Assuming this listing captures most cyberattacks immediately before the invasion and thereafter (see below note for a type of cyberattack that was not captured), the timeline suggests that cyber activity against Ukraine increased post-invasion but to a lesser degree than what many commentators expected. Thus, while Russia has enjoyed some degree of success in cyberspace in prosecuting its invasion, its cyber operations have fallen short of many experts' pre-invasion predictions.

This lack of impact has characterized both strategic and tactical dimensions of the conflict. Strategically, Russian cyberattacks have not affected Ukraine's critical infrastructure on a large scale, as electric power and Internet services remain up and running in many parts of Ukraine, including some that have been bombed or shelled. Tactically, Russian military operations have used a variety of traditional battlefield tactics, techniques, and procedures, but with cyber operations playing a significantly lesser role.

This article explores the use of offensive cyber operations in the Russia-Ukraine conflict as they have been seen and discussed in the public domain.

On the Value of Offensive Cyber Operations

Analysts often distinguish between coercive and warfighting uses of military force. Coercive uses of or threats to use force seek to influence an adversary's decisions, whereas warfighting uses of force seek to degrade an adversary's military power or effectiveness.

The international relations literature persuasively establishes that successful coercion is not simply a matter of a more militarily powerful party asserting dominance over a less powerful one—coercion is a more complex endeavor and success is less certain. Vast nuclear superiority is widely believed to have coerced Japan's surrender in World War II and the Soviet Union to back down during the Cuban Missile Crisis. However, the record on non-nuclear coercion is much more mixed. As Byman and Waxman put it, "[w]hile the US military arsenal may be extremely precise in a technological sense, the ability to finely tune the political effects its use has on an adversary's population, elite, or key regime decision makers remains largely beyond U.S. planners."[20]

How, if at all, does the capability to launch powerful cyberattacks change these conclusions? On the first, how, if at all, does the ability to exercise significant offensive cyber capabilities give nations greater coercive power against their adversaries? On the second, how, if at all, does the use of significant offensive cyber capabilities enhance the warfighting effectiveness of a nation's armed forces?

Note –
Physically-Mediated Cyberattacks on Ukraine

On May 13, 2022, the State Service of Special Communication and Information Protection of Ukraine published a notice alleging that "Russia's special services" had physically targeted Ukrainian internet service providers (ISPs).[18] Apparently, the Russians military physically invaded the offices of Stratus, a Ukrainian internet service provider located in Kherson, and at the point of a gun, ordered the staff in the office to alter the availability of websites that users of the service would normally be able to access.

Such outcomes could, of course, be caused through various cyberattacks carried across the internet. But attacks that compromise cyber functionality through the use of or the threat of physical force are an understudied phenomenon.

Two points are particularly relevant here. First, insider attacks are a well-known problem in cybersecurity. Trusted (authorized) insiders can be "turned" to take actions for which they have the proper technical authorization but for purposes that are contrary to the rationale for granting those authorizations in the first place.

Second, the physical facilities of ISPs have also been known to be vulnerable, as exemplified by cuts in fiber-optic cables resulting in denials of service to customers depending on those cables. That is, the physical security of cyber infrastructure has always been an important, if often neglected, aspect of cybersecurity.

While a demand for an ISP located in a region under Russian military occupation to conform to Moscow's pressure regarding Internet connectivity is not surprising, one can also imagine similar activities directed against ISPs located in other regions whose governance is contested. Physical violence against cyber personnel in lawless environments as an element of cyberattack is another dimension of cyber conflict, and its importance has been neglected for way too long. But we do not even have a category in the cyber conflict lexicon to address its nature or significance.[19]

As an important preliminary point, offensive cyber capabilities do provide nations with additional instruments of covert action (e.g., sabotage, espionage, and political subversion).[21] Through actions taken in cyberspace, nations can cause physical damage to important facilities as demonstrated in the outcome of cyberattacks against Iranian uranium centrifuges and steel mills in 2010 and 2022, respectively.[22] They can also steal confidential information of high economic or intelligence value,[23] sometimes in sufficient quantity to be of strategic significance.[24] Finally, they can interfere in democratic political processes, such as elections.[25] Although sabotage, espionage, and political subversion are distinctly hostile acts that seek to weaken adversaries, they are neither acts of coercion (they are not undertaken in an attempt to seek concessions from adversaries) nor acts of warfighting. Several analysts believe that a relative insignificance of cyberattacks in the Russian-Ukraine conflict validates this view.[26]

Not all analysts share this view, however. Arguing before February 24 in favor of the proposition that offensive cyber capabilities do increase coercive power, William Courtney and Peter A. Wilson wrote in *The Hill* that a Russian invasion would "likely employ massive cyber and electronic warfare tools and long-range PGMs . . . to create 'shock and awe,' [and] causing Ukraine's defenses or will to fight to collapse."[27] Jason Healey of Columbia University said that "a Russian cyber offensive . . . might have far more impact on the battlefield, more coercive power, more lethal and widespread effect than many doubters would expect."[28]

As for warfighting potential, the U.S. Department of Defense (DoD) asserts a rather broad utility for offensive cyber operations. For example, Joint Publication 3-12 characterizes cyberattacks as a form of fires,[29] similar in principle to artillery or machine-gun fire, that degrades, disrupts, destroys, or manipulates adversary information or information systems. DoD doctrine also acknowledges the value of cyber operations for exploitation, including military intelligence activities, maneuver, information collection, and other enabling actions required to prepare for future military operations.[30]

THE STRATEGIC PERSPECTIVE

As noted earlier, Russian cyber operations against Ukraine have apparently had little coercive effect on Ukraine. This section explores possible reasons for this outcome.

First, prophylactic defensive measures by Ukrainian and Western cyber experts may have borne significant fruit in hardening many Ukrainian critical infrastructure systems. Since 2014, Ukraine has served as a kind of cyber test range for Russian cyber attackers, but the US, the European Union, and NATO member states have provided cybersecurity assistance to help Ukraine prepare for future attacks. For example, the U.S. Agency for International Development announced in 2020 that it was investing $38 million in Ukrainian cybersecurity over four years.[31] On March 10, 2022, General Paul Nakasone, Commander of U.S. Cyber Command (USCYBERCOM), testified to the Senate Intelligence Committee that "we've worked very, very hard with Ukraine over the past several years. . . We had 'hunt forward' teams from U.S. Cyber Command in Kyiv. We worked very, very closely with a series of partners at NSA and the private sector to be able to provide that information."[32] The US has also helped to broker a number of public-private partnerships between Ukraine and Western information technology companies such as Microsoft and Google. These companies identified and blocked Russian cyber threats against Ukraine in near-real-time as they emerged,[33] and their familiarity with and instrumentation of Ukrainian networks enabled them to act more rapidly than government agencies.

Second, Ukraine or Western military or intelligence organizations may themselves have been conducting offensive cyber operations against Russian hackers to disrupt cyberattacks against Ukraine. Information about any such operations would be highly classified, but on March 10, 2022, Anne Neuberger, Deputy National Security Advisor to the President for Cyber & Emerging Technology, described a three-part strategy for responding to Russian cyberattacks against Ukraine, one of which was to "make it harder for attackers to conduct disruptive operations, whether that is disrupting [their] infrastructure and more sensitive operations that I won't get into here."[34] A precedent for such activity may have been the reported disruption of the Internet Research Agency, a Russian troll farm, by USCYBERCOM[35]—according to *The Washington Post*, offensive actions by USCYBERCOM blocked Internet access for the IRA on election day, 2018. Similar actions could have disrupted the operations of Russian hacker groups targeting Ukraine.

Nor are Western government agencies the only parties capable of conducting offensive cyber operations against Russia. A variety of news reports indicates that non-government hackers have acted against Russian information systems, including actions to slow the transport of Russian troops and equipment by putting the trains into a manual control mode,[36] breaching Russian databases and hacking Russian media and government websites,[37] and releasing personal information on Russian soldiers who operated in Bucha, as well as Russian intelligence agents in the Federal Security Service (FSB).[38] On balance, such activities force Russian cyber forces to expend considerable time and effort on countermeasures,[39] leaving them with fewer resources to go on the offensive themselves.

Third, the apparent paucity of Russian cyberattacks may also reflect their omission from the Russian planning process for the invasion. Integrating offensive cyber capabilities into an overall military operational plan is relatively new, compared to more traditional military capabilities such as armor and artillery. Russian military leaders seemed caught off-guard when relatively simple logistical problems slowed the invasion to a snail's pace, and there is no reason to conclude that planning deficiencies were limited to the logistical aspects of ground combat—Russian military planners may simply have neglected or consciously chosen to omit Russian offensive cyber capabilities in their invasion plan. Supporting this possibility, Ciaran Martin, former head of the UK National Cyber-Security Centre, noted that "if . . . Putin withheld knowledge of his invasion plans from large sections of the Russian military and intelligence bureaucracy, then they wouldn't have had time to prepare those attacks, and you can't just conjure up a powerful cyberattack overnight."[40]

Fourth, Russia may want to keep its cyber powder dry for use against the West if and when necessary. Former CISA director Chris Krebs wrote on March 20, 2022, that "as political and economic conditions deteriorate, the red lines and escalation judgments that kept Moscow's most potent cyber capabilities in check may adjust. Western sanctions and lethal aid support to Ukraine may prompt Russian hackers to lash out against the west."[41] Around the same time, Senate Intelligence Committee Chair Mark Warner told *Politico* that "we have not seen their A-game tools."[42] In this view, the Russians may believe that the likelihood of successfully conducting specific offensive cyber operations diminishes the more they are used, and are saving their most potent weapons for later use.

Lastly, previous cyberattacks targeting Ukrainian critical infrastructure have been conducted at a level considerably below a "whole-of-country" effort. These cyberattacks constituted proofs of principle of Russian cyber capabilities, at least against the Ukrainian cyber defenses of the time, but many in the West extrapolated from such demonstrations a capability to attack all Ukrainian critical infrastructure more or less simultaneously in an all-out prelude to the ground invasion. Such extrapolations rely on an assumption that resource constraints did not exist for Russian cyber attackers, and perhaps in reality resource constraints have prevented a significant scaling-up of Russian cyberattacks. Moreover, to the extent that Russian offensive cyber operations would be conducted wirelessly, cyber operations deep in the heart of Ukraine would likely be more challenging to coordinate than those that were mostly contained on the Russia-Ukraine border, as many such previous Russian operations had been.[43]

THE TACTICAL PERSPECTIVE

The intense kinetic attack on Ukraine has caused extensive damage to Ukrainian infrastructure, which may well have reduced the need to use cyberattacks to target infrastructure as part of the invasion. Dmitri Alperovitch, founder of the cybersecurity company CrowdStrike, noted that "cyber is a fantastic tool for gray-zone conflict, that area between peace and war, where you are trying to hit back at the other party, but you don't want to escalate this to an actual kinetic conflict… [but] once conflict actually begins, once bombs are flying, cyber becomes much less useful."[44] Christopher Painter, former State Department cybersecurity coordinator, observed that "physical invasion trumps cyber. . . You don't need cyber as much when you have tanks and planes on the ground and men on the ground, so maybe cyber … maybe it isn't the perfect weapon."[45] Ciaran Martin, former head of the United Kingdom's National Cyber Security Center, has suggested that Russia may have wished to preserve Ukrainian infrastructure for use during the invasion,[46] especially for communications assets such as cell phone networks.[47] (Note that these explanations seem somewhat contradictory—the first saying that Russians refrained from cyberattacks because kinetic weapons are pulverizing the infrastructure and the second saying that it is because the Russians wanted to maintain the infrastructure in operable condition for their own use. Still, both reasons could be operative at the same time.)

The remainder of this section discusses some of the important reasons that the role of cyberattack in most combined-arms operational plans is inherently circumscribed. A key first step in directing fires is to identify suitable targets. Many kinetic targets are well-known and well-characterized—e.g., military bases, headquarters buildings, ammunition and fuel storage facilities, and telecommunications facilities. Accessing these targets can be planned as routes through three-dimensional physical space. By contrast, many targets in cyberspace appear and disappear from the Internet with the flick of a switch, to say nothing of an access path to them. Even worse, targets that minimize use of networked information technology are less vulnerable to offensive cyber operations. Note that this statement is not synonymous with the use of advanced technology. For example, a Javelin anti-tank missile makes extensive use of digital electronics, but it is not connected to other systems (i.e., it is not networked). Thus, a cyber operation to disable Javelin missiles must be conducted on each individual missile—a daunting task on a fast-moving battlefield.[48]

Matching weapons to targets is an important second step. Compared to kinetic weapons, the effectiveness of a cyber weapon depends heavily on the target's characteristics. Any ship hit by a torpedo with a sufficiently large warhead will be damaged, whether the ship is made of wood or steel. Anything within the crater of a nuclear weapon will be destroyed, regardless of how it was built. A few physical parameters (e.g., target hardness, yield of weapon, distance between point of weapon impact and the target) mostly determine the damage suffered in a kinetic attack. The nature of target-weapon interaction with kinetic weapons can usually be estimated based on physics experimentation and calculation. Most importantly, a sufficiently small but non-zero change in the properties of the target or the weapon generally will result in a small change in the damage inflicted by the weapon.

This is not true for target-weapon interactions in cyberspace, because the alteration of a cyber target by one bit, which is the smallest change possible in a cyber target's characteristics, can completely change the response of the target to the weapon. For example, it may be a one-bit difference in configuration that instructs a targeted system to accept or not to accept data from the Internet. Set one way, a bit can enable an adversary to gain access to the target through the Internet using a particular technique. Set the other way, the use of that technique can be entirely prevented, and thus a cyberattack based on that technique will have no effect at all on the targeted system. In cyberspace, physics and continuous mathematics provide no assistance in calculating or estimating expected effects.

Extreme dependency on small details as to target characteristics has several deleterious consequences that increase the difficulty of making accurate predictions about the outcomes of an offensive cyber operation. For example, in contrast to kinetic weapons, the weapons and capabilities of offensive cyber operations are often customized in detail to the specific target(s) against which these operations may be directed, particularly when precision of attack is needed (for example, to minimize collateral damage). Yet customization generally is time-intensive and technically demanding.[49] Put differently, "off the shelf" weapons and capabilities to support offensive cyber operations are far less available than is the case with their kinetic counterparts.

Intelligence information on target characteristics must also be precise, high-volume, high-quality, current, and available at the time of the weapon's use. For example, key intelligence information may include whether a certain patch has been installed in the target's operating system. Unless the targets of interest have been extensively probed ("prepared") in advance, such detailed information is generally unavailable on a timely basis in a highly dynamic environment, especially in battlefield environments in which individual platforms are online and offline at unpredictable intervals.

Assuming that targets have been identified and offensive capabilities programmed against them, a subsequent step is to conduct the cyberattack. However, two timelines must be compatible if the cyberattack is to be useful. The first is how long it takes for a cyberattack to realize its effects on its target. The second is driven by the overall operational plan, which will often involve other military operations conducted on land, in the air or space, or at sea.

One of the most critical dimensions of an operational plan is proper synchronization of the various activities in the plan, without which the effectiveness of the plan can be significantly diminished. For example, adversary surface-to-air missile sites and radars need to be destroyed or disabled before friendly penetrating aircraft come into range—suppression of enemy air defenses (SEAD) after that point will do much less to enhance bomber penetrativity.

Success rates are quite high for cyberattackers who have the luxury of unlimited time to penetrate a target's cyber defenses, yet no reasonable operational plan allows for unlimited time frames. In addition, the time needed to penetrate adversary defenses is highly variable—it may take a few minutes or many days, depending on the attacker's luck of the draw. While no defense, no matter how strong, can withstand a concerted cyberattack indefinitely, robust defenses can prolong the time it takes for an adversary to succeed. Such delays can upend the synchronization of an operational plan and thereby significantly diminish the impact of cyberattacks.

To reduce time delays and make attack timelines more predictable, would-be attackers often try to prepare a cyber target well before the actual attack, for example, by surreptitiously installing a "back door" that gives the attacker access at a later time. Such access can be used to download a customized attack payload that accounts for new intelligence information becoming available. Advance preparation facilitates prompt access that circumvents the target's cyber defenses, but many targets are not susceptible to being prepared in advance.

Lastly, in contrast to kinetic attacks, the state of the art in assessing damage caused by cyberattacks is still primitive. Damage caused by a cyberattack is usually invisible to the human eye. Returning to the SEAD scenario—if the intent of the cyberattack is to turn off the power to a specific radar installation in the nation's air defense network at a specific time, it will be difficult to distinguish between a successful attack and a smart and wily defender who has detected the attack, shut the power down, and can turn it back on at a moment's notice. By contrast, a radar destroyed by an anti-radiation missile leaves debris scattered about and a smoking hole in the ground, visually confirming a successful attack. Commanders need to know that a SEAD attack was successful, and attacking with an anti-radiation missile is more likely to yield a high-confidence answer than the use of a cyberattack. In integrating cyberattack into combined arms operational planning, commanders must therefore expect greater uncertainty with cyberattacks than with their physical world counterparts, which in turn may cause more reliance on the latter depending upon the mission.

CONCLUSION

The Cyber Peace Institute's timeline of cyberattacks on Ukraine confirmed an uptick in the weeks before the ground invasion began,[50] but these attacks were more or less consistent in intensity and significance to other attacks that Ukraine had experienced over the past several years. By contrast, in the weeks and months before the invasion, Russia deployed unprecedented numbers of troops to Russian-Ukrainian borders. These deployments understandably took center stage in the Ukrainian consciousness, and these troops—rather than the cyberattacks—were widely viewed as the primary element of an attempt to force Ukraine to accede to Russian political demands, such as a change in the Ukrainian constitution to forbid NATO membership permanently. In any event, given Ukraine did not accede to Russian demands, it is fair to say that neither Russian cyber operations nor troops were successfully brandished to achieve a coercive effect on Ukraine.

What about warfighting? How and to what extent, if any, have Russian offensive cyber capabilities improved Russia's ability to degrade Ukrainian military power or effectiveness? There have been no reports of cyberattacks against Ukrainian weapons systems or military command and control systems per se. As suggested above, cyberattacks are less effective against targets in the category of "absolutely, positively must be destroyed or disabled with high confidence and certainty or on a certain timetable."

On the other hand, cyberattacks can be more useful when directed against a target set consisting of many entities, only some of which need to be destroyed or disabled to have a significant effect. (This attack scenario would be analogous to the Nigerian prince seeking suckers who will send him money and sending out millions of emails, knowing that he will make money even if only a very small fraction of recipients responds positively. In this case, the prince does not particularly care who responds, only that some do.) Moreover, cyberattackers who are indifferent to any external timetable can take as much time as needed to obtain results.

The planning and operational coordination of cyberattacks that satisfy the "some out of many" condition above is also much simpler. A relatively simple statement of intent to the cyberattackers likely suffices for command and control—"go forth and damage Ukrainian institutions that provide government, military, and economic functions, that inform the Ukrainian public, or that constitute Ukrainian critical infrastructure."[51] Such cyber operations need not be timed carefully to synchronize with other operations, yet a large number of cyber operations occurring in the same general time frame with a large number of kinetic operations will often result in some of each happening contemporaneously. Thus, it may appear as though cyber and kinetic operations were deliberately synchronized. Many of the cyberattacks conducted against Ukrainian infrastructure in the days immediately after February 24 appear to be of this nature.

It is also noteworthy that the synchronization of cyberattacks with a larger operational plan is not needed; such attacks can be conducted by parties other than Russian military cyber operators. Russian cybercriminal groups are quite capable of conducting such attacks on their own, and should they do so their activities would be largely indistinguishable from those of military cyber operators, at least initially.

Finally, in trying to understand the significance of Russian offensive cyber operations against Ukraine, it is important to keep two points in mind. First, many possible reasons have been offered as explanations for the paucity of Russian offensive cyber operations against Ukraine; others no doubt will be posited in the future. It is almost certainly true that there are multiple reasons for this surprising outcome. Ground truth on the “real” story will be elusive, pending debriefings with senior Russian commanders and other decision-makers (a prospect that does not appear probable any time in the near future).

Second, as of this writing, the war is still going on, it still appears to be indefinite in duration—nowhere near conclusion, and its outcome remains in doubt. If the ground invasion continues to stall, Russia may yet turn to large-scale cyberattacks,[52] either on Ukraine or the West or both, to put pressure on Ukraine for concessions or on the West to cease or cut back on its military support for Ukraine. Such attacks would depend on high-level decisions and resource availability (i.e., tools, personnel, and knowledge/intelligence). At this point, however, it is simply a fact that Western intelligence sources lack insight into what senior Russian decision-makers will choose to do in the future. Thus, conclusions regarding the importance of cyber operations to the conduct of the Russian-Ukraine war are preliminary at best, and generalizations about the strategic utility of offensive cyber operations for coercion are almost certainly premature.

ACKNOWLEDGMENTS

I gratefully acknowledge the assistance of Thomas Berson, Gil Baram, Joseph Nye, Brandon Williams, and two reviewers for commentary on earlier drafts of this paper. Errors and other inadvertent misinformation are my responsibility alone.

NOTES

[1] Maggie Miller, “Russian invasion of Ukraine could redefine cyber warfare,” *Politico*, January 28, 2022, https://www.politico.com/news/2022/01/28/russia-cyber-army-ukraine-00003051.

[2] “Will war in Ukraine lead to a wider cyber-conflict?” *The Economist*, February 23, 2022, www.economist.com/europe/2022/02/23/will-war-in-ukraine-lead-to-a-wider-cyber-conflict.

[3] Nadiya Kostyuk and Erik Gartzke, “Cyberattacks have yet to play a significant role in Russia’s battlefield operations in Ukraine – cyberwarfare experts explain the likely reasons,” *The Conversation*, April 4, 2022, theconversation.com/cyberattacks-have-yet-to-play-a-significant-role-in-russias-battlefield-operations-in-ukraine-cyberwarfare-experts-explain-the-likely-reasons-178604.

[4] Lennart Maschmeyer and Nadiya Kostyuk, “There is no Cyber ‘Shock and Awe’: Plausible Threats in the Ukrainian Conflict,” *War on the Rocks*, February 8, 2022, warontherocks.com/2022/02/there-is-no-cyber-shock-and-awe-plausible-threats-in-the-ukrainian-conflict/.

[5] Andry Greenberg, “Russia’s Sandworm Hackers Attempted a Third Blackout in Ukraine,” *Wired,* April 12, 2022, www.wired.com/story/sandworm-russia-ukraine-blackout-gru/.

[6] Patrick Howell O’Neill, “Russian hackers tried to bring down Ukraine’s power grid to help the invasion,” *MIT Technology Review*, April 12, 2022, www.technologyreview.com/2022/04/12/1049586/russian-hackers-tried-to-bring-down-ukraines-power-grid-to-help-the-invasion/.

[7] Sean Lyngaas, “US Satellite operator says persistent cyberattack at beginning of Ukraine war affected tens of thousands of customers,” *CNN*, March 30, 2022, www.cnn.com/2022/03/30/politics/ukraine-cyberattack-viasat-satellite/index.html.

[8] Kim Zetter, “Viasat Hack ‘Did Not’ Have Huge Impact on Ukrainian Military Communications, Official Says,” Substack newsletter, *Zero Day* (blog), September 26, 2022, https://zetter.substack.com/p/viasat-hack-did-not-have-huge-impact.

[9] Kyle Fendorf and Jessie Miller, “Tracking Cyber Operations and Actors,” Council on Foreign Relations, March 24, 2022, www.cfr.org/blog/tracking-cyber-operations-and-actors-russia-ukraine-war.

[10] Presentation by Rob Joyce, director of cybersecurity at NSA, “State of the Hack: NSA’s Perspective,” *RSA Conference,* San Francisco, June 7, 2022.

[11] Dan Goodin, “Mystery solved in destructive attack,” *Ars Technica*, March 31, 2022, arstechnica.com/information-technology/2022/03/mystery-solved-in-destructive-attack-that-knocked-out-10k-viasat-modems/; “Ukraine: Timeline of Cyberattacks on critical infrastructure and civilian objects,” Cyber Peace Institute, May 12, 2022, cyberpeaceinstitute.org/ukraine-timeline-of-cyberattacks/.

[12] “Ukraine: Timeline of Cyberattacks.”

[13] Valerie Insinna, “SpaceX beating Russian jamming attack was ‘eyewatering’: DoD official,” *Breaking Defense*, April 20, 2022, breakingdefense.com/2022/04/spacex-beating-russian-jamming-attack-was-eyewatering-dod-official/.

[14] “Ukraine: Timeline of Cyberattacks.”

[15] Charlie Osborne, “Ukraine destroys five bot farms that were spreading ‘panic’ among citizens,” *ZDnet,* March 29, 2022, www.zdnet.com/article/ukraine-takes-out-five-bot-farms-spreading-panic-among-citizens/.

[16] David Cattler and Daniel Black, “The Myth of the Missing Cyberwar: Russia’s Hacking Succeeded in Ukraine—And Poses a Threat Elsewhere, Too,” *Foreign Affairs*, April 6, 2022, www.foreignaffairs.com/articles/ukraine/2022-04-06/myth-missing-cyberwar.

[17] “Special Report: Ukraine. An overview of Russia’s cyberattack activity in Ukraine.” *Microsoft Digital Security Unit*, April 27, 2022, query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.

[18] State Service of Special Communications and Information Protection of Ukraine, May 5, 2022, https://cip.gov.ua/en/news/okupanti-shantazhem-i-pogrozami-zmushuyut-ukrayinskikh-provaideriv-pidklyuchatisya-do-rosiiskikh-merezh.

[19] Herbert Lin, “The Emergence of Physically Mediated Cyberattacks?,” *Lawfare*, May 21, 2022, https://www.lawfareblog.com/emergence-physically-mediated-cyberattacks.

[20] Daniel Byman and Matthew Waxman, *Dynamics of Coercion: American Foreign Policy and the Limits of American Military Might* (New York: Cambridge University Press, 2002), 236.

[21] Thomas Rid, “What Would a Real Cyberwar Look Like?” *Slate*, September 15, 2013, slate.com/technology/2013/09/cyber-war-and-cyberattacks-its-really-espionage-subversion-or-sabotage.html; Joshua Rovner, “Cyber War as an Intelligence Contest,” *War on the Rocks,* September 16, 2019, warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest/.

NOTES

22. On the first, see Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," *WIRED,* November 3, 2014, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/. On the second, see Isabel Debre, "Large Cyberattack on Iranian Industrial Sector Targets Three Steel Plants," *Times of Israel*, June 28, 2022, https://www.timesofisrael.com/large-cyberattack-on-iranian-industrial-sector-targets-three-steel-plants/.

23. On economic value, see "The Economic Impact of Cybercrime and Cyber Espionage," Center for Strategic and International Studies, July 2013, http://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf; on intelligence value, see National Counterintelligence and Security Center, Cyber Aware Case Study-Office of Personnel Management, Office of the Director of National Intelligence, https://www.dni.gov/ncsc/e-Learning_CyberAware/pdf/Cyber_Aware_CaseStudy_OPM.pdf; Michael Adams, "Why the OPM Hack Is Far Worse Than You Imagine," *Lawfare*, March 11, 2016, https://www.lawfareblog.com/why-opm-hack-far-worse-you-imagine.

24. Josh Rogin, "NSA Chief: Cybercrime constitutes the 'greatest transfer of wealth in history'," *Foreign Policy*, July 9, 2012, https://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/.

25. See, for example, Robert S. Mueller, III, "Report On Yhe Investigation Into Russian Interference In The 2016 Presidential Election," U.S. Department of Justice, March 2019, Volumes I and II (https://www.justice.gov/archives/sco/file/1373816/download.

26. See, for example, John Popham, "Russia's Failure in Cyberspace," Georgia Institute of Technology, March 10, 2022, www.cc.gatech.edu/news/russias-failure-cyberspace.

27. William Courtney and Peter A. Wilson, "Expect 'shock and awe' if Russia invades Ukraine," *The Hill,* December 8, 2021, https://thehill.com/opinion/international/584805-expect-shock-and-awe-if-russia-invades-ukraine.

28. Joseph Marks, "Here's what cyber pros are watching in the Ukraine conflict," *The Washington Post*, February 24, 2022, https://www.washingtonpost.com/politics/2022/02/24/heres-what-cyber-pros-are-watching-ukraine-conflict/.

29. Joint Publication 3-12, *Cyberspace Operations,* Joint Chiefs of Staff, Department of Defense, June 8, 2018, II-7, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf; Fires refer to the use of weapons systems to create specific effects on a target; See Joint Publication 3-0, *Joint Operations*, Joint Chiefs of Staff, Department of Defense, January 17, 2017, Incorporating Change 1 October 22, 2018, , irp.fas.org/doddir/dod/jp3_0.pdf, III-30.

30. Joint Publication 3-12, *Cyberspace Operations,* Joint Chiefs of Staff, Department of Defense, June 8, 2018, II-6, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.

31. Maggie Miller, "Despite years of preparation, Ukraine's electric grid still an easy target for Russian hackers," *Politico,* February 19, 2022, www.politico.com/news/2022/02/19/despite-years-of-preparation-ukraines-electric-grid-still-far-from-ready-for-russian-hackers-00010373.

32. United States Senate Select Committee on Intelligence, "Hearing on Worldwide Threats," *Committee Hearing Channels,* March 10, 2022, (02:20:41), www.intelligence.senate.gov/hearings/open-hearing-worldwide-threats-2.

33. David E. Sanger, Julian E. Barnes, and Kate Conger, "As Tanks Rolled Into Ukraine, So Did Malware. Then Microsoft Entered the War," *The New York Times*, February 28, 2022, www.nytimes.com/2022/02/28/us/politics/ukraine-russia-microsoft.html.

34. Kara Swisher, "Are We Ready for Putin's Cyber War? I Asked One of Biden's Top Cybersecurity Officials," *Sway, The New York Times*, guest speaker Anne Neuberger, March 10, 2022, www.nytimes.com/2022/03/10/opinion/sway-kara-swisher-anne-neuberger.html.

35. Ellen Nakashima, "U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms," *The Washington Post,* February 27, 2019, www-washingtonpost-com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html.

36. Ryan Gallagher and Bloomberg, "Hackers in Belarus claim to have disrupted trains to 'slow down the transfer' of Russian troops into Ukraine," *Fortune*, February 27, 2022, fortune.com/2022/02/27/belarus-hackers-disrupt-trains-russia-invasion-ukraine-cyber-partisans/.

37. Monica Buchanan Pitrelli, "Anonymous declared a 'cyber war' against Russia, Here are the results" *CNBC,* March 16, 2022, www.cnbc.com/2022/03/16/what-has-anonymous-done-to-russia-here-are-the-results-.html.

38. Kate Conger and David E. Sanger, "Hackers Claim to Target Russian Institutions in Barrage of Cyberattacks and Leaks," *The New York Times,* April 22, 2022, www.nytimes.com/2022/04/22/us/politics/hackers-russia-cyberattacks.html.

NOTES

39. Danielle Kurtzleben, "Volunteer hackers form 'IT Army' to help Ukraine right Russia," *All Things Considered*, NPR, guest speaker Dina Temple-Raston, March 27, 2022, www.npr.org/2022/03/27/1089072560/volunteer-hackers-form-it-army-to-help-ukraine-fight-russia.
40. Maggie Miller, "The world holds its breath for Putin's cyberwar." *Politico*, March 23, 2022, www.politico.com/news/2022/03/23/russia-ukraine-cyberwar-putin-00019440.
41. Chris Krebs, "The cyber warfare predicted in Ukraine may be yet to come," *Financial Times,* March 20, 2022, www-ft-com/content/2938a3cd-1825-4013-8219-4ee6342e20ca.
42. Miller, "The world holds its breath."
43. Insinna, "SpaceX beating Russian jamming attack was 'eyewatering'."
44. Ibid.
45. Ibid.
46. "Cyber-attacks on Ukraine are conspicuous by their absence," *The Economist*, March 1, 2022, www.economist.com/europe/2022/03/01/cyber-attacks-on-ukraine-are-conspicuous-by-their-absence.
47. As one example, Era is a Russian communications system that is designed to provide secure, encrypted communications for personnel on the ground. However, its use requires the presence of an existing 3G or 4G wireless communications network. It is thus unfortunate, from the Russian point of view, that the Russian ground assault destroyed a substantial number of Ukrainian 3G/4G towers, thus forcing Russian soldiers to use less secure methods of communication (Rob Waugh, "'Idiots': Russian military phone calls hacked after own soldiers destroy 3G towers," *yahoo!news,* March 8, 2022, news.yahoo.com/russian-military-being-hacked-after-its-own-soldiers-destroy-3-g-internet-towers-104303881.html.)
48. In principle, a supply chain attack on the digital electronics used in such missiles could be part of an effort to disable them when put into use, but triggering such an attack without real-time access to the missiles would be quite difficult.
49. Steven M. Bellovin, Susan Landau, and Herbert S. Lin, "Limiting the Undesired Impact of Cyber Weapons: Technical Requirements and Policy Implications," *Journal of Cybersecurity* 3(1):59-68, March 1, 2017, https://academic.oup.com/cybersecurity/article/3/1/59/3097802.
50. "Ukraine: Timeline of Cyberattacks."
51. "Special Report: Ukraine. An overview of Russia's cyberattack activity in Ukraine." *Microsoft Digital Security Unit,* April 27, 2022, query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.
52. For example, on April 20, 2022, the cybersecurity authorities of the Five Eyes warned private sector organizations that Russia's invasion of Ukraine could expose organizations both within and beyond the region to increased malicious cyber activity, https://www.cisa.gov/uscert/ncas/alerts/aa22-110a.

Tactics and Technicalities Undermining Strategy: *Cyber Security is Distracting National Security Communities*

Brigadier Martin White

ABSTRACT

National security communities cannot protect all their information. Yet the exigencies of cyber security and identified network vulnerabilities are trumping more strategic consideration of information protection, and national security communities have found it difficult to adhere to clear and defensible information protection principles. A more strategic approach would focus on identifying and prioritizing the most important organizational information; a defense that aligns information security resources to the most important information, with a clear view of the actions needed to protect against the intelligence capabilities of strategic competitors; and, established mechanisms for situations when preventive security measures will so often fall short, which include standing deception plans and well-coordinated reparative measures. Without defensible principles, the immense cyber security investments being made will not have the desired information security effect.

INTRODUCTION

Should national security communities[1] care as much as they seem to about cyber security?[2] The orthodoxy would suggest that this is an absurd question. National governments have habitually accelerated the provision of resources to improve cyber security.[3] Strategic and technical commentary alike define the cyber domain as a central consideration in any notion of success in future conflict.[4] Credible commentators are not questioning cyber security's importance to national security or arguing to limit cyber security resources. More cyber security is the convention. Accordingly, national security communities have made considerable effort to broadly improve cyber security.

Brigadier Martin White is an Australian military officer. He has served in a range of military appointments, including operational service in Timor Leste, Afghanistan, and Iraq. Martin received a Conspicuous Service Cross in 2016, among other awards. He completed his Ph.D. in defence policy and energy security from La Trobe University. The views represented in this article are the author's alone.

Nonetheless, the familiar aphorism "tactics without strategy is the noise before defeat" comes to mind. Traditional national security models that demand high levels of broad information assurance—including of classified information—are becoming increasingly untenable as information becomes easier to disclose. Although it is not specific to a particular national security community or country, a preoccupation with cyber security is analogous (in the contemporary security environment) to a pre-occupation with the tactical and technical aspects of security. This preoccupation has precluded a more strategic concept of protecting the most important information and information links[5]—a nation's Crown Jewels—based on clear and defensible principles. Attention to cyber security is crowding out the more important considerations of how to protect a nation's most important information in the face of an immense contemporary intelligence threat. A strategic approach irrefutably requires extensive cyber security efforts; cyber security is a fundamental technical and tactical tool that is essential for the defense of critical information, but it is not the only tool that is needed. National security communities should look beyond this single aspect, if major investments in cyber security measures are to prove meaningful.

The rapidly changing threat environment has made it difficult for policymakers to enunciate clear and defensible information protection principles. The dearth (in the cyber security literature) of concepts such as: information protection beyond cyber security; senior leaders as the most valuable intelligence targets; the value of deception in defending information during peacetime;[6] the profound vulnerability of classified information to compromise; and the importance of reparative actions as a key and integrated component of national strategies suggests that national security communities are encumbered by the need to address urgent cyber security challenges at the expense of more strategic consideration of information protection.

There are six principles that may contribute to the overall coherence of a national security community's approach to protecting its Crown Jewels. These principles outline the need to clearly identify the most important information; to ensure detailed understanding of all intelligence capabilities used by strategic competitors; and to establish mechanisms to deal with the failure of preventive security measures. The principles are:

1. Cyber security represents a critical tactical and technical tool but should always be framed within a broader strategic concept to protect a nation's Crown Jewels.
2. National security communities must clearly prioritize the information they seek to protect. But even if information protection is done well, a national security community will still only be able to defend a fraction of its information over time.
3. The intelligence capabilities of strategic competitors should be habitually assessed against the protections offered to a nation's Crown Jewels.
4. Senior leaders should be the highest priority for information protection measures.
5. Planned deception measures should be enacted as a standing operation in peacetime, to provide a temporal advantage in the event of a conflict.
6. Reparative arrangements in the aftermath of information compromise should be more comprehensively integrated in national strategies.

Senior leaders should devote less attention to the tactical and technical aspects of cyber security and base their guidance on defining and defending the most important national information using these six principles, where such protection will offer a decisive advantage in the event of conflict.

THINKING LIKE A SPY

1. Cyber security represents a critical tactical and technical tool but should always be framed within a broader strategical concept to protect a nation's Crown Jewels.

Over recent years, national security communities have sought to consolidate their vast numbers of disparate information and computer networks,[7] and to provide greater information security to the military industry.[8] In Australia, the Department of Defence has minimized the number of standalone information systems in operation.[9] More than 700 standalone systems, regularly built by military units who needed to achieve a specific task, were sometimes not maintained with sufficient cyber security hygiene and presented a risk to organizational information.[10] The Department of Defence pursued the closure of these standalone systems as a priority. Progress reports identified the number of standalone systems taken offline as a key metric.

Once the vulnerability was recognized, the efforts to shut down an individual system as soon as possible could be considered quite rational—a systematic solution (a reduction in attack surface, to allow cyber security resources to be more focused) to progressively address a challenging, identified risk. However, when looking at this solution from an intelligence targeting perspective, another view emerges.

If an intelligence collector had identified the Australian military's standalone systems as priority targets, that collector could observe the system closure process. It is reasonable for the intelligence collector to assess that the systems first closed were the easiest to remove from operation. In a process that prioritizes withdrawing individual systems as soon as possible, the first closed systems may well contain the least important organizational information. If the closure of a specific system would negatively impact an important organizational function, that higher priority system would need to remain operational for longer. This simplifies targeting for the strategic competitor, leaving them to take actions such as metadata analysis or exploitation of known software vulnerabilities in order to obtain intelligence. And higher value information was raised in profile because a technical and tactical approach was applied. The standalone systems needed to be closed because of intelligence concerns, yet the likely actions of an intelligence collector were inadequately mitigated.

The simplified risks presented in this short case study are by no means unique to military organizations or to any specific country. Most countries are grappling with the same challenges, often under intense public or political scrutiny. In the rush to enhance cyber security in an immediate and tactical way through decisive actions, it is possible that the actions taken are unintentionally weakening security associated with the most important national information, and do not clearly account for how intelligence collectors operate.

Cyber security is a term used so commonly now that it is often not clear what it encompasses or what it is that national security communities must secure. The 2018 US Department of Defense Cyber Strategy was non-specific, identifying the need to "defend its own networks, systems (and) those networks and systems operated by non-DoD Defense Critical Infrastructure"; that is, virtually everything that might be related to cyber.[11] The term is regularly used with impossibly high criteria,[12] and with non-specific objectives relating to whole-of-organization (or even whole-of-nation) cyber security. National cyber strategies all have excellent intentions, but they consistently try to satisfy many competing priorities, with little sense of what bounds the problem and focuses the resources.[13] And the demand for more cyber resources is relentless.[14]

Of course, definitions and boundaries matter little to intelligence collectors, and they have few concerns about where they get their information.[15] To be sure, cyber operations are very effective because so much information is now digitized. But whether information comes from a cyber-exploitation operation, electro-optical satellite imaging, mobile telephony interception, or human intelligence, is largely irrelevant. In fact, many nations deliberately seek to gain intelligence from a broad range of sources to increase confidence in their assessments. Therefore, actions to pursue cyber security in a manner that is disengaged from the broader problem of information protection would be futile, if other means of obtaining the same information are also available for an intelligence collector.

Further, an intelligence collector would be attentive if their national security target sought to broadly apply cyber security measures across many networks and systems—to seek an average standard of protection for everything—rather than focus security measures on their Crown Jewels. An effort to apply similar levels of information security across many systems may have had some merit prior to the information age, where any intelligence collection was felt to have some value. However, as information has become far more accessible, the greatest intelligence value can be gained by focusing the collection of multiple intelligence assets on the highest value information.

If a national security community is not clear and consistent over time about what its most important information is; has not anticipated seeing much of its classified information compromised over time; and has not protected its most important information in a prioritized way, a concentrated intelligence effort could prove particularly damaging.

Put simply, intelligence collectors will consistently seek the most valuable information for the least effort and will often aggregate a diverse range of collection capabilities to obtain important information. When considering the problem from this perspective, averaging out cyber security resources across many information systems may not be most effective and may even be futile if the highest priority information disclosures can occur through non-cyber collection.

A FAIR GO FOR ALL (INFORMATION)

2. National security communities must clearly prioritize the information they seek to protect. But even if information protection is done well, a national security community will still only be able to defend a fraction of its information over time.

Priorities are inherent in all national security decisions. Senior leaders must constantly make choices that privilege certain missions, agencies or capabilities above others. It is therefore surprising how rarely the idea of information prioritization features in policy and commentary, when commentary on cyber security is so prolific and when information is considered such a strategic resource. Aspects of prioritization sometimes appear, as in the periodic debate about the importance of protecting (or not protecting) metadata. But this is the exception.

Information needs to be prioritized to allow the most important information to be defended. This tenet is not consistently represented in national policies or in cyber commentary. Conversely, equity is often the governing aspect. There is a sense in policy and commentary that all information can be protected or, that national security communities should try to offer near-complete protection. An apparent failure to protect information—even if not of particularly high value—from cyber exploitation is often met with heavy criticism. However, trying to protect all information (including classified information) and mitigate all possible vulnerabilities—either as a deliberate policy or through the inertia of continuing what is already established—will remain prohibitively expensive[16] and will divert resources from the most important areas.

To be sure, official information necessitates a range of technical security measures that demonstrate its priority over information held in the private sector. For example, information classification, the vetting of personnel and physical security measures are long-established methods that demonstrate prioritization of higher-value information is necessary and is important to national security communities. Yet national policies relating to cyber security contain few references to the prioritization of information to defend, and rarely acknowledge that cyber-attack is but one of many vectors that a strategic competitor may use to obtain or disrupt information.

Two recent authoritative national policy documents underscore this point. Neither the 2018 US National Cyber Strategy[17] nor the 2016 Australian Cyber Security Strategy[18] prioritized the most important information as a key aspect of the strategy, nor did either strategy enunciate that cyber-attacks are only one way for a threat to gain information or disable a system. National strategies consistently highlight the growing resources being applied to cyber security[19] however, the magnitude of resourcing is a poor gauge if the protection is not optimized. For instance, Australian national cyber security resources have historically been allocated to respond to "the full range of cyber incidents from national crises to...individual members of the public,"[20] indicating that information is treated equally. This is not consistent with a national policy that prioritizes resources to contend with the most significant threats.

There are often minor references to information prioritization in lower-level technical documentation. For example, the Federal Communications Commission's cybersecurity advice to small business refers to the protection of "critical data."[21] A 2019 Australian Information Security Manual articulated a sub-principle that "the identity and value of systems, applications and information (should be) determined and documented."[22] Such references demonstrate that the concept of information prioritization has been enunciated, but these scant references do not represent a fundamental approach to information security.

Commentators have mostly approached cyber security in a similar way, seeking urgent, broad improvement but with few references to prioritization. Some commentators have argued that certain industries should be prioritized,[23] although national governments are sometimes ambiguous when describing the parts of the economy that constitute critical industries (or perhaps more importantly: what industries are less critical).

A common cyber security metric has been the number of cyber security specialists in employment, with the consistent view that there are too few and they do not have sufficient training.[24] The recruitment of cyber specialists for national security purposes is clearly an important challenge, and most security communities believe their nation needs more.[25] This may well be so. But such discussion must be contingent on the information that must be protected. The necessary size of a cyber workforce will be difficult to quantify until there is a clearer understanding of information protection priorities. Where there are other non-cyber, intelligence vectors where certain information can be compromised, the size of the cyber workforce is only part of a solution. And public debate rarely touches on the need for a workforce to be assigned to other information protection functions, such as mitigation against a strategic competitor's satellite collection; Russian military forces occupying Ukraine may wish they had considered this type of intelligence collection in greater depth.[26]

There are rational explanations for the lack of attention to information prioritization. First, there is a genuine public and political desire for national security information to be more secure, and policymakers do not want cyber-attacks against their national security community to succeed. As a result, some commentators view data loss as a preventable failure.[27] Second, policymakers want to be seen to be listening to and responding to the concerns of all citizens, and many citizens are indeed concerned about cyber security.[28] Stated priorities for information protection could ostracize some parts of the public or the security community. Third, the cyber threat is so immense that it can be difficult to establish a principles-based strategy, as "the urgent" overrides "the most important" and there is a need to be seen responding to all cyber vulnerabilities. Fourth, there is a high level of trust in classified networks because of the additional security measures established within these networks, and this could cause complacency. Finally, there is a degree of faddism relating to the (relatively novel) topic of cyber. Some commentators may profess views while having limited knowledge of the subject. It is also possible that no policymaker wants to be seen to accept a perceived or relative weakening of cyber security, which would occur if some areas were preferred over others.

Ultimately, a lack of prioritization and the belief that any information compromise is bad detracts from the pursuit of a more strategic approach to information protection. A strategic approach would coordinate prioritization of cyber and non-cyber efforts to achieve a credible information defense for a nation's Crown Jewels. This means that other information becomes a lower priority and may be more readily disclosed. National security communities clearly have information and information links that are critical to their business. Whether these information and information links are plans for new military hardware, or specific secure links between intelligence agencies, or a specific highly sensitive mission, national security communities should clearly understand where resources must be applied to optimize information protection.

When nations make immense cyber security investments, they strongly signal that information security is a priority. But if information security truly is a priority, national security communities must focus beyond tactics and technical aspects. They must prioritize the information that must be protected to maintain an advantage in the event of a conflict, then seek to protect these Crown Jewels (through cyber security and through other non-cyber investments in security) against strategic competitors. In this way, nations will consider the intelligence capabilities available to sophisticated strategic competitors.

THE WHOLE TRUTH

3. The intelligence capabilities of strategic competitors should be habitually assessed against the protections offered to a nation's Crown Jewels.

The intelligence threat from strategic competitors is largely a concealed problem. Senior leaders often do not know if intelligence collection against a national security community has been conducted, and the public will know even less. Counterintelligence can also be an expensive and practically limitless undertaking.[29] With so many competing priorities for resources and for senior leaders' attention, few are enthused by the prospect of a largely amorphous and distant problem with challenging metrics and an expensive upkeep usurping what is currently seen as a relatively straightforward (and mostly unquestioned) ability to assign resources to cyber security.

Put simply, why would national security communities make information protection a bigger problem? The answer to this question lies in the intelligence threat that national security communities face from the full range of intelligence collection capabilities maintained by sophisticated strategic competitors. Perhaps most critically, intelligence collection during peacetime has the potential to decisively jeopardize a nation's preferred operating model in the event of conflict.

Most nations need no convincing that their information is targeted by strategic competitors. However, the extent of intelligence collection is rarely fully explained, and the prominence of cyber threats masks a complete view of threats to critical information. Intelligence collection now comprises an immense range of sophisticated capabilities. These include satellite and ground systems;[30] many human intelligence techniques;[31] underwater acoustic collection systems;[32] video surveillance;[33] and, un-crewed intelligence collection platforms,[34] to name just a few.

Underpinning intelligence collection is a range of fusion and analysis capabilities, now enabled by technological advancement in data analytics. Sophisticated fusion and analysis capabilities offer a range of benefits, such as allowing intelligence to be focused against targets of interest and ensuring that data can be quickly aggregated. China's prioritization of "informatized warfare" and of its military Strategic Support Force are examples of national-level efforts to improve information fusion.[35]

The following diagram outlines many of the intelligence collection capabilities that are currently targeting national security communities. Each of these capabilities represents a discrete means to disclose information. And when aggregated against a specific information requirement, it is difficult for a national security community to mitigate, especially over time.

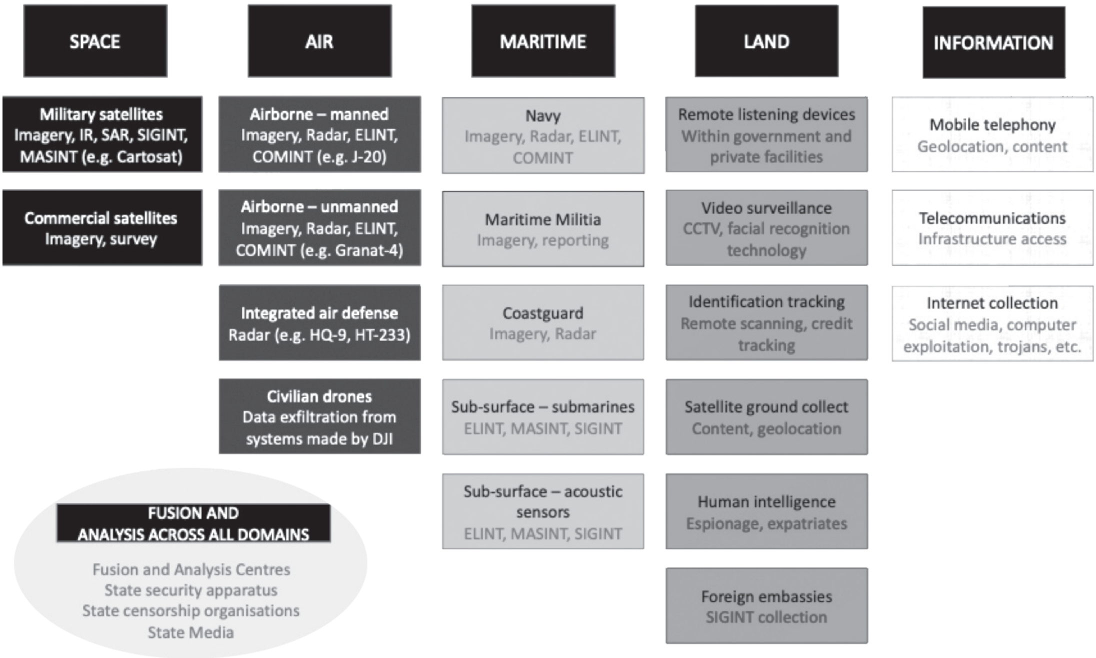


Figure 1: Intelligence collection, by domain

To be sure, every strategic competitor has competing priorities that demand intelligence effort. However, intelligence resources will mostly be concentrated against valuable information targets; particularly national security community targets. If a national security community does not identify and offer adequate and consistent protection against a range of intelligence threats over time, it is foreseeable that the most important information will be compromised at some point or another.

If a national security community does identify its Crown Jewels and seeks to deny access to this information to sophisticated strategic competitors, the information would need to be protected, over time, from all forms of threat intelligence as noted in Figure 1 and not just from cyber exploitation. This is no trivial undertaking. Figure 1 suggests that a strong cyber security capability would only partially protect a national security community's Crown Jewels. Cyber security alone does not mitigate the intelligence threat. Indeed, a nation with strong cyber security but weak security (or unclear security objectives) in other domains invites information theft by herding intelligence collection into its weaker domains. Typically, sophisticated intelligence assessment organizations seek information that has been derived from a range of sources to provide greater validity to their assessments.

Alternatively, nations are not compelled to benchmark against the most sophisticated intelligence threats. There are different levels of information security that a national security community may achieve, and it may be reasonable for senior leaders to pragmatically accept more risk while ensuring information protection against a less sophisticated intelligence threat. For example, senior leaders may accept that sophisticated threat intelligence will gain more information than they would prefer, but establish measures to ensure that terrorist groups are unable to access the personal details of intelligence personnel. Senior leaders regularly make these sorts of risk management decisions across all parts of national security strategies.

But most nations and their security communities have not made this trade-off. Given the considerable investments made by nations in cyber security in recent years, and the strident policy statements outlining the need to mitigate cyber-attacks,[36] one can only conclude that nations have the intention to protect important information from the most challenging intelligence threats. As stated, focus on cyber security does not offer this protection. It makes little sense to invest significantly in cyber security without dealing with the threat to the same information from all types of intelligence collection, or without specifically prioritising protecting the most important information. The broader aspects of information protection (beyond cyber security) are largely absent from the public discourse.

Figure 1 also shows information trends that national security communities must consider. First, there are few geographic and temporal boundaries for intelligence collectors. While some have sought to characterize intelligence collection purely in a conflict context,[37] most of the identified threat intelligence capabilities can be directed towards priority targets at any time. For example, military and commercial satellite collection can often occur anywhere in the satellite footprints and will mostly be conducted outside periods of conflict.

Second, Figure 1 makes no delineation between "private" and "work" communications systems, or between "training" and "operational" communications. If a senior leader uses a personal email account, those communications are considered an equally valid target as an official email account. Training activities are as valid intelligence targets as operational deployments. And a temporary lapse in protection can result in permanent information disclosure.

Third, many of the data sets from individual intelligence collection methods can now be compared to other data sets, offering a range of insight to a strategic competitor that may not even be apparent to the targeted nation. Protecting a small amount of specific information, over a long period of time, is becoming an immense challenge.

LEADERSHIP IS LESS LONELY WITH A CONSTANT COMPANION

4. Senior leaders should be the highest priority for information protection measures.

Intelligence agencies are no different from other organizations in that they seek the greatest possible effect at the lowest cost. It may be a popular mantra that a country like China will focus on a "thousand grains of sand" intelligence strategy,[38] but this surely misses the reality that threat intelligence agencies will seek the most efficient way to access a nation's Crown Jewels.

While sources like insider threats will remain valuable, sophisticated intelligence collection is likely to focus on national security communities via two main vectors. First, intelligence collection will target senior leaders. Second, intelligence agencies will collect massive quantities of lower-value data, on tactical platforms, more junior personnel and communications systems, to undertake big data analysis. The first method is very efficient and may provide authoritative information; the second method will establish correlations that may not otherwise be apparent and can improve a strategic competitor's technological capacity.[39]

Senior leaders can reasonably be considered a rich source of intelligence for a strategic competitor and should anticipate foreign intelligence agencies being their perpetual but unseen attendant. This is because senior leaders handle information that is authoritative, timely, accurate, and distilled. Further, senior leaders are consistently mobile due to the nature of their work. While senior leaders will have access to equipment and training to provide information security, they also often rely on poorly secured communications systems (such as mobile telephones and the internet), effectively voiding some of the established systemic security advantages. Senior leaders also leave lengthy trails of metadata breadcrumbs through their often-extensive communications.[40]

Indeed, there is ample evidence of the problems associated with relying on specific intelligence that is not derived from senior leaders. Secretary of State Colin Powell famously based his 2002 justification for the Iraq invasion on communications intercepts of mid-level Iraqi officers.[41] Subordinate officials will consistently not have the same context or information accuracy as senior leaders. Therefore, targeting senior leaders meets the requirement for intelligence collection efficiency—importance of information, accuracy and timeliness of information, and ease of access.

There is little reference in strategic policy or cyber security literature about the fact that senior leaders make the best intelligence targets, or should be a priority for cyber security. This is a shortfall in the literature which skews the view of cyber security priorities and necessary measures to protect Crown Jewels. While some may argue that it is obvious that senior leaders are a primary target for intelligence, it is difficult to conclude that their information security is consistently prioritized.

National security communities' most important information will be handled mostly by its most senior people. The fact that senior leaders rely heavily on poorly secured communications platforms, thereby negating many of the advantages associated with specific security measures designed for senior leaders, underscores the intelligence opportunity for any strategic competitor. Contemporary cyber security policy and commentary only occasionally emphasize this point. The tactical and technical approach to cyber security has trumped a more strategic consideration of protecting a nation's Crown Jewels.

FOOLING SOME OF THE PEOPLE, SOME OF THE TIME

5. Planned deception measures should be enacted as a standing operation in peacetime, to provide a temporal advantage in the event of a conflict.

Returning to the Australian military's challenging standalone system problem (described earlier), one alternate approach follows. The objective of this alternate approach is to close the systems with higher value information as soon as possible, while using the lower value systems to distract intelligence collectors.

The Australian military will initially leave all of its standalone systems operating, to prevent easy identification of the highest value systems. Over time, some of the systems with the lowest value information will be deliberately made less secure (for example, by failing to patch software vulnerabilities), making them comparatively easier cyber targets. Additional low value or bogus information will be added to the lowest value systems, and these low value systems (and the apparent desire to close them down) will be more widely known by intelligence collectors. In the intervening period, the priority will be placed on hardening the most important standalone systems and getting the information ready to be transferred to a more secure enterprise network. The highest value systems will then be withdrawn, before the lowest value systems.

Such an approach may or may not have been feasible for the standalone system problem. However, the establishment of a credible operational deception plan during peacetime to protect a nation's Crown Jewels and provide a temporal advantage during conflict will often be viable and offer great benefit. In this example, deception measures raise the cyber risk for some lower value systems but reduce the overall enterprise risk associated with the entire standalone system problem. Deception may even turn existing information risk into an intelligence opportunity, as a national security community can monitor intrusions onto the lower value systems.

Even after prioritizing the Crown Jewels and mitigating the specific risks associated with sophisticated intelligence collection, a national security community's information can still be compromised. This is an information age reality. An operational deception plan resourced and conducted during peacetime provides an additional layer of protection to a nation's

Crown Jewels. Such an approach accepts that national security communities must be on an operational footing at all times. Some have termed such a peacetime approach as gray zone operations.[42]

Deception is well understood across national security communities. Some agencies and departments have existing doctrine to leverage. Some of this doctrine identifies the importance of deception to cause an adversary to "squander intelligence assets" and "form inaccurate impressions."[43] If national security communities accept that they cannot prevent a strategic competitor from gaining access to important information at all times, deception offers a second chance to protect or sufficiently obscure a nation's Crown Jewels.

An operational deception campaign should be centrally coordinated and have numerous aims. It may seek to: make certain capabilities appear stronger for deterrence reasons; make it difficult for an intelligence collector to distinguish real information from false information; make certain information more prominent to induce a certain action; limit exposure of certain national capabilities that would be critical during conflict; and confuse a strategic competitor as to who may be a key decision-maker in different situations. Rather than apply deception measures across all information sources, an operational deception plan should be prioritized to deceive intelligence collectors if they gain access to the security community's most important information.

Deception must be coordinated, but it does not demand perfection. In some cases, presenting multiple alternative pieces of information may reveal a deception campaign, but still prevent a strategic competitor from understanding a situation clearly. Deception can also be effective against non-cyber threats; for example, deliberately inserting bogus information onto a government information system may mitigate some of the risk associated with an insider threat (like the case of Edward Snowden) stealing information.

To be sure, deception entails some reputational and operational risks. First, in a society that values transparency and honesty, deception represents a partly conflicting approach. If a security community actor was publicly exposed injecting bogus information onto a government information network, how would this be perceived? Second, if a deception operation is exposed, a national security community may have surrendered information it did not need to give up, or a strategic competitor can view the typical deception activities. Third, if not done properly, there is a risk that the organisation could deceive itself in various ways. However, these risks can be mitigated by using deception measures sparingly and as a second chance only for the most important national security information.

In summary, even if a national security community has prioritized resources to harden its most important information, the most sophisticated information protection measures can sometimes fail. Deception offers a second chance, and the application of deception measures should be prioritized towards safeguarding the highest value information.

PLANNING TO FAIL?

6: Reparative arrangements in the aftermath of information compromise should be more comprehensively integrated in national strategies.

The need to conduct reparative actions and consequence management[44] after a significant information compromise is well known to cyber practitioners but is less prominent in national cyber security strategies. For example, Rothrock argued in the Fall 2017 *The Cyber Defense Review* that an effective plan requires security, but also requires "resilience: the ability to fight back, quickly and effectively."[45] Given the extraordinary rate of information compromises relating to governments and businesses that are identified publicly (and the likely higher number of undisclosed compromises), the paucity of reference to reparation within national cyber strategies (and the disjunction with the known, active approach taken by cyber practitioners to combat cyber security breaches[46]) is curious.

Beyond cyber security, it is common for an organization or government to provide limited detail on how it would manage consequences in the aftermath of a significant incident, when such an incident could be linked to the failure of that organization or government to take sufficient preventive action. Prevention is a predominant policy focus. Road safety is a perfect example: despite Western nations mostly having effective consequence management systems that save lives (such as ambulance networks), road safety strategies consistently do not refer to post-crash actions.[47]

The 2016 Australian Cyber Security Strategy did not refer to consequence management actions in the aftermath of a major information breach. Among more than 30 recommendations, only one touched on post-incident requirements, and even this recommendation adopted an almost exclusively preventive focus.[48] The future requirement for consequence management actions was absent (excluding a reference to the low uptake in cyber insurance), suggesting a limited focus on post-incident considerations in the strategy. Similarly, in the US, the 2018 Department of Defense Cyber Strategy barely referred to consequence management in the aftermath of a breach.[49]

To be sure, there are reasonable explanations for the lack of reference in cyber strategies to reparative actions, even though reparative actions are well embedded in many assessment and response frameworks. First, it is (obviously) better to prevent a negative event than to have to manage its repercussions.[50] Second, strategies consistently adopt a positive focus. If the public is a target audience for a strategy, one aim is almost certainly to instil confidence that the government has the ability to protect its citizens. Third, some governments may prefer to restrict knowledge of their consequence management actions, to prevent cyber-attacks impacting their recovery efforts. Finally, reparative actions in some countries are simply under-developed or even hopefully avoided.

Most of these explanations are unconvincing. Information compromises are so common now that most citizens would expect government departments to have well established clean-up strategies that are fully coordinated with broader strategies. Post-incident actions may be classified, but this would not stop them being referred to as an integral part of a strategy. Reparative actions simply should not be under-developed, given the likelihood of future successful attacks.

Perhaps most importantly, if reasonable security and resilience measures have been taken, a loss of information should not inevitably be viewed as a major failing on the part of the targeted organization. Successful intelligence collection is inevitable. If a national security community has prioritized protection for its Crown Jewels and rehearsed its reparative actions, loss of information may become an annoying reality of life, but will not undermine fundamental operating models.

No one seriously expects that there will not be major compromises of high-value information at future junctures. Without a well understood strategy incorporating information protection and consequence management actions, national security communities could be exposed as much to the post-action repercussions as they are to the actual incident, and unrealistic expectations may be created.

CONCLUSION

The technical and tactical aspects of cyber security are overshadowing more strategic consideration of information protection across national security communities. Indeed, this phenomenon is not specific to any particular security community or nation—it is widespread because there are many pressures and immediate challenges leading to this tactical approach. But as nations face sophisticated strategic competitors, their national security communities must be focused on a more comprehensive approach to protecting their most important information.

If cyber security is indeed a priority, it has presumably been given this priority because there is a need to protect national security communities' information and information links from the most serious threats. If this is true, then a broad effort to achieve wide-ranging cyber security is neither addressing the full problem nor offering an adequate structure for future threats. This impacts the efficacy of cyber security investment.

The recommended principles outlined in this paper may add to the coherence of information security plans and strategies. They are premised on the fact that a nation's key information can now be obtained in many ways, in large quantity, by a strategic competitor. It is hardly an alarmist position to predict that significant information compromises—including of classified data—are likely to occur regularly. Any national security community whose operating model requires protection of certain information for it to be successful must be clear about what its Crown Jewels are; prioritize the protection of those Crown Jewels against specific threat intelligence; enact measures like standing deception plans to limit the benefit a strategic competitor can gain through effective intelligence collection; and develop comprehensive response and recovery plans to enhance resilience in the event of compromises and failures.

NOTES

1. The membership of most national security communities and intelligence communities is extensive. For example, see Office of the Director of National Intelligence, Members of the IC, website, https://www.dni.gov/index.php/what-we-do/members-of-the-ic, accesed une 20, 2020; Australian Government, *Australian National Security*, [website], https://www.nationalsecurity.gov.au/WhatAustraliaisdoing/Pages/NationalSecurityAgencies.aspx, accessed April 20, 2020.
2. Cyber security can be defined as the protection of networks, devices, programs and data from attack, damage or unauthorized access.
3. Department of Prime Minister and Cabinet, Australia's Cyber Security Strategy: Enabling innovation, growth and prosperity (Commonwealth of Australia, 2016), 33; Scott Morrison, $156 million to protect Australians from online attacks (Media Release, April 29, 2019), 1-2.
4. For example, Keith Joiner, "How Australia can catch up to U.S. cyber resilience by understanding that cyber survivability test and evaluation drives defense investment" *Information Security Journal: A Global Perspective* (26:2, 2017), 74-75.
5. Information links refers to networks that transfer data but are not specifically for human-to-human communications to allow the effective functioning of military equipment; for example, the uplink to control an un-crewed aerial system for flight and navigation control. For brevity, 'information and information links' will be described as 'information' in this paper.
6. This paper acknowledges 'peacetime' as a relative concept, blurring the distinction between peace, competition and conflict, but for brevity will use the term 'peacetime' to describe periods where there is no declared conflict.
7. Department of Defense, *DoD Cloud Strategy* (Washington, D.C., December 2018), 1-2.
8. Michael Kansteiner, *Mitigating Risk to DoD Information Networks by Improving Network Security in Third-Party Information Networks* (Monterey, California: Naval Postgraduate School, June 2016), xv-xvi.
9. That is, those information systems not supported as part of Defence's primary enterprise networks such as the Protected Network. See Chief Information Officer Group, 'Our Projects', Department of Defence, https://www.defence.gov.au/CIOG/Projects.asp, accessed November 15, 2019; Department of Defence, Defence Annual Report 2013-14: Volume One (Commonwealth of Australia, 2014), 51.
10. Informatech, *Our Experience*, https://informatech.com.au/projects, accessed November 18, 2019.
11. Department of Defense, Summary: Department of Defense Cyber Strategy (Washington, D.C., 2018), 2.
12. For example, 'to enable all Australians to be secure online,' See Department of Prime Minister and Cabinet, "Australia's Cyber Security Strategy: Enabling innovation, growth and *prosperity*" (Commonwealth of Australia, 2016), 3.
13. President of the United States, National Cyber Strategy of the United States of America (Washington, D.C., September 2018), 1; Department of Prime Minister and Cabinet, Australia's Cyber Security Strategy: Enabling innovation, growth and prosperity (Commonwealth of Australia, 2016).
14. David Barno and Nora Bensahel, "Why the United States Needs an Independent Cyber Force," *War on the Rocks*, May 4, 2021, https://warontherocks.com/2021/05/why-the-united-states-needs-an-independent-cyber-force/, accessed September 25, 2021.
15. Standing intelligence agency rivalries aside; for example, Manoj Shrivastava, Re-energising Indian Intelligence (Centre for Land Warfare Studies, Vij Books, India, 2013), 5; In the Australian context, see Sally Neighbour, "Hidden agendas," in *The Monthly,* November 2010, https://www.themonthly.com.au/issue/2010/november/1289174420/sally-neighbour/hidden-agendas, accessed November 15, 2019.
16. Hervé Debar, "Cybersecurity: high costs for companies,: *The Conversation*, February 4, 2019, https://theconversation.com/cybersecurity-high-costs-for-companies-110807, accessed September 25, 2021.
17. President of the United States, National Cyber Strategy of the United States of America.
18. Department of Prime Minister and Cabinet, Australia's Cyber Security Strategy: Enabling innovation, growth and prosperity (Commonwealth of Australia, 2016).
19. Australian Government, Australia's 2020 Cyber Security Strategy: A call for views (Commonwealth of Australia, 2019), 7-9; the paper referred to essential services as areas of most concern (although only incorporating services such as water providers), and this could be built upon to determine where a priority for information security could be applied.
20. Australian Signals Directorate, Annual Report 2018-19 (Australian Government, Canberra, 2019), 23.
21. Federal Communications Commission, *Cybersecurity for Small Business,* https://www.fcc.gov/general/cybersecurity-small-business, accessed June 1, 2020.

NOTES

22. Australian Cyber Security Centre, *Information Security Manual* (Australian Government, November 2019), 5.
23. Nigel Phair, "Cybersecurity strategy should focus on corporate Australia," *The Strategist*, September 27, 2019, https://www.aspistrategist.org.au/cybersecurity-strategy-should-focus-on-corporate-australia/, accessed November 15, 2019.
24. Inspector General U.S. Department of Defense, Summary of Reports Issued Regarding Department of Defense Cybersecurity From July 1, 2017, Through June 30, 2018 (Washington, D.C., January 9, 2019), 10; AustCyber, Sector Competitiveness Plan – Chapter 3 – The challenge: Australia needs to fill the workforce gap, remove startup barriers and strengthen research and development, https://www.austcyber.com/resources/sector-competitiveness-plan/chapter3, accessed April 20, 2020.
25. Jennifer Li and Lindsay Daugherty, *Training Cyber Warriors: What Can Be Learned from Defense Language Training?* (Santa Monica, CA: RAND Corporation, 2015), 1-3; Greg Austin, 'Cyber revolution' in Australian Defence Force demands rethink of staff, training and policy,' *The Conversation*, July 3, 2017, https://theconversation.com/cyber-revolution-in-australian-defence-force-demands-rethink-of-staff-training-and-policy-80317, accessed November 16, 2019.
26. Mariel Borowitz, 'War in Ukraine highlights the growing strategic importance of private satellite companies—especially in times of conflict', *The Conversation*, August 15, 2022, https://theconversation.com/war-in-ukraine-highlights-the-growing-strategic-importance-of-private-satellite-companies-especially-in-times-of-conflict-188425, accessed September 29, 2022.
27. For example, Ben Fitzgerald, 'Australia needs calibrated deterrence against cyber attacks', *The Interpreter,* December 10, 2015, https://www.lowyinstitute.org/the-interpreter/australia-needs-calibrated-deterrence-against-cyber-attacks>, accessed November 15, 2019.
28. Thomas Daemen, 'Cyber attack fear hinders progress', Microsoft, June 26, 2018, https://news.microsoft.com/en-au/2018/06/26/cyber-attack-fear-hinders-progress/, accessed November 15, 2019.
29. Indeed, the Australian Security and Intelligence Organisation recently argued that there were insufficient resources being applied to counter-intelligence. See Colin Packham, 'Australian intelligence agency wants more resources to counter foreign interference', *Reuters*, October 16, 2019, https://www.reuters.com/article/us-australia-security/australian-intelligence-agency-wants-more-resources-to-counter-foreign-interference-idUSKBN1WW05M, accessed November 25, 2019.
30. Chethan Kumar, 'Surgical Strikes: First major use of Cartosat images for Army', The Times of India, September 30, 2016, https://timesofindia.indiatimes.com/india/Surgical-Strikes-First-major-use-of-Cartosat-images-for-Army/articleshow/54596113.cms, accessed November 1, 2019; Jane's Intelligence Review, *China integrates long-range surveillance capabilities*, 2017, https://www.janes.com/images/assets/477/75477/China_integrates_long-range_surveillance_capabilities.pdf, accessed October 1, 2019.
31. Andrew Greene, 'Chinese spy Wang Liqiang alleges Beijing ordered overseas murders, including in Australia', *ABC News*, November 23, 2019, https://www.abc.net.au/news/2019-11-23/chinese-spy-wang-liqiang-seeks-political-asylum-australia-report/11732174, accessed November 23, 2019.
32. Anthony Kuhn, 'China is Placing Underwater Sensors in The Pacific Near Guam, NPR, February 6, 2018, https://www.npr.org/sections/parallels/2018/02/06/582390143/china-is-placing-underwater-sensors-in-the-pacific-near-guam, accessed October 10, 2019.
33. Pieter Velghe, 'Reading China: The Internet of Things, Surveillance, and Social Management in the PRC', in *China Perspectives* (2019(1), 86; Qiao Long, 'China Aims For Near-Total Surveillance, Including in People's Homes', *Radio Free Asia*, March 30, 2018, https://www.rfa.org/english/news/china/surveillance-03302018111415.html, accessed November 15, 2019.
34. Nikolai Novichkov, 'Russia Creates SIGINT Payloads for Granat-4 UAV', Real Clear Defense, February 17, 2016, https://www.realcleardefense.com/2016/02/18/russia_creates_sigint_payloads_for_granat-4_uav_279172.html, accessed December 3, 2019.
35. M. Taylor Fravel, 'China's "World-Class Military" Ambitions: Origins and Implications,' *The Washington Quarterly* (43:1, Spring 2020), 85-86, 95-96.
36. Sabra Lane, 'AM with Sabra Lane', *ABC News*, December 21, 2018, https://www.abc.net.au/radio/programs/am/we-will-shine-a-light:-tobias-feakin-on-chinas-cyber-spying/10645354, accessed November 15, 2019.
37. Including US assessments, such as Defense Intelligence Agency, "China Military Power: Modernizing a Force to Fight and Win" (DIA-02-1706-085, 2019), 24.

NOTES

38. Sudhansu Nayak, "Few grains from the "Thousand Grains of Sand," Observer Research Foundation, March 8, 2017, https://www.orfonline.org/expert-speak/few-from-thousand-grains-of-sand/, accessed November 20, 2019.
39. David Cooper, *Economic Espionage: Information on Threat From U.S. Allies* (United States General Accounting Office, Testimony, February 28, 1996), 1-2.
40. Damien Manuel, 'Think your metadata is only visible to national security agencies? Think again', *The Conversation*, August 5, 2019, https://theconversation.com/think-your-metadata-is-only-visible-to-national-security-agencies-think-again-121253, accessed May 2, 2021.
41. Joseph Cirincione, Jessica Tuchman Mathews, George Perkovich, with Alexis Orton, WMD in Iraq: Evidence and Implications (, Washington, D.C.: Carnegie Endowment for International Peace, January 2004), 80.
42. Angus Campbell, *War in 2025* (Speech, Australian Strategic Policy Institute International Conference, June 13, 2019), 9.
43. United States Department of Defense, *Military Deception* (Joint Publication 3-13.4, 13 July 2006), vii-viii.
44. Reparative actions and consequence management can include actions such as damage assessments, declassification of information, disposal of hardware, international liaison, media releases and mandatory reporting.
45. Ray Rothrock, 'Digital Network Resilience: Surprising Lessons from the Maginot Line', *The Cyber Defense Review*, Fall 2017, https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/Digital%20Network%20Resilience_Rothrock.pdf?ver=2018-07-31-093725-860, accessed September 25, 2021.
46. For example, see National Cyber Security Centre, *NCSC Cyber Assessment Framework guidance*, 2019, https://www.ncsc.gov.uk/collection/caf, accessed May 2, 2021.
47. For example, J. Wall, J. Woolley, G. Ponte and T. Bailey, "Post crash response arrangements in Australia compared to other high performing road safety nations," Proceedings of the 2014 Australasian Road Safety Research, Policing & Education Conference, Melbourne, November 12-14, 2014), 1-3.
48. Australian Signals Directorate, "Strategies to Mitigate Cyber Security Incidents" (Australian Cyber Security Centre, Australian Government, February 2017), 1-2.
49. Department of Defense, *Cyber Strategy* 2018, 3.
50. Sean Duca, "Cybersecurity: Why prevention is better than the cure," *CEO Magazine*, May 22, 2018, https://www.theceomagazine.com/business/innovation-technology/cybersecurity-why-prevention-is-better-than-the-cure/>, accessed April 20, 2020.

The Cyber Defense Review

◇ Professional Commentary ◇

Cyber-Physical Coordinated Attacks: The Emerging Complexity of Crisis Management

John C. Checco

MULTI-MODAL THREATS

It is conceivable and probable that today's adversaries have contemplated and recruited for event scenarios in which a physical crisis is pre-ignited by a series of more carefully orchestrated cyber incidents. As extremist groups grow bolder and attract younger more technology-astute prospects, there will be a convergence where both logical and physical attacks methods are used in concert towards a singular goal. These will be much more complex and targeted than the typical diversionary tactics we are prepared for today.

This new breed of threat is **multi-modal**; it takes advantage of the operational silos between organizations, whether those are departments within a corporation, supply chains or competitors across an industry, regional government agencies across a nation, or multiple governing nations across a global coalition. Planning such complex executions requires extremely intimate knowledge of the disparate targets and their relationships.

In every sector there are vulnerabilities with the potential to affect both cyber and physical operations. Attackers are connecting the dots to create complex attacks utilizing multiple disparate tactics, techniques, and procedures (TTPs) to amplify overall impact or create cross-sector ramifications.

Relationship Between Cyber and Physical Attacks

Not all multi-modal attacks are the same in purpose and effect. Several specific categories can be defined where cyber and physical threats intersect:

- **Precursor:** This occurs when a party uses cyber-attacks on the infrastructure to prepare a target for a hostile takeover, as in the case of Russia and Georgia in 2008.[1]

John C. Checco is special advisor to the board of the Wall Street Technology Association, past president of InfraGard's NY Metro Chapter and co-chairs the annual NY Metro Joint Cyber Security Conference & Workshop. John currently resides as Resident CISO in Financial Services for a global security platform provider. Prior to this role, he was SVP for Bank of America's Global Information Security Innovation Group; integral in the establishment of their Zero Trust initiative, Responsible Automation guidelines, the Analysis & Resiliency Center for Systemic Risk, and participated in the DHS Loaned Executive Program. John also served as the Senior Information Security and Risk Advisor for Bloomberg L.P. where he introduced the BISO role to their various lines of business. His past experience encompasses emerging technology research and development at NYNEX, Pitney Bowes and IBM. John is a part-time Fire Instructor and volunteer firefighter with special teams training in extrication and dive rescue.

- **Scaffolding:** Similar to the precursor modus operandi, scaffolding attacks disrupt the supply chain for a larger economic and/or operational attack, which may have been the focus of the Colonial Pipeline attack.[2]
- **Direct Diversion:** As a diversionary tactic, a single party initiates a cyber-attack to redirect remediation resources away from a physical target.[3]
- **Indirect Diversion:** in this scenario, the party that performs subsequent cyber-attacks is exploiting the advantage of another party's conflict, as we currently see with several uninvolved nation states increasing their cyber-attacks during the Russia-Ukraine conflict.[4]

It is important to note that not all multi-modal attacks start with a cyber-attack. In the case study on electromagnetic pulse (EMP), it is the physical attack that cripples many electronic capabilities including communications and internet routing devices.

Case Study: The EMP (Electromagnetic Pulse) Threat

The most simplistic explanation of what an EMP attack is: flooding an air space with electrons, so those electrons overload the capacitors and resistors in any electronics device in its path, rendering them inoperable and, in many cases, irreparable. To be clear, an EMP attack is more complicated than a typical blast wave as it generates both short-term (M1) and long-term (M3) effects. To make matters more complicated, EMPs can travel great distances and are frequently created by solar flares, but are protected by the earth's magnetic shield.

This adversarial threat comes in two form factors: (1) detonating a nuclear device at an altitude high above their target, or (2) using smaller devices, known as EMP cannons, to affect a specific facility. The national risk of a major EMP event created by a nation-state actor is considered extremely high impact but low probability. Groups such as InfraGard's National Disaster Resiliency Council (NDRC), Domestic Electromagnetic Spectrum Operations (DEMSO) and the Energy Information Sharing and Analysis Center (E-ISAC) are focused on electromagnetic pulses as a disruption path to any target dependent on the resiliency of the electrical grid.[5]

Resiliency against EMP events is not simply an energy sector issue. During an EMP attack, the consumers of energy are most likely not protected. Where will power facilities be delivering energy? The prediction is that industries such as agriculture, food supply, transportation, communications will only be able to operate at 10% capacity over an 18-month period.[6] It has been estimated that a power generation facility that has 10% resiliency can still generate about 80% of the power needs it serves.[7] Preparation is key, because the low probability of an attack still includes both man-made upper atmospheric nuclear detonation[8] as well as the natural solar flare, such as the Carrington event of 1859.[9]

Beyond using EMP to disrupt technology and operations, high-value human targets are at risk. There is circumstantial evidence pointing to suspected localized low energy pulse attacks against US government employees both abroad (Cuba,[10] Guangzhou[11]) and domestic arenas.[12]

Cross-Sector Affectation & Scaffolding Dependencies

An attack in any one of these categories would leave the targeted region extremely vulnerable to physical attacks. In many cases, a primary cyber-attack is used to simplify the secondary physical attack methods, as, after a cyber-attack, the normal protectors for minimizing physical damage have been significantly diminished.

Scaffolding dependencies, whereby the success of a high-level complex operation relies on the continued sustenance of one or more lower-level operations, further complicate matters, as indirect and/or collateral damage may far outweigh any direct destruction as direct effects tend to be acute while collateral effects are often long-lasting.

The Roman Empire & Kill Chain

A documentary about the technologies of the Romans[13] shows they were the most advanced civilization of their time. Several distinct innovations, each one dependent on the prior success, were key to their success:

1. The formulation of **marine concrete**.
2. Architectures using **arches and domes** using custom-formed blocks of concrete.
3. Water **aqueducts** built using arches, for irrigation as well as waste removal.
4. Utilizing water flow to power massive **grain milling operations.**
5. Prioritizing **food supply** to keep armed forces healthy.

This combination of innovative technologies that supported each other came about because of astute governing concepts and sustained a highly advanced civilization. If any of these tenets did not exist, or were disrupted, then their society would not have survived.

Eventually, the Roman Empire fell due to what today we call the kill chain, the disruption of an entire operation by simply destroying one of its dependencies.

Similarly, the Food & Agriculture sector is one of the only sectors that is dependent on the remaining fifteen sectors as defined by the US DHS, as identified by the National Disaster Resilience Council (NDRC).[14]

Industry Vulnerabilities (capable of multi-modal affectation)

In each sector, cyber threats have the potential to affect physical and downstream operations exist. Understanding where these vulnerabilities are and where cyber-attacks can be used for amplifying incidents where cross-sector ramifications are far greater than its parts is crucial.

Banking & Financial Services

The banking and financial services industry experiences persistent direct attacks against components such as consumer bank accounts, ATMs, and institutional payment systems. There are many scenarios where cyber events seek one or more of the following situations: (a) financial gain from playing a series of long or short market positions, (b) retribution against a specific public company or the financial institutions themselves, or (c) disrupting the economy on a national or global scale regardless of any financial gain.

The unintended applications of a technology can lead to more systemic events, whether through intentional misuse (for example, the utilization of cryptocurrency to bypass sanctions[15]) or, exploiting the lack of operational guardrails preventing runaway execution such as automated high frequency micro-trading which resulted in the Flash Crash of 2010.[16] Since this 2010 economic event, regulations have been introduced to automatically halt trading to prevent spiraling of the stock market.

SWIFT Protocol Abuse

According to security threat intelligence vendor F-Secure, SWIFT is characterized as an easily exploited technology:

> Attackers realized that focusing on low profile, calculated, and sophisticated attacks on financial institutions has the potential for a much higher gain and requires less overall effort than continuously targeting individual customers. There have been at least eight high-profile attacks on SWIFT systems over the past five years (among many other lower-profile attacks), all resulting in significant financial loss.[17]

Fake News/Alerts

Fake news, especially rampant across social media channels, has played directly into moving economic markets and allowing threat actors to capitalize on that market response. As CNBC reported:

> The FBI and SEC are to launch investigations after more than £90bn was temporarily wiped off the US stock market when hackers broke into the Twitter account of the Associated Press and announced that two bombs had exploded at the White House, injuring Barack Obama.[18]

Automated (unsupervised) High Frequency Micro-Trading

A noted analyst from JP Morgan warns about the exponential rise of HFMT, the automated technology that caused the Flash Crash of 2010:

> Automated trading strategies are programmed to automatically sell into weakness. Together, index and quant funds now make up as much as two-thirds of assets under management globally, and 90 percent of daily trading comes from those or similar strategies.[19]

Cryptocurrency as a [Financial] Weapon

Morgan Wright, reporting from The Hill, "Iran is doing what every respectable state sponsor of terrorism does when their economy is going down the drain. They turn to bitcoin. Just like North Korea did (and still does)."[20] A senior Iranian official confirmed: "[Crypto]currency would facilitate the transfer of money (to and from) anywhere in the world ... It can help us at the time of sanctions."[21]

Blockchain Weaponization

The [pseudo-]anonymity of cryptocurrencies could also be used by those same nations to financially support and arm terrorist groups, acting as an underground payment system "in plain sight" with attribution capabilities by our cyber-defenses limited to coalescing disparate crypto-wallets;[22] but really having no other actionable remediation.

> National security experts are warning about cold-war type scenarios where the blockchain and cryptocurrencies are weaponized to illicit ends and governments (such as North Korea) can use it to evade sanctions and unleash an era of financial warfare.[23]

Public Utilities / Infrastructure

The utility sectors are similar to banking and finance since they serve the public at large, and most citizens will be affected by downed utilities. We have seen explicit attempts to obstruct energy production, specifically with the advent of StuxNet. Industrial control systems (ICS) are the computer control systems for managing one or more physical devices. Many times, these devices have embedded ICS consoles. The systems that aggregate and maintain large sets of devices via ICS are known as supervisory control and data acquisition (SCADA) systems.

In assessing the risks within ICS/SCADA systems, two characteristics need to be considered: threat type and location sensitivity.

- **Threat Types**
  - **Operational** threats have an immediate impact on business with little to no warning, and should be considered a significant risk to the organization.
  - **Targeted** threats are those that have a specific goal on altering business operations, critical data exfiltration, and/or holding entities at risk by embedding and burrowing until C2 actions are taken.
  - **Indirect** threats are characterized by disrupting ancillary operations, such as disabling the physical access control systems.
- Location Sensitivity
  - **Tier 1** facilities are critical to daily operations of the business.
  - **Tier 2** facilities can sustain short-term outages without affecting critical areas of operations.
  - **Tier 3** facilities do not affect short-term operations, but may have longer-term impacts.

Historically, different reporting lines are responsible for different systems; thus, there are inconsistent levels of protection across these systems.

> Many of the computers controlling industrial systems are old and predate the consumer Internet. Companies, against the advice of hacking gurus, increasingly brought them online in the past decade as a way to add 'smarts' to U.S. infrastructure. Often, they are connected directly to office computer networks, which are notoriously easy to breach. America's power grid, factories, pipelines, bridges and dams—all prime targets for digital armies—are sitting largely unprotected on the Internet.[24]

Transportation

As far back as 2016, a Booz Allen Industrial Cybersecurity Threat Briefing has predicted what we are seeing today, "New targets, including light rail operators, and new tactics such as supervisory control and data acquisition (SCADA) access as a service (SAaaS) and ransomware against ICS, are likely to emerge and expand."[25]

Water Utilities

Various events have targeted water sources and water treatment plants over the decade:

2013: "Iranian hackers infiltrated the control system of a small dam less than 20 miles from New York City two years ago, sparking concerns that reached to the White House."[26]

2017: "An unnamed water district, dubbed the Kemuri Water Company (KWC), experienced unexplained patterns of valve and duct movements over at least a period of 60 days."[27]

2021: "Hackers remotely accessed the water treatment plant of a small Florida city last week and briefly changed the levels of lye in the drinking water, in the kind of critical infra structure intrusion that cybersecurity experts have long warned about."[28]

Electric Grid

James Heyen's research identified increased threats against the electrical grid in times of disruption. "Following the [U.S.] Northeast Blackout of 2003, there was an uptick of scanning by rogue actors for weaknesses in many industrial control systems."[29]

Smart Cities

Even as our traditional city infrastructures are under attack, Smart Cities are gaining national momentum as a playground for technology innovation and experimentation. Yet only a handful of groups are addressing the cyber and physical security needs for protecting these cities' infrastructures which are inevitably an entirely new attack surface for predators. 30

> The increased complexity of city's systems, interdependencies, globally connected social, economic and political sub systems has increased the vulnerability of a city's security. The interface between urban growth, technology, infrastructure and capital requirement presents a unique set of opportunities and challenges to the implementation of Smart cities.[31]

Any one of these scenarios would leave the targeted region extremely vulnerable to physical attacks. In many cases a primary cyber-attack simplifies secondary physical attack methods, as the normal protectors for minimizing physical damage have been significantly diminished: "Los Angeles, Houston, Chicago, and Dallas each had more than 2 million exposed cyber assets that make them vulnerable to exploitation and compromise."[32]

After the financial sector, the energy sector has been the most aggressive industry in the cyber and physical security arena and has focused on many critical infrastructure impacts from EMP (electromagnetic pulses) to better information sharing amongst the various ISACs under the GRF/EASE initiative.

> ISO/IEC 30182:2017 describes, and gives guidance on, a smart city concept model (SCCM) that can provide the basis of interoperability between component systems of a smart city, by aligning the ontologies in use across different sectors.[33]

Commercial Facilities

Compared to energy and other public infrastructure, risks to commercial facilities ICS/SCADA components exist as well. The attackers' TTPs (Tactics, Techniques and Procedures) are similar, but the risk and response plans are governed by individual private entities—corporations, landlords and/or facility management firms. Threats to commercial facilities fall into two major areas: direct breaches of systems, and exploitation of organization procedure weaknesses.

> One international law enforcement agency estimates that victims lose about $400 billion each year worldwide—making it a bigger criminal enterprise than the global trade in marijuana, cocaine and heroin combined.[34]

Many differing guidelines exist for creating defense-in-depth with such networks, even to the point of isolated network systems separating BMS/SCADA from internet-facing corporate networks. Existing data centers and facilities cannot feasibly migrate to air-gapped isolation as it would require:

- Significant resources in standing up a new network infrastructure;
- Whitelist-based point-to-point routing rules (possibly breaking current operations);
- Separate consoles for accessing BMS and corporate systems;
- Disconnection of BMS data into existing logging/monitoring tools (on the corporate network);
- Disablement of remote manufacturer direct access to BMS systems (perhaps a good thing);

Aviation

The Aviation ISAC (A-ISAC) encompasses six different aspects of the industry: airlines, airports, platforms, satellites, engines, and equipment manufacturers.[35] Regrettably, each operates in its own lane with regards to tabletop exercises and cross-functional potential events. Conversely, there is no overriding authority for managing the entire sector: terminals are owned/operated by the regional authority, logistics (parking, food, et al) are consigned services, airlines rent gate space, airplane manufacturers are not directly involved in daily flight operations, and security (TSA, FAA, or other) is an isolated resource.

The International Air Transport Association (IATA) is a trade association representing ~300 airlines and over 80% of total air traffic.[36] "IATA has a list of recommendations to address present and future aviation threats including a focus on the universal implementation of global security standards, effective information-sharing among governments and with the industry, sustainable risk-based security measures, and emerging risks."[37]

The International Civil Aviation Organization (ICAO) has a Global Aviation Security Plan (GASeP) "provides the foundation for States, industry, stakeholders and ICAO to work together with the shared and common goal of achieving five key priority outcomes: (1) enhance risk awareness and response, (2) develop security culture and human capability, (3) improve technological resources and innovation, (4) improve oversight and quality assurance; and (5) increase cooperation and support." [38]

Many attacks in the air transportation industry were preceded by the ability to physically bypass existing security checkpoint systems. Using cyber-attacks to bypass security checkpoints opens up an entirely new set of attack surfaces.

Passenger/Reservation Systems

The lowest hanging fruit in the air transportation sector is the ability to manipulate the airlines' corporate and operational systems by manipulating flight reservations and passenger identities.

> Air Canada said that it detected unusual login activity … It is possible to use the [exposed] information to obtain genuine documents such as driving licenses and new passports.[39]

Airplane Scheduling Systems

Airlines use the concept of day-bedding for ensuring the maximum number of flights in/out of multiple airports. With the airlines, one's departing flight is directly dependent on another's incoming flight. When operated properly, this prevents the need for any airline to have planes in the hangar thereby reducing costs. However, when it fails, the cascading affects can be global: "Four air carriers now control approximately 85 percent of domestic capacity. All it takes is one airline to experience an outage and thousands of passengers could be stranded."[40]

Baggage Handling Systems

It is surprising to know that not all bags on commercial airlines are scanned. There exists the distinct possibility that the baggage handling systems can be hacked to bypass scanning based on certain tag number formats or baggage attributes.

> The six typical vectors for introducing explosives are: passengers (on person); passenger carry-on baggage; passenger checked baggage; cargo originating from known, unknown, or consolidated shippers; courier bags; and mail. More subversive vectors include crew members (e.g., pilots or flight attendants); an intentional or accidental security bypass; food catering service or meal cart; duty-free items; cleaning crew; and service crew (e.g., mechanics, fuelers, baggage handlers). To prevent the introduction of an explosive, all of these vectors must be secure.[41]

X-Ray / Passenger Inspection Systems

X-Ray passenger inspection systems suffer from a variety of limitations such as the following:

- **Missed identifications** are commonplace due to opaqueness, clutter and similarity of consumer electronics to detonation devices. "No security X-ray system has yet been produced that can make autonomous decisions for acceptable and reliable threat detection. All still heavily depend on human operators to view and interpret the images."[42]
- **Screening Avoidance** such as the recent trend surrounding weapons made of non-detectable materials. "The Liberator, Wilson's plastic pistol, would contain a 6-ounce piece of steel that can be removed, raising the possibility that walk-through metal detectors would not detect the guns."[43]

Healthcare / Medical

The healthcare sector reformed the security system with HIPAA (Health Insurance Portability and Accountability Act) in 1996 and HITECH (Health Information Technology for Economic and Clinical Health Act) in 2009. HIPAA requires better protecting patient information, while the HITECH Act requires that all medical records be in electronic form. Yet, no standard format was defined for electronic health records. Because the electronic data is not normalized, this lack of standardization leads to more cases of medical identity fraud and misdiagnoses. Normalization is the process of restructuring relational data to reduce data redundancy and improve data integrity. Having multiple unsynchronized instances of the same patient and medical data creates a broad attack surface ripe for unauthorized modification and abuse.

> A hospital employee snooped on patients' information for 14 years before the breach was discovered. The breach affected 1,100 patient records and remained undetected until one of the patients called in with a complaint.[44]

Misdiagnosis/Death from Patient Identities Fraud

There are two serious scenarios that occur from such disarray:

- **Medical Identity Theft**

  Some (mostly low-income) families or communities will reuse the identities of family members who have health insurance to piggyback on their insurance plans. This is unhealthy to all patients using the same identity, as the medical history does not accurately reflect any single patient and a rogue patient may be subject to undue medications and treatments.

- **Misdiagnosis/Mistreatment Against a Target**

  This more nefarious scenario would be a cyber-attacker altering the medical history of a target to create a situation where an improper medication/treatment is given to the target, resulting in death. The number of healthcare data breaches have been growing exponentially annually.[45]

Death from Manipulating Devices

Similar to the scenarios above, medical devices can be directly hacked to achieve a similar outcome. Medical devices including pacemakers, heartrate monitors, MRIs, and Insulin pumps have been found to be exploitable with potentially deadly results. 46 As new exploits are found in medical devices, a volunteer group known as I Am the Cavalry works to identify, address, and assist medical device manufacturers/facilities in remediating issues.[47]

> Every single medical device that is connected to a network is a breach opportunity. Put another way, every single medical device that can be operated remotely presents unthinkable possibilities.[48]

Healthcare is a fragile target, as there is an imbalance between keeping critical medical devices secure (patched) versus keeping them operational.[49]

Telecommunications/Internet

There are espionage cyberattacks on many of our legacy communications systems to garner information about operations and targets for further attacks. These include, but are not limited to:

SS7 Vulnerabilities

Signaling System 7 (SS7) was developed in the 1970s as a method to coordinate and route calls across the Public Switch Telephone Network (PSTN). The notion of secured communications was not a concern in the 1970s, and SS7 is vulnerable. Even as more varieties of newer technologies (ISDN, xDSL, Ethernet) were invented, SS7 remained the primary one in use and securing communications that happen on this platform is inconceivable due to the sprawl and impact area for changing (breaking) the protocol. What we are left is a legacy protocol that was never meant for arbitrary inline inspection as it runs over transports that are designed to allow unrestricted and anonymous tapping of information flow almost anywhere in the communication flow.

> Cyber criminals exploited SS7 flaws to intercept two-factor authentication codes (one-time passcode, or OTP) sent to online banking customers and drained their bank accounts.[50]

SIP Abuse

Session Initiation Protocol (SIP) is one of the modular capabilities added onto SS7 to allow customer premise equipment (CPE) such as PBX systems to provide endpoint identification to the switch network. Prior to this, switching systems relied on massive telecommunication databases to convert complex circuit numbers and trunking information to be translated to actual phone numbers.

As originally designed, SIP allowed arbitrary injection of metadata into the signaling layer, without any consideration for misuse; the engineering assumption was that all endpoint devices (CPE) would properly identify themselves. Although SIP was created to fill a deficiency in SS7, it is now widely used for cellular networks as well as internet traffic; allowing indiscriminate devices to identify themselves without any endpoint authentication or verification.

As a result, we are in a situation today where phone number spoofing is rampant, and call-blocking does not prevent the true call originators. More disturbing is how internet providers are utilizing SIP for VoIP protocols.

> Because VoIP is not inherently tied to a particular location and often provides access to multiple phone numbers, it provides a level of anonymity that allows subscribers to mask their identities as well as the physical locations. The relative ease of access to and the ability to veil location and identity through VoIP networks provides ample opportunity for misuse and furtherance of illegitimate goals.[51]

Border Gateway Protocol (BGP) Hijacking

BGP routers are the road signs that allow internet traffic to find the shortest open path to its destination. However, if the communication stream were diverted to take an alternate route—one that allows the traffic to be captured and analyzed without the knowledge of either the sender or receiver—then even encrypted sessions (prior to TLSv1.3) could be decrypted offline and its information used for future cyber and physical attacks.52 Such is the case in a BGP attack, and it is not as uncommon as it first may seem.

> Routers rely on the BGP to puzzle out the best route between two IP addresses; when one party advertises incorrect routing information, routers across the globe can be convinced to send traffic on geographically absurd paths.[53]

BGP hijacking has been an ongoing attack vector resulting from conflicts, espionage, and misconfigurations. Some of the most notable incidents are: 2022 (Ukraine[54]), 2019 (EU/China[55]), 2018 (Nigeria/China[56]), 2017 (US/Russia[57]), 2015 (Malaysia[58]), 2014 (Russia/China[59]), 2013 (Iceland/Belarus[60]), 2010 (Worldwide/China[61]).

Telecommunication Security

Unfortunately, little effort exists to provide technology protections to areas such as SS7 and SIP. All efforts have been limited to laws enacted against fraudulent identity activity or misrepresentation[62]. But this has an obvious conundrum: How does one report a fraudulent identity? Reporting the false SIP information (i.e. Caller-ID) does not provide any attribution towards the true actor – especially if the SIP being used is your own phone number.[63]

Internet Communication Security

There have been many efforts to secure internet communications:

- **DNSSEC** *"DNS data itself is [cryptgraphically] signed by the owner of the data."*[64]
- **BGPSEC** *"Each hop in the [routing] path now protected with a signature."*[65]
- **TLSv1.3** *"Renegotiation is not possible in a TLSv1.3 connection."*[66]

As a matter of reference, DNSSEC has been around since 1997; BGPSEC was introduced in 2000 and yet neither has a significant adoption rate.[67]

MANAGING THE COMPLEX THREAT LANDSCAPE

The most common issue in organizations is a gap in proper delineation of responsibilities, which leaves them vulnerable to internal and external threats. This will culminate in the orchestration of cyber and physical tactics for a single terrorist objective. It is the precursor to more advanced and complex threats; some scenarios even seemingly unfathomable. Make no mistake; multi-modal attacks are certainly in our future. The end goal here is to gain situational awareness and prepare for any invocation of these complex threats.

Sector-Independent Coordinated Collaboration

One aspect that should be addressed globally is the inter-dependencies of sectors. Each sector has its own Information Sharing & Analysis Center (ISAC),[68] but they are not perfect in sharing IOCs (indicators of compromise) or attack TTPs (tactics, techniques, and procedures). The issue of sharing data in an ISAC is not always the same. Some examples of disparate sharing are:

- The **Energy Sector** is divided into several distinct ISACs: Electricity (E-ISAC,[69] Oil & Natural Gas (ONG-ISAC,[70] Downstream Natural Gas (DNG-ISAC),[71] Nuclear Energy Institute (NEI, [72] and Energy Analytic Security Exchange (GRF/EASE[73]). The Multi-State ISAC (MS-ISAC[74]) attempts to resolve this issue by sharing data from across these other ISACs.
- The **Aviation Sector** ISAC (A-ISAC[75]) combines several disparate sub-industries under the same umbrella: airlines, airports, platforms, satellites, engines, and equipment manufacturers. Many times, the data presented is not relevant to more than one of those six categories thus, it inadvertently creates a high noise-to-signal ratio, making focused analysis very difficult.
- The **Financial Sector** ISAC (FS-ISAC[76]) has a slightly different issue; the ISAC consists of many major financial firms as well as a myriad of much smaller financially focused organizations. Although IOCs and TTPs are shared, it is usually latent reporting. In some cases, an organization would not report the attack at all, except for legal notification, as it may bring undue attention to reputational risks and regulatory audits.
- The **Analysis & Resilience Center for Systemic Risk**[77] has been one successful model for a multi-sector targeted mission to identify systemic risks to any critical infrastructure.
- **InfraGard**, an FBI outreach program through their Office of Private Sector, focuses on both cyber and physical threats across U.S. critical infrastructures.[78]
- **ASIS International**, traditionally a physical security organization, expanded its focus in 2016 to include cybersecurity.[79]
- **DHS/CISA** created a shared collaboration space in 2018 for their NCC physical security watchdogs to work alongside the CISA cyber security watchdogs.[80]

Crisis Resource Management & Cybersecurity Frameworks

The FAA, in response to the crash of United Airlines Flight 173 on December 28, 1978, developed one of the first critical thinking guidelines for crisis management. Originally known as Cockpit Resource Management, this process is integrated by many emergency services into their Incident Command System.[81] One aspect of this guideline that applies to any group of decision-makers is the use of the three decision outcome avenues.[82]

- **Avoid:** plan to prevent possibilities of a crisis.
- **Trap:** recognize bad decisions and fix potential problems before a crisis.
- **Mitigate**: minimize the negative effect during a crisis.

It is important to note that whenever an unexpected/unplanned event occurs that requires the use of this catch-all activity, an investigation post-crisis is necessary to review and codify the event handling procedures for future possible incidents.

This concept of "decision outcome avenues" applies directly to information security planning. It has been expanded by the National Institute of Standards and Technology (NIST) into the formal Cyber Security Framework (CSF) as: Identify, Protect, Detect, Respond and Recover. The NIST CSF paradigm has advanced in several ways; most significantly to include the Cyber Defense Matrix [83] authored by security researcher Sounil Yu. Although originally designed to assess the security coverage provided by technology, it can also be used to assess potential scaffolding impacts. To augment the NIST CSF tenets, I would boldly venture to add a far left tenet of **Preempt** as a security strategy positioned to the leftmost pillar. The concept of Preempt would be to remove the attack surface itself, thus eliminating the capability of a threat actor to operate.

An example of preempt is the use password compromise. In the Identify stage, one can list a myriad of vulnerabilities and weaknesses with their organization's password policies and technologies. Consequently, a Protect plan would define password controls, such as stronger patterns or shorter password rotations. The Preempt principle, however, would take an alternate approach by implementing passwordless authentication using FIDO/2, transferring first-stage biometric authentication to the verified end-user device. [84] Organizations should utilize both the crisis management plan and defense framework in concert to build a more holistic preplan of managing the unexpected multi-modal incident.

Managing [Crisis] Without Authority

Marine Corps LtCol (Ret.) Robert J. Darling has defined a crisis management roadmap, which was originally designed for smaller organizations, for building resiliency plans against both physical and cyber threats. [85] Promoted as the mnemonic: **Start, Doing, More, To, Live!**™. This method breaks down crisis management into five distinct actions that can be performed by anyone at any level of the organization.

- **Sensing:** refers to one's situational awareness to recognize an unfolding crisis. Examples of this are communication loss, erratic operational performance, upstream issues, or proximal events where proximity refers to either physical (locale) or logical (technology stack).
- **Decisioning:** defines the crucial initial steps once a crisis event has been recognized. This unfolds into two stages: Assuming Leadership and Triaging the immediate situation.
  - **Assuming Leadership:** requires the mindset of preparing to take control as well as ensuring you can display the proper demeanor that allows you to take control.
  - **Triage**: implements initial short-term actions to address the immediate dangers, with a focus on four specific aspects: Prioritization, Control Awareness, Direction, and Response.
    - a) ***Prioritization:*** is the foremost activity for triage determining the order of operations, coarsely categorized as: Life, Safety, Property and Exposures. Life can be further broken down into concentric circles of preservation: self, team, affected victims, clients/customers, bystanders and finally everyone else.
    - b) ***Control Awareness:*** is identifying which attributes of the situation can be controlled and which are out of your control.
    - c) ***Direction:*** defines the guardrails for a proposed action plan.
    - d) ***Response:*** is coalescing all the information gathered up to this point into a structured plan of action, addressing a priority which you can control, understanding any ramifications of decisions. Note that, although you want to focus on things directly within your control, you never discard what is out of your control but rather park it as observe-and-report.
- **Making:** is the act of moving forward with purpose. This is the outward display of assuming leadership, but to be effective, you also need to be very structured in your approach:
  - **Know Your People:** Take the time to determine their capabilities and expertise as well as their willingness to assist. Assigning the right people to the right task is as important as the task itself.
  - **Define a series of RPOs (Recovery Point Objectives):** Break down any large plan into a series of smaller achievable milestones. Bystanders who are inadvertent participants[86] can achieve better results without being overwhelmed by the enormity of the situation.
  - **Scale In-Band Operations (Business Continuity):** Among any response is to work within your control, which typically means to focus on what the team knows best within their existing roles.

- **Implement Out-of-Band Operations (Emergency Response):** For those tasks that are outside of the normal working roles, a leader must determine and convince the most capable persons to assist in handling those non-traditional tasks. This is never an easy decision. Sometimes the best person for an out-of-band task is also the best person for an in-band task. Other times, someone with the expertise does not have the willingness to step out of their comfort zone.
- ***If All Else Fails*** ... Apply the tenets of Avoid/Trap/Mitigate. Control what you can; minimize the impacts of what you cannot. Do not try to focus on what you cannot affect.

- **Terminating:** includes understanding the conditions where emergency operations can be concluded. Similar to Sensing where situational awareness is used to define abnormal conditions a leader needs to use that same awareness to: (1) establish criteria for **Normalcy,** (2) determine conditions that warrant an **RTO** (return to operations), (3) specify tasks for **Salvage** and cleanup, and (4) take explicit actions to demonstrate that they **Relinquish Leadership.**
- **Learning:** is the continuous iterative process of review during and after the incident. It is comprised of: (1) interim debriefing sessions, (2) introspection as well as peer evaluation, (3) improvement of the decision-making processes, and (4) commitment to instantiate changes.

This method has proven effective for many types of multi-modal events (cross-sector, cyber-physical and scaffolding).

Non Sequitur

We should also be aware of three pitfalls with this topic: tunnel vision, apophenia, and bias.

- **Tunnel Vision:**

  Most enterprise security professionals focus on affectations and impacts to their operations and rightly so. Due to the sheer volume of signals that our SOC (security operations center) analysts must attend to, there is neither the time nor resources to identify systemic attacks.

  Focused impact analysis is the normal modus operandi for many organizations, and will not change. For all intents and purposes, it should not change, but be augmented by a small team responsible for looking above the water line.

- **Apophenia:**

  At the other end of the gamut, there are organizations teams solely looking for patterns; they interpret every problem in the context of a multi-modal threat. This swing of the pendulum is counterproductive as it could lead to unnecessary actions and expenditures. The Analysis & Resilience Center for Systemic Risk[87] is a textbook example of an organization built to look for systemic threats yet, they have an SOP which defines criteria to characterize and park seemingly non-systemic events, along with the ability pull them back into the fold if there is a correlation.

- **Bias, Preference or Expertise?**

  The prevalence of bias has historically contributed to a myopic behavior in every industry, and effectively working within the constraints of each sector's risk culture may be an effort upon itself. Risk assessment calculations are skewed by two key biases: motivational bias and cognitive bias.

  - **Motivational Bias** (predisposed by reward/punishment):

    Reputational risks are rated as high as other risk areas, as consumer/institutional confidence directly affects their market value;

  - **Cognitive Bias** (distortion of conscious beliefs):

    Although cyberattacks may cause fiduciary losses directly, indirect collateral damage to the larger financial ecosystem may not be felt for some time afterwards, which may cause firms to underestimate the residual risks after such an attack has been mitigated;

SUMMARY

Multi-modal capabilities will be the **point of inflection for all future attacks**, and we must be prepared. Organizations need to stop artificially treating cyber from other types of threats but must correlate both logical and physical risks as equal attributes in the same threat model. Collectively, we need to focus more efforts on identifying global cross-sector disruptions. The global economy has experienced the effects of our own indiscretions with regard to the mortgage crisis in 2008, resulting in a wholesale lack of trust in both the financial and real estate sectors as well as our regulators. And this was our own doing!

We must be careful of over-stepping the bounds of sanity. This can happen by confusing our highly advanced technical capabilities with bias and hubris, such as with the ludicrous suggestion (by a former senior advisor to the U.S. State Department Antiterrorism Assistance Program) that our response to potential threats should be a preemptive cyber-attack.

I leave you with one final excerpt:

Those wishing to do us harm have no state allegiance; they cross borders to share information and collaborate to refine their methods of causing chaos and destruction. The focus of governments must be on protecting people. And that cannot be done with insular thinking.[88]

NOTES

1. "Russia's Cyberattack on Georgia," Human Events Archive, August 15, 2008, https://archive.humanevents.com/2008/08/15/russias-cyberattack-on-georgia/.
2. R. Virani, "The Supply Chain Is the Next Big Cyberattack Target," Supply & Demand Chain Executive, March 16, 2022, https://www.sdcexec.com/safety-security/article/22118933/alliant-cybersecurity-the-supply-chain-is-the-next-big-cyberattack-target.
3. "Cyber-warfare, cyber diversions and cyber terrorism," https://book.cyberyozh.com/cyber-warfare-cyber-diversions-and-cyber-terrorism/.
4. Audrey Conklin, "Chinese cyberattacks on NATO countries increase 116% since Russia's invasion of Ukraine: study," Fox Business News, March 26, 2022, https://www.foxbusiness.com/technology/chinese-cyberattacks-nato-increase-ukraine.
5. InfraGard, "INFRAGARD EMP RESOURCE CENTER," https://www.empcenter.org.
6. T. Ahasan, "Preparing for the crash: The threat of an electromagnetic pulse," March 26, 2018, https://globalresilience.northeastern.edu/2018/03/preparing-for-the-crash-the-threat-of-an-electromagnetic-pulse/.
7. InfraGard NDRC, "Chapter VI: Resilient Communities using an Island Concept," in Powering Through "From Fragile Infrastructures To Community Resilience, Curtis 1000, 2016.
8. J. Stavridis, "North Korea's Secret Weapon: A Huge Electromagnetic Storm," April 25, 2018, https://www.bloomberg.com/view/articles/2018-04-25/north-korea-s-secret-weapon-an-electromagnetic-storm.
9. P. Dockrill, "Here's What Would Happen if a Solar Storm Wiped Out Technology as We Know It," June 21, 2018, https://www.sciencealert.com/here-s-what-would-happen-if-solar-storm-wiped-out-technology-geomagnetic-carrington-event-coronal-mass-ejection.
10. P. Martin, "American diplomats in Cuba were targeted with microwave weaponry," September 2, 2018, http://revolutionradio.org/2018/09/02/american-diplomats-in-cuba-were-targeted-with-microwave-weaponry/.
11. B. M. Farmer, "Is an invisible weapon targeting U.S. diplomats?" CBS News 60 Minutes Overtime, June 27, 2021, https://www.cbsnews.com/news/is-an-invisible-weapon-targeting-u-s-diplomats-60-minutes-2021-06-27/.
12. J. Herb, "US investigating possible mysterious directed energy attack near White House," CNN, April 29, 2021, https://www.cnn.com/2021/04/29/politics/us-investigating-mysterious-directed-energy-attack-white-house/index.html.
13. History Channel, "Ancient Impossible," 2014, https://play.history.com/shows/ancient-impossible/season-1/episode-8.
14. InfraGard NDRC, "Chapter 5," in Powering Through: Building Critical Infrastructure Resilience, Bowker, 2021.
15. D. Dudley, "Iran Dabbles In Crypto For Cross-Border Trade, In Effort To Bypass Sanctions," Forbes, August 10, 2022, https://www.forbes.com/sites/dominicdudley/2022/08/10/iran-dabbles-in-crypto-for-cross-border-trade-in-effort-to-bypass-sanctions/?sh=4d4a50704776.
16. Andrei Kirilenko, "The Flash Crash: The Impact of High Frequency Trading on an Electronic Market," CFTC, 2010.
17. F-Secure, "Threat Analysis: SWIFT Systems and the SWIFT Customer Security Program," https://www.f-secure.com/content/dam/f-secure/en/business/common/collaterals/f-secure-threat-analysis-swift.pdf.
18. P. Foster, "'Bogus' AP tweet about explosion at the White House wipes billions off US markets," April 23, 2013, https://www.telegraph.co.uk/finance/markets/10013768/Bogus-AP-tweet-about-explosion-at-the-White-House-wipes-billions-off-US-markets.html.
19. H. Son, "JP Morgan's top quant warns next crisis to have flash crashes and social unrest not seen in 50 years," CNBC, Sep 4, 2018, https://www.cnbc.com/2018/09/04/jpmorgan-says-next-crisis-will-feature-flash-crashes-and-social-unrest.html.
20. M. Wright, "As Iran turns to Bitcoin and its own cryptocurrency to avoid sanctions, maybe it's time to build another Stuxnet," *The Hill*, August 19, 2018, http://thehill.com/opinion/technology/402477-as-iran-turns-to-bitcoin-and-its-own-cryptocurrency-to-avoid-sanctions.
21. Fox News, "Iran, North Korea and Venezuela turning to cryptocurrency to bypass US sanctions, experts warn," FOX News, September 7, 2018, https://www.foxnews.com/tech/2018/09/07/iran-north-korea-and-venezuela-turning-to-cryptocurrency-to-bypass-us-sanctions-experts-warn.html.
22. *MIT Technology Review*, "Bitcoin Transactions Aren't as Anonymous as Everyone Hoped," August 23, 2017, https://www.technologyreview.com/s/608716/bitcoin-transactions-arent-as-anonymous-as-everyone-hoped/.
23. A. Cruz, "Blockchain Weaponization, National Security Concerns, and Attacks of the Foreseeable Future," May 18, 2018, https://www.linkedin.com/pulse/blockchain-weaponizion-national-security-concerns-attacks-cruz-1/.

NOTES

24. D. Yadron, "Iranian Hackers Infiltrated New York Dam in 2013," *The Wall Street Journal*, December 20, 2015, https://www.wsj.com/articles/iranian-hackers-infiltrated-new-york-dam-in-2013-1450662559?cb=logged0.9423363890964538.
25. Booz Allen Hamilton, "Industrial Cybersecurity Threat Briefing," June 16, 2016, https://www.slideshare.net/BoozAllen/booz-allen-industrial-cybersecurity-threat-briefing.
26. D. Yadron, 2015.
27. K. Brocklehurst, "U.S. Water Utility Breach and ICS Cyber Security Lessons Learned," February 22, 2017, https://www.belden.com/blog/industrial-security/u-s-water-utility-breach-and-ics-cyber-security-lessons-learned.
28. N. Perlroth, "'Dangerous Stuff': Hackers Tried to Poison Water Supply of Florida Town," February 2021, https://www.nytimes.com/2021/02/08/us/oldsmar-florida-water-supply-hack.html.
29. J. Heyen, "Honey, I Hacked The SCADA! : Industrial CONTROLLED Systems!" March 19, 2016, https://www.youtube.com/watch?v=QAl2GkhT4Jg.
30. P. Vuppuluri, "Investing In Innovation: The Rise Of The Smart City," December 3, 2020, https://www.forbes.com/sites/forbesfinancecouncil/2020/12/03/investing-in-innovation-the-rise-of-the-smart-city/?sh=47f008395ba6.
31. EY, "Cyber Security: A necessary pillar of Smart Cities," November 18, 2016, https://web.archive.org/web/20180218234603/http://www.ey.com:80/Publication/vwLUAssets/ey-cyber-security-a-necessary-pillar-of-smart-cities/$FILE/ey-cyber-security-a-necessary-pillar-of-smart-cities.pdf.
32. Trend Micro, "Shodan Reveals Exposed Cyber Assets," November 28, 2017, https://www.trendmicro.com/vinfo/sg/security/news/internet-of-things/cities-exposed-in-shodan.
33. ANSI, "Smart and Sustainable Cities," https://webstore.ansi.org/industry/smart-cities.
34. D. Paillet, "Defending Against Cyber Threats to Building Management Systems," January 3, 2019, https://www.se.com/ww/en/download/document/998-2095-12-08-15AR0_EN/.
35. "Aviation ISAC," https://www.a-isac.com/.
36. "AITA," https://www.iata.org/en/about/.
37. M. Garcia, "IATA Warns Of Aviation Security Risks, Calls For Better Collaboration With Governments," February 27, 2019, https://www.forbes.com/sites/marisagarcia/2019/02/27/iata-warns-of-aviation-security-risks-calls-for-better-collaboration-with-governments/?sh=3c9d344e36e2.
38. "ICAO GLOBAL AVIATION SECURITY PLAN (GASeP)," 2017, https://www.icao.int/Security/Pages/Global-Aviation-Security-Plan.aspx.
39. BBC News, "Air Canada app data breach involves passport numbers," August 29, 2018, https://www.bbc.com/news/technology-45349056.
40. B. Sullivan, "How Airlines Are Vulnerable to Cyber Attacks," August 19, 2016, https://cyberscout.com/en/blog/how-airlines-are-vulnerable-to-cyber-attacks.
41. *National Academies Press*, "Assessment of Technologies Deployed to Improve Aviation Security: First Report (1999) - Chapter 4 Baggage Handling," 1999, https://www.nap.edu/read/9726/chapter/6.
42. X-Ray Screener, "X-Ray Limitations," https://www.x-rayscreener.co.uk/?xray=x-ray-limitations, accessed December 3, 2020.
43. S. Almasy, "A judge ruled that a website has to suspend downloads for 3D gun plans. But they're already out there," August 1, 2018, https://www.cnn.com/2018/07/31/us/3d-guns-downloaded-plans-states.
44. F. Donovan, "1.13M Records Exposed by 110 Healthcare Data Breaches in Q1 2018," May 7, 2018, https://healthitsecurity.com/news/1.13m-records-exposed-by-110-healthcare-data-breaches-in-q1-2018.
45. Healthcare IT News, "The biggest healthcare data breaches of 2018 (so far)," October 25, 2018, https://www.healthcareitnews.com/projects/biggest-healthcare-data-breaches-2018-so-far.
46. K. Harris, "Hacking medical devices: Managing and bolstering MedTech cybersecurity defenses," August 19, 2021, https://www.hologram.io/blog/medical-device-hacking.
47. IAmTheCavalry.org, "Medical," November 4, 2020, https://iamthecavalry.org/issues/medical/.
48. P. Martyn, "The Lack of Medical Device Security -- Accidents Waiting To Happen," July 11, 2018, https://www.forbes.com/sites/paulmartyn/2018/07/11/the-lack-of-medical-device-security-accidents-waiting-to-happen.

NOTES

49. J. Davis, "AHA, other groups call for medical device security guidance, financial support," July 5, 2018, https://www.healthcareitnews.com/news/aha-other-groups-call-medical-device-security-guidance-financial-support.y 5.
50. S. Khandelwal, "Real-World SS7 Attack: Hackers Are Stealing Money From Bank Accounts," May 4, 2017, https://thehackernews.com/2017/05/ss7-vulnerability-bank-hacking.html.
51. R. Koch, "Criminal Activity Through VoIP: Addressing the Misuse of your Network," December 2005, http://www.tmcnet.com/voip/1205/special-focus-criminal-activity-through-voip.htm.
52. Noction, "BGP Hijacking overview. Routing incidents prevention and defense mechanisms," April 14, 2018, https://www.noction.com/blog/bgp-hijacking.
53. N. Anderson, "How China swallowed 15% of 'Net traffic for 18 minutes," November 17, 2010, https://arstechnica.com/information-technology/2010/11/how-china-swallowed-15-of-net-traffic-for-18-minutes/.
54. A. Siddiqui, "Did Ukraine suffer a BGP hijack and how can networks protect themselves?" MANRS, March 4, 2022, https://www.manrs.org/2022/03/did-ukraine-suffer-a-bgp-hijack-and-how-can-networks-protect-themselves/.
55. D. Goodin, "BGP event sends European mobile traffic through China Telecom for 2 hours," ARS Technica, June 8, 2019, https://arstechnica.com/information-technology/2019/06/bgp-mishap-sends-european-mobile-traffic-through-china-telecom-for-2-hours/.
56. Reuters, "Nigerian Firm Takes Blame For Routing Google Traffic Through China," Slashdot, November 13, 2018, https://tech.slashdot.org/story/18/11/13/2142249/nigerian-firm-takes-blame-for-routing-google-traffic-through-china.
57. C. Morales, "BGP hijackers: 'This traffic is going to Russia!'," December 14, 2017, https://blog.vectra.ai/blog/bgp-hijackers-this-traffic-is-going-to-russia.
58. A. Toonk, "Massive route leak causes internet slowdown," Cisco, June 12, 2015, https://bgpmon.net/massive-route-leak-cause-internet-slowdown/.
59. D. Madory, "Chinese Routing Errors Redirect Russian Traffic," November 6, 2014, https://blogs.oracle.com/internetintelligence/chinese-routing-errors-redirect-russian-traffic-v3.
60. K. Zetter, "Someone's Been Siphoning Data Through a Huge Security Hole in the Internet," December 5, 2013, https://www.wired.com/2013/12/bgp-hijacking-belarus-iceland/.
61. N. Anderson, 2010.
62. FCC, "Caller ID Spoofing," September 23, 2020, https://www.fcc.gov/consumers/guides/spoofing-and-caller-id.
63. Verizon Wireless, "What can be done - my number is being used in a caller ID spoofing scam," December 18, 2017, https://community.verizonwireless.com/thread/941600.
64. ICANN, "DNSSEC – What Is It and Why Is It Important?" March 5, 2019, https://www.icann.org/resources/pages/dnssec-qaa-2014-01-29-en.
65. Noction, "BGP security: the BGPsec protocol," April 30, 2015, https://www.noction.com/blog/bgpsec_protocol.
66. "TLS1.3," October 7, 2018, https://wiki.openssl.org/index.php/TLS1.3.
67. T. Chung, "Why DNSSEC deployment remains so low," December 6, 2017, https://blog.apnic.net/2017/12/06/dnssec-deployment-remains-low/.
68. "Information Sharing and Analysis Organization Standards Organization (ISAO SO)," UTSA Center for Infrastructure Assurance and Security, https://www.isao.org/information-sharing-groups/.
69. "Energy ISAC (Information Sharing & Analysis Center)," https://www.eisac.com/.
70. "Oil & Natural Gas ISAC (Information Sharing & Analysis Center)," https://ongisac.org/.
71. Ibid.
72. "Nuclear Energy Institute," https://www.nei.org.
73. "Energy Analytic Security Exchange (EASE)," Global Resilience Federation, https://grf.org/ease.
74. "Multi-State ISAC (Information sharing & Analysis Center)," https://www.cisecurity.org/ms-isac/.
75. "Aviation ISAC (Information Sharing & Analysis Center)," https://www.a-isac.com/.
76. "Financial Services ISAC (Information Sharing & Analysis Center)," https://www.fsisac.com/.
77. Business Wire, October 30, 2020, https://www.businesswire.com/news/home/20201030005462/en/Announcing-the-Formation-of-the-Analysis-Resilience-Center-ARC-for-Systemic-Risk.

NOTES

78. "Federally-Defined Critical Infrastructure Sectors," US DHS CISA, https://www.cisa.gov/critical-infrastructure-sectors.
79. ASIS International, "ASIS International Strategic Plan 2016-2021," January 23, 2017, https://www.asisonline.org/globalassets/about-asis/strategic-plan/asis-strat-plan-final-april-2017.pdf.
80. DHS/CISA, "NIPP Supplemental Tool: Connecting to the National Infrastructure Coordinating Center (NICC) and National Cybersecurity and Communications Integration Center (NCCIC)," 2018, https://www.cisa.gov/publication/connecting-nicc-and-nccic.
81. D. Rubin, "Crew Resource Management," *Firehouse Magazine,* 2006.
82. FAA, "CRM Error Management," https://www.hf.faa.gov/webtraining/TeamPerform/TeamCRM013.htm.
83. Sounil Yu, "Cyber Defense Matrix," https://cyberdefensematrix.com/.
84. "FIDO Alliance," https://fidoalliance.org/fido2/.
85. Lt. Col. (Ret) Robert J. Darling, "Turning Point Crisis Management," https://tpcm-usa.com.
86. D. Keltner, "We Are All Bystanders," *Greater Good Magazine,* September 2006, https://greatergood.berkeley.edu/article/item/we_are_all_bystanders.
87. *Business Wire,* October 30, 2020.
88. M. Garcia, "IATA Warns Of Aviation Security Risks, Calls For Better Collaboration With Governments," 2019.

The Impending Data Literacy Crisis Among Military Leaders

Lieutenant Colonel Andrew G. Farina

INTRODUCTION

You would be hard pressed to find a room full of office typists in any present-day corporate setting. Office typists (who reached an apex in the mid-20th century) employed fast typing skills, a mastery of language and grammar, and the ability to take real-time dictation through shorthand.[1] However, with the advent of personal computers and email, the speed of business required leaders to improve their own typing and communication skills. Those that embraced these skills quickly outperformed those that failed to adapt. Today, office typists are obsolete; their skills are now integral to everyone in an organization.

Similarly, today's business leaders rely on teams of data scientists[2] to manage, analyze, and model large amounts of data to inform decisions. Will data scientists one day sustain a fate similar to office typists? It may be too early to make such a prediction. Nonetheless, to compete in the near-future global market, leaders–military and civilian alike–will need to adapt these skills and become data literate with deep knowledge of data capabilities.

Data provide a competitive advantage[3] to the businesses and governments who know how to use them. The private sector employs cross-functional data science teams to analyze and build valuable prediction models from large clusters of data that are used to drive business decisions and maximize outcomes. The ubiquitous use of personal devices that capture our every step, social media post, and internet search, along with rapidly improving infrastructures to handle such large-scale structured and unstructured information, have given rise to machine learning (ML) and artificial intelligence (AI). We interact with ML algorithms daily; these techniques allow for endless possibilities to make data-driven decisions to enhance nearly any aspect of life. Amazon recommends items to purchase based

LTC Andrew Farina is an Infantry Officer and Assistant Professor at the U.S. Military Academy. He is the Management Program Director in the Department of Behavioral Sciences and Leadership. He has ten combat deployments with both conventional and special operations units. He is a U.S. Military Academy graduate, earned a Ph.D. at Tufts University, an MBA at the University of North Carolina, and completed a data science professional certificate through HarvardX.

on the purchase history of people similar to you. Google Maps provides routes based on your route preferences along with current traffic, speed, and accident data. Digital assistants, such as Siri and Alexa, use language processing to predict what information you are requesting. On discount travel sites, you may even find different prices based on an algorithm that predicts those using Apple computers are less price sensitive than those that use Windows PCs. With these relatively low-risk examples, the cost of getting the prediction wrong is fairly low. Data scientists tune parameters to improve the algorithm's performance based a context specific optimization of precision, sensitivity, and specificity.

MILITARY APPLICATION OF ML/AI TECHNOLOGIES

The U.S. Army is actively building advanced data capabilities that leverage ML and AI to revolutionize the future of warfare against increasingly capable adversaries. The potential for AI to drastically change the speed of decisions, and thereby the speed of war, will be revolutionary. Unfortunately, without a focused effort to improve military leaders' understanding of the data science field, commanders will lack trust in these technologies or, far worse, will over-rely on amoral machines to make decisions for them.

A quick search of the military's use of ML/AI results in numerous, cutting-edge efforts to revolutionize warfare. Project Maven[5] is one example where the U.S. Special Operations Command (SOCOM) is leveraging AI to assist in analyzing surveillance video using visual detection algorithms. The initial foray into AI-supported analysis has the potential to drastically improve SOCOM's ability to analyze vast amounts of raw video data and reduce the intelligence analyst's time needed to conduct this task. Although tactical-level leaders acknowledge the potential, the science fiction-like expectation is inconsistent with the reality, thus hindering the full integration.[6]

Project Convergence[7] is a second example where the U.S. Army is leveraging AI. With Project Convergence, the goal is to dramatically reduce the time needed to identify enemy forces and employ lethal munitions. This initiative demonstrated some success recently in an exercise where the Fires Synchronization to Optimize Responses in Multi-Domain Operations (FIRESTORM)[8] recommendation algorithm was used to support rapid decision-making to deliver lethal effects on identified targets. This project has the potential to dramatically improve the targeting cycle and quickly overwhelm our adversaries. However, leaders must have intricate knowledge[9] of how these systems work to understand the inherent biases that may exist within the algorithms and the potential clashes between moral values and AI-based decision-making.

The Operations Research/Systems Analysis (ORSA) is a functional area within the Army that traditionally supplied data analysts to support data-driven decision-making on strategic level staffs.[10] ORSA personnel are evolving their role from data analysts (analyzing data to produce new insights) into data scientists[11] (building predictive models and visualizing data to produce new insights) to support strategic-level decision-makers. Currently, however, neither ORSA personnel nor other data scientist teams are consistently available to support tactical- and operational-level decision-makers. Yet, leaders still find themselves making decisions in data-rich environments. Because of this, it is imperative that leaders at all levels improve their data literacy to operate in conflicts of both today and well into the future.

ML/AI IMPLICATIONS FOR LEADERSHIP

New military leaders are often told to "trust but verify,"[12] a phrase made popular by former President Ronald Reagan when discussing nuclear disarmament. This notion is usually followed by, "don't expect what you don't inspect," a mantra that is paramount to anyone employing ML algorithms and AI in a high-risk context. Given quality data, properly trained algorithms can find patterns and make predictions far better than humans.[13] However, many applications of ML/AI use "black box" approaches that obfuscate the decision-making rules that are used. In high-risk environments, when making data-driven decisions, leaders must understand why decisions are being recommended, think critically about potential biases, and verify the tradeoff[14] between precision (out of those predicted as A, how many are really A), sensitivity (out of those that are A, how many were predicted to be A), and specificity (out of those that are not A, how many were predicted to not be A).

Compared to the low-risk predictions involved in Google Maps and Amazon shopping, in the military, the cost of getting a prediction wrong could be catastrophic. Decision-making algorithms need to be informed by subject matter experts and be trained on the same type of data that leaders would utilize to make decisions. As an example, team leaders would never use a Google Maps algorithm to conduct route planning from a forward operating base to a target location unless they knew numerous variables were considered, such as historic enemy activity, friendly force location, and the potential to encounter deeply buried improvised explosive devices. The team leader would still want to verify the recommended route based on their own experience, mission objectives, and organizational capability.

WHAT DO LEADERS NEED TO UNDERSTAND?

At a minimum, military leaders employing ML/AI technologies must understand[15] the data pipeline, as well as algorithm development and underlying assumptions to identify the strengths (when it should work well), limitations (when it will be unreliable), and indicators of drift (when reinforcement learning algorithms in production become less reliable over time).

Data Pipeline

Algorithms are only as good as the data upon which they are trained. If these data are biased in any way, the algorithm will also be biased.[16] It is important for leaders to understand how data are obtained and processed so that they can appreciate the limits of an ML/AI application. Raw data must be processed and transformed before it can be used in ML/AI. Turning raw data[17] into usable data can be as complex as the algorithm-building process itself. When data engineers clean and transform raw data, the decisions they make will impact the performance of the algorithm. For leaders to fully appreciate what decisions, and ultimately what biases underlay the algorithm, they must have some knowledge of this data-cleaning process.

When unbalanced data sets are used for training, it can also introduce bias into detection algorithms. For example, one of the most popular data sets used to train algorithms to predict age and gender from a static image is based on the 100,000 most popular actors and actresses.[18] The data set contains a disproportionate number of Caucasian men, as well as images that appear much younger than their true age. As a result, most algorithms trained on these data can accurately detect Caucasian men, but have a substantially harder time classifying minority women, and almost always predict their age as older than they actually are. If diverse groups are not equally represented in a military object detection algorithm,[19] the results could disproportionately misclassify and endanger under-represented individuals. Leaders must critically think through potential biases inherent within training data sets to understand the limits of ML/AI algorithms.

When ML/AI applications are designed to continue learning as new data are considered–also called reinforcement learning algorithms–it is important for leaders to identify when contextual changes or data quality changes may impact the accuracy of the prediction models. By understanding how often new data are introduced and how often an algorithm's performance is tested, leaders can better identify this drift in accuracy.

Algorithm Development

Similar to data engineers making decisions about data processing, ML engineers make decisions when determining what algorithms to use and how to optimally tune them. Leaders employing ML/AI capabilities would certainly benefit from understanding how an algorithm makes decisions. The interpretability of an algorithm is an important consideration for ML engineers and leaders alike. Black box approaches, such as deep neural networks,[20] may provide a slight improvement in performance over more interpretable approaches, such as decision-tree classification algorithms. However, black box approaches come at a cost. Leaders that cannot articulate why an algorithm concluded what it did will either not be able to fully trust the recommendation or, perhaps more dangerously, blindly trust the decision.

FINAL THOUGHTS

As technology changes, all leaders (military and civilian) must learn the capabilities and limitations of the tools that they employ. The United States Military Academy was founded on a desire to bring the technical expertise of civil engineering and artillery[21] into our fledgling Nation's military officer corps at the turn of the 19th century. The technical expertise needed during today's information age is data literacy.

Across the country, most, if not all, colleges and universities are developing data science undergraduate and graduate degrees. Educational settings[22] may be an opportune context to develop data literacy and many initiatives are currently underway. In fact, West Point has several initiatives that are building this knowledge among our young military leaders. All current Cadets take a two-course core information technology program,[23] in which faculty members recently began to incorporate data science into the curriculum.[24] The Center for Data Analysis and Statistics,[25] the Applied Statistics and Data Science Major,[26] and the Computer Science Major[27] also provide additional opportunities for Cadets to further learn about data science and develop their knowledge and skills. Even within the behavioral sciences, I have introduced the R programming language[28] in an attempt to improve each Cadet's data literacy and algorithmic thinking.

With such training becoming increasingly prevalent across both military and civilian educational settings, in the near future, junior leaders will have a basic understanding of data and data-driven technologies. Mid- to senior-level leaders will need to embrace and consider ways to improve their own understanding of these technologies or risk these advances outpacing our leader's ability to employ them. This concept is not new or without support. As discussed in the *2019 ADP 6-22: Army Leadership and the Profession*, "The adaptable leader remains aware of the capabilities and shortcomings of advanced technology and ensures subordinates do as well."[29] We no longer need office typists, but we will always need adaptable leaders.

DISCLAIMER

Views expressed here are those of the authors and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, or the Department of Defense.

NOTES

1. "Shorthand-Typist: A Common Job for Women in 1950s UK," accessed October 17, 2021, https://www.1900s.org.uk/1950s-shorthand-typing.htm.
2. "How to Structure a Data Science Team: Key Models and Roles to Consider" *AltexSoft*, June 30, 2020, https://www.altexsoft.com/blog/datascience/how-to-structure-data-science-team-key-models-and-roles/.
3. Peter Bell, "Creating Competitive Advantage Using Big Data," *Ivey Business Journal (Online)*, May/June 2013.
4. James Hennig, Peter Schwartz, and Kathryn Bailey, "Mission Command on Semi-Automatic," *www.army.mil,* March 2017, https://www.army.mil/article/184031/mission_command_on_semi_automatic.
5. Richard H. Shultz and Gen. Richard D. Clarke, "Big Data at War: Special Operations Forces, Project Maven, and Twenty-First-Century Warfare," *Modern War Institute,* August 2020, https://mwi.usma.edu/big-data-at-war-special-operations-forces-project-maven-and-twenty-first-century-warfare/.
6. Shultz and Clarke, "Big Data at War."
7. Joseph Lacdan, "Project Convergence Aims to Accelerate Change in Modernization Efforts," *www.army.mil,* September 2020, https://www.army.mil/article/238960/project_convergence_aims_to_accelerate_change_in_modernization_efforts.
8. Jen Judson and Nathan Strout, "At Project Convergence, the US Army Experienced Success and Failure and It's Happy about Both," *Defense News*, accessed October 14, 2020, https://www.defensenews.com/digital-show-dailies/ausa/2020/10/12/at-project-convergence-the-us-army-experienced-success-and-failure-and-its-happy-about-both/.
9. Yinying Wang, "When Artificial Intelligence Meets Educational Leaders' Data-Informed Decision-Making: A Cautionary Tale," *Studies in Educational Evaluation*, From Data-Driven to Data-informed Decision Making:Progress in the Field to Improve Educators and Education, 69 (June 1, 2021), https://doi.org/10.1016/j.stueduc.2020.100872.
10. Center for Army Analysis, "ORSA Handbook for the Senior Commander," March 2008, https://apps.dtic.mil/dtic/tr/fulltext/u2/a489398.pdf.
11. Cardy III Moten, "Functional Area 49 Operations Research and Systems Analysis Announcement," *www.army.mil,* June 2018, https://www.army.mil/article/207520/functional_area_49_operations_research_and_systems_analysis_announcement.
12. Kevin Coleman, "Trust But Verify," Military.com, July 2010, https://www.military.com/defensetech/2010/07/19/trust-but-verify.
13. Ophir Tanz, "Can Artificial Intelligence Identify Pictures Better Than Humans?" *Entrepreneur,* April 2017, https://www.entrepreneur.com/article/283990
14. Alon Lekhtman, "Should I Look at Precision & Recall OR Specificity & Sensitivity?" (Towards Data Science, August 5, 2019), https://towardsdatascience.com/should-i-look-at-precision-recall-or-specificity-sensitivity-3946158aace1.
15. Mike Walsh, "Why Business Leaders Need to Understand Their Algorithms," *Harvard Business Review,* November 19, 2019, https://hbr.org/2019/11/why-business-leaders-need-to-understand-their-algorithms.
16. Joy Buolamwini and Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," in *Machine Learning Research 81:1-15, 2018*, ed., Sorelle A. Friedler and Christo Wilson, vol. 81, 2018, 15.
17. Karl Weinmeister, "Turn Your Raw Data into a Machine Learning Model Without Python or SQL," *Google Cloud Blog,* April 2020, https://cloud.google.com/blog/products/ai-machine-learning/from-raw-data-to-machine-learning-model-no-coding-required/.
18. Amber Camilleri et al., "Bias in Machine Learning: How Facial Recognition Models Show Signs of Racism, Sexism and Ageism," *Toward Data Science*, December 2019, https://towardsdatascience.com/bias-in-machine-learning-how-facial-recognition-models-show-signs-of-racism-sexism-and-ageism-32549e2c972d.
19. Benjamin Wilson, Judy Hoffman, and Jamie Morgenstern, "Predictive Inequity in Object Detection," *arXiv Preprint arXiv:1902.11097*, February 2019. http://arxiv.org/abs/1902.11097.
20. James Montantes, "3 Reasons to Use Random Forest Over a Neural Network: Comparing Machine Learning Versus Deep...," *Medium*, November 2014, https://towardsdatascience.com/3-reasons-to-use-random-forest-over-a-neural-network-comparing-machine-learning-versus-deep-f9d65a154d89.
21. The United States Military Academy, "USMA Faculty Manual," November 2014, https://www.westpoint.edu/sites/default/files/pdfs/Academics/USMA%20Faculty%20Manual%202014.pdf.

NOTES

22. Erica Sachiyo Deahl, "Better the Data You Know: Developing Youth Data Literacy in Schools and Informal Learning Environments," *SSRN Electronic Journal*, 2014, https://doi.org/10.2139/ssrn.2445621.
23. "Core Information Technology | United States Military Academy West Point", accessed October 24, 2020, https://www.westpoint.edu/academics/academic-departments/electrical-engineering-and-computer-science/curriculum/core-information-technology.
24. Malcolm Haynes et al., "Integrating Data Science into a General Education Information Technology Course: An Approach to Developing Data Savvy Undergraduates," in *Proceedings of the 20th Annual SIG Conference on Information Technology Education* (Tacoma WA USA: ACM, 2019), 183–88, https://doi.org/10.1145/3349266.3351417.
25. "Center for Data Analysis and Statistics | United States Military Academy West Point", accessed October 24, 2020, https://www.westpoint.edu/academics/academic-departments/mathematical-sciences/centers/center-for-data-analysis-statistics.
26. "Applied Statistics & Data Science | United States Military Academy West Point", accessed October 24, 2020, https://www.westpoint.edu/academics/academic-departments/mathematical-sciences/applied-statistics-and-data-science.
27. "Computer Science | United States Military Academy West Point", accessed October 24, 2020, https://www.westpoint.edu/academics/academic-departments/electrical-engineering-and-computer-science/computer-science.
28. R Core Team, "R: A language and environment for statistical computing, R Foundation for Statistical Computing, Vienna, Austria," 2020, https://www.R-project.org/.
29. Department of the Army Headquarters, "ADP 6-22: Army Leadership and the Profession," July 2019, https://fas.org/irp/doddir/army/adp6_22.pdf.

Contract AI Risk Engine (CARE) to Reduce Cyber Contracting Risk

Major Y. Brian Lee
Major Dennis Kim
Major Wallace Rollins

INTRODUCTION

The Fiscal Year 2019 National Defense Authorization Act (NDAA) established the National Security Commission on Artificial Intelligence (NSCAI) to consider the methods and means necessary to advance development of artificial intelligence (AI), machine learning (ML), and other associated technologies to address America's national security concerns. NSCAI's final report to the President and Congress identified areas of weakness that the federal government must address to elevate data security as a national security priority. NSCAI recommended the federal government implement a security development lifecycle approach for AI systems, prioritize data privacy and security considerations as part of larger efforts to strengthen foreign investment screening and supply chain intelligence and risk management, and integrate national security considerations into efforts to legislate and regulate data protection and privacy.[1]

Current Department of Defense (DoD) information technology (IT) contracting policies, vehicles, and practices lack definitive language or terms that give due process to national security considerations. Without contracting language specifically tailored to the cyber security threats facing the United States (US), DoD cannot adequately secure the DoD Information Network (DODIN) nor protect it from foreign influence. Contractual languages often favor the vendor. For example, DoD cyber vendors can potentially circumvent DoD prohibited IT equipment or prevent DoD Cyber Protection Teams from inspection or damage assessment during cyber breaches or attacks, citing ambiguous contracting language and proprietary corporate intellectual protection as justifications.[2] Unfortunately, contracting personnel, commanders, and staffs across the DoD lack training and expertise in

Major Y. Brian Lee, U.S. Army, is a Medical Service Corps officer assigned to the Department of Defense Chief Digital and Artificial Intelligence Office, Arlington, VA. He holds a BA from Washington University in St. Louis, a MS from the University of Maryland Global Campus, and a Masters in Operational Studies from the U.S. Army Command and General Staff College. During his career, MAJ Lee served with the Joint Artificial Intelligence Center, 7th Special Forces Group, 2nd Infantry Division, 82nd Airborne Division, and 65th Medical Brigade.

reducing cyber security risk. An objective cyber contract risk score does not exist. DoD should leverage ML in the cyber contract requirements generation process to reduce cyber contract risk and position DoD to better prevent, monitor, and respond to cyber threats.

Issue

Contracts for cyber or IT related products and services present a cyber supply chain risk for the DoD. Cyber supply chain risk stems from a lack of visibility into, understanding of, and control over many of the processes and decisions involved in the development and delivery of cyber products to the Joint Force.[3]

Requirement owners and contract management offices are at the forefront of cyber supply chain risk management (C-SCRM). As the requiring activity, commanders and their staff determine and develop requirements and generate the performance work statement (PWS). Contracting officers, vested with the authority to obligate the US government to legally binding contracts, coordinate and finalize contracting actions to provide the goods or services needed by the requiring activity. Unfortunately, requiring activities and contracting professionals often lack the technical expertise to articulate specific C-SCRM measures within contracts. Further, existing resources that provide guidelines and standards for C-SCRM are inadequate with respect to the granular process of contract writing and are spread across a multitude of DoD policies (Figure 1).

Publications from the National Institute of Standards and Technology (NIST), Defense Acquisition University (DAU), and DoD Instruction documents describe how to conduct C-SCRM, but no publication goes into more nuanced details on contract language, thus creating gaps in cyber supply chains. Current acquisition processes account for various risks, but in-depth technical understanding of the cyber supply chain is required to properly translate mitigation measures into contract language during the requirements generation process.

Major Dennis Kim, U.S. Army, is a Medical Service Corps officer assigned to 65th Medical Brigade, Camp Humphreys, Republic of Korea. He holds a BS from Boston University, an MBA from The College of William and Mary, and a Masters in Operational Studies from the U.S. Army Command and General Staff College. During his career, MAJ Kim served with the 10th Mountain Division, 2nd Infantry Division, and the U.S. Army Medical Materiel Agency.

During a lecture at the U.S. Army Command and General Staff College in April 2021, Brigadier General (BG) Paul Craft, Commandant of the U.S. Army Cyber School, used the cloud migration of Army data as an opportunity to address both the benefits and challenges that data contracting presents. BG Craft acknowledged it is unrealistic to expect all contracting officers to be cyber security experts, but a lack of understanding of cyber security can lead to inadequate language in contracts. This has led to instances where data became lost, mishandled, or the DoD denied access to its own data and required to pay to get data back. BG Craft cautioned that this situation can be especially damaging when there is a breach, and the language of the contract does not authorize DoD Cyber Protection Teams to investigate the breach. This lack of transparency and access erodes the public trust and harms national security.

APPROACH AND SOLUTION

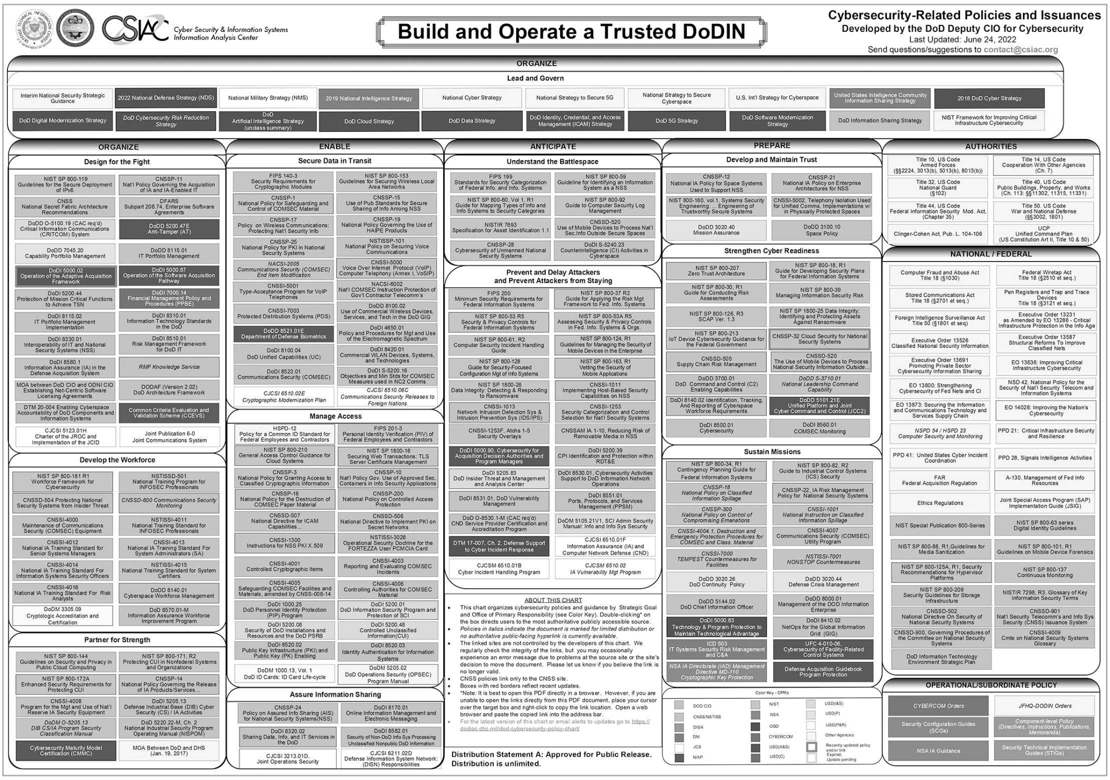
This proposal recommends the use of AI through ML to review draft contracts uploaded by contracting officers and analyze the cyber security risk to the DoD. After review, the Contract AI Risk Engine (CARE) produces recommended clauses most advantageous to DoD for cyber security along with a cyber risk level which measures the level of risk to DoD for the contract as written. The requiring activity reviews the recommendations and adjusts the contract as necessary. The contracting officer subsequently takes the improved contract and obtains a new risk score, with scores above a certain threshold requiring command concurrence by both the requiring activity commander and the supporting contracting commander before moving to contract fulfillment. As a pilot, CARE recommendations are initially based upon the Army Contracting Command's (ACC) repository of previous IT and cyber related contracts. Upon successful testing, the intent will be to incorporate a Joint solution and include data from all services and DoD agencies. CARE relies upon cloud computing and AI platforms, such as the DoD's Advana enterprise analytics platform, for data analysis, model generation, and risk score calculation.

Artificial Intelligence Design

Contracting affects DoD agencies and activities, the military services, and Combatant Commands. Using CARE to reduce cyber contracting risk is a feasible ML project with immediate real-world applications and implications where end users can see the benefits of augmenting contracting processes with AI. DoD has partnered with national academic research institutions, such as the MIT Lincoln Laboratory and the Army's AI Task Force at Carnegie Mellon University, to accelerate the research and development of national security AI priorities. While partnerships and national conversations on the research, development, and applications of AI advance the state of DoD AI initiatives, Soldiers, Airmen, and Sailors have yet to experience the transformational benefits promised by AI in daily operations. Incorporating AI into the Joint Force will create a generational shift in how business is conducted. For commanders to champion AI and for the end user to experience the benefits of AI, DoD must bridge the crisis of trust between humans and AI, whether that AI is operating in autonomous-capable weapons systems or as software platforms.[5] Building trust requires repetitive exposure through the rapid development and implementation of small-scale projects rather than conceptual projects that will not mature for years to come. Quick wins that create buy-in from the operational force will advance the state of DoD AI.

The human-machine relationship should be carefully considered when designing AI projects and use cases. Requirement developers and AI practitioners determine the degree of autonomy granted to each AI product. The three degrees of autonomy are commonly referred to as human-in-the-loop, human-on-the-loop, and human-out-of-the-loop. In human-in-the-loop (HITL) operations, the machine performs a task and waits for the human

Major Wallace Rollins, U.S. Army, is an Acquisition Corps officer assigned to Program Executive Office Soldier, Fort Belvoir, VA. He holds a BA from Virginia Polytechnic and State University, an MBA from the University of Kansas, and a Masters in Operational Studies from the U.S. Army Command and General Staff College. During his career, MAJ Rollins served with the 82nd Airborne Division, 3rd U.S. Infantry Regiment, "The Old Guard," the 1st Cavalry Division, and 1st Security Force Assistance Brigade.



Cyber Security & Information Systems Information Analysis Center

Build and Operate a Trusted DoDIN

Cybersecurity-Related Policies and Issuances
Developed by the DoD Deputy CIO for Cybersecurity
Last Updated: June 24, 2022
Send questions/suggestions to contact@csiac.org

ORGANIZE

Lead and Govern

Interim National Security Strategic Guidance
2022 National Defense Strategy (NDS)
National Military Strategy (NMS)
2019 National Intelligence Strategy
National Cyber Strategy
National Strategy to Secure 5G
National Strategy to Secure Cyberspace
U.S. Int'l Strategy for Cyberspace
United States Intelligence Community Information Sharing Strategy
2018 DoD Cyber Strategy
DoD Digital Modernization Strategy
DoD Cybersecurity Risk Reduction Strategy
DoD Artificial Intelligence Strategy (unclass summary)
DoD Cloud Strategy
DoD Data Strategy
DoD Identity, Credential, and Access Management (ICAM) Strategy
DoD 5G Strategy
DoD Software Modernization Strategy
DoD Information Sharing Strategy
NIST Framework for Improving Critical Infrastructure Cybersecurity

ORGANIZE

Design for the Fight

NIST SP 800-119 Guidelines for the Secure Deployment of IPv6
CNSSP-11 Nat'l Policy Governing the Acquisition of IA and IA-Enabled IT
CNSS National Secret Fabric Architecture Recommendations
DFARS Subpart 208.74, Enterprise Software Agreements
DoDD O-5100.19 (CAC req'd) Critical Information Communications (CRITCOM) System
DoDD 5200.47E Anti-Tamper (AT)
DoDD 7045.20 Capability Portfolio Management
DoDD 8115.01 IT Portfolio Management
DoDI 5000.02 Operation of the Adaptive Acquisition Framework
DoDI 5000.87 Operation of the Software Acquisition Pathway
DoDI 5200.44 Protection of Mission Critical Functions to Achieve TSN
DoDI 7000.14 Financial Management Policy and Procedures (PPBE)
DoDI 8115.02 IT Portfolio Management Implementation
DoDI 8310.01 Information Technology Standards in the DoD
DoDI 8330.01 Interoperability of IT and National Security Systems (NSS)
DoDI 8510.01 Risk Management Framework for DoD IT
DoDI 8580.1 Information Assurance (IA) in the Defense Acquisition System
RMF Knowledge Service
MOA between DoD CIO and ODNI CIO Establishing Net-Centric Software Licensing Agreements
DODAF (Version 2.02) DoD Architecture Framework
DTM 20-004 Enabling Cyberspace Accountability of DoD Components and Information Systems
Common Criteria Evaluation and Validation Scheme (CCEVS)
CJCSI 5123.01H Charter of the JROC and Implementation of the JCID
Joint Publication 6-0 Joint Communications System

Develop the Workforce

NIST SP 800-181 R1 Workforce Framework for Cybersecurity
NSTISSD-501 National Training Program for INFOSEC Professionals
CNSSD-504 Protecting National Security Systems from Insider Threat
CNSSD-600 Communications Security Monitoring
CNSSI-4000 Maintenance of Communications Security (COMSEC) Equipment
NSTISSI-4011 National Training Standard for INFOSEC Professionals
CNSSI-4012 National IA Training Standard for Senior Systems Managers
CNSSI-4013 National IA Training Standard For System Administrators (SA)
CNSSI-4014 National IA Training Standard For Information Systems Security Officers
NSTISSI-4015 National Training Standard for System Certifiers
CNSSI-4016 National IA Training Standard For Risk Analysts
DoDD 8140.01 Cyberspace Workforce Management
DoDM 3305.09 Cryptologic Accreditation and Certification
DoD 8570.01-M Information Assurance Workforce Improvement Program

Partner for Strength

NIST SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing
NIST SP 800-171, R2 Protecting CUI in Nonfederal Systems and Organizations
NIST SP 800-172A Enhanced Security Requirements for Protecting CUI
CNSSP-14 National Policy Governing the Release of IA Products/Services…
CNSSI-4008 Program for the Mgt and Use of Nat'l Reserve IA Security Equipment
DoDI 5205.13 Defense Industrial Base (DIB) Cyber Security (CS) / IA Activities
DoDM O-5205.13 DIB CS/IA Program Security Classification Manual
DoD 5220.22-M, Ch. 2 National Industrial Security Program Operating Manual (NISPOM)
Cybersecurity Maturity Model Certification (CMMC)
MOA Between DoD and DHS (Jan. 19, 2017)

ENABLE

Secure Data in Transit

FIPS 140-3 Security Requirements for Cryptographic Modules
NIST SP 800-153 Guidelines for Securing Wireless Local Area Networks
CNSSP-1 National Policy for Safeguarding and Control of COMSEC Material
CNSSP-15 Use of Pub Standards for Secure Sharing of Info Among NSS
CNSSP-17 Policy on Wireless Communications: Protecting Nat'l Security Info
CNSSP-19 National Policy Governing the Use of HAIPE Products
CNSSP-25 National Policy for PKI in National Security Systems
NSTISSP-101 National Policy on Securing Voice Communications
NACSI-2005 Communications Security (COMSEC) End Item Modification
CNSSI-5000 Voice Over Internet Protocol (VoIP) Computer Telephony (Annex I, VoSIP)
CNSSI-5001 Type-Acceptance Program for VoIP Telephones
NACSI-6002 Nat'l COMSEC Instruction Protection of Gov't Contractor Telecomm's
CNSSI-7003 Protected Distribution Systems (PDS)
DoDD 8100.02 Use of Commercial Wireless Devices, Services, and Tech in the DoD GIG
DoDD 8521.01E Department of Defense Biometrics
DoDI 4650.01 Policy and Procedures for Mgt and Use of the Electromagnetic Spectrum
DoDI 8100.04 DoD Unified Capabilities (UC)
DoDI 8420.01 Commercial WLAN Devices, Systems, and Technologies
DoDI 8523.01 Communications Security (COMSEC)
DoDI S-5200.16 Objectives and Min Stds for COMSEC Measures used in NC2 Comms
CJCSI 6510.02E Cryptographic Modernization Plan
CJCSI 6510.06C Communications Security Releases to Foreign Nations

Manage Access

HSPD-12 Policy for a Common ID Standard for Federal Employees and Contractors
FIPS 201-3 Personal Identity Verification (PIV) of Federal Employees and Contractors
NIST SP 800-210 General Access Control Guidance for Cloud Systems
NIST SP 1800-16 Securing Web Transactions: TLS Server Certificate Management
CNSSP-3 National Policy for Granting Access to Classified Cryptographic Information
CNSSP-10 Nat'l Policy Gov. Use of Approved Sec. Containers in Info Security Applications
CNSSP-16 National Policy for the Destruction of COMSEC Paper Material
CNSSP-200 National Policy on Controlled Access Protection
CNSSD-507 National Directive for ICAM Capabilities…
CNSSD-506 National Directive to Implement PKI on Secret Networks
CNSSI-1300 Instructions for NSS PKI X.509
NSTISSI-3028 Operational Security Doctrine for the FORTEZZA User PCMCIA Card
CNSSI-4001 Controlled Cryptographic Items
CNSSI-4003 Reporting and Evaluating COMSEC Incidents
CNSSI-4005 Safeguarding COMSEC Facilities and Materials, amended by CNSS-008-14
CNSSI-4006 Controlling Authorities for COMSEC Material
DoDI 1000.25 DoD Personnel Identity Protection (PIP) Program
DoDI 5200.01 DoD Information Security Program and Protection of SCI
DoDI 5200.08 Security of DoD Installations and Resources and the DoD PSRB
DoDI 5200.48 Controlled Unclassified Information(CUI)
DoDI 8520.02 Public Key Infrastructure (PKI) and Public Key (PK) Enabling
DoDI 8520.03 Identity Authentication for Information Systems
DoDM 1000.13, Vol. 1 DoD ID Cards: ID Card Life-cycle
DoDM 5205.02 DoD Operations Security (OPSEC) Program Manual

Assure Information Sharing

CNSSP-24 Policy on Assured Info Sharing (AIS) for National Security Systems(NSS)
DoDI 8170.01 Online Information Management and Electronic Messaging
DoDI 8320.02 Sharing Data, Info, and IT Services in the DoD
DoDI 8582.01 Security of Non-DoD Info Sys Processing Unclassified Nonpublic DoD Information
CJCSI 3213.01D, Joint Operations Security
CJCSI 6211.02D Defense Information System Network: (DISN) Responsibilities

ANTICIPATE

Understand the Battlespace

FIPS 199 Standards for Security Categorization of Federal Info. and Info. Systems
NIST SP 800-59 Guideline for Identifying an Information System as a NSS
NIST SP 800-60, Vol 1, R1 Guide for Mapping Types of Info and Info Systems to Security Categories
NIST SP 800-92 Guide to Computer Security Log Management
NISTIR 7693 Specification for Asset Identification 1.1
CNSSD-520 Use of Mobile Devices to Process Nat'l Sec.Info Outside Secure Spaces
CNSSP-28 Cybersecurity of Unmanned National Security Systems
DoDI S-5240.23 Counterintelligence (CI) Activities in Cyberspace

Prevent and Delay Attackers and Prevent Attackers from Staying

FIPS 200 Minimum Security Requirements for Federal Information Systems
NIST SP 800-37 R2 Guide for Applying the Risk Mgt Framework to Fed. Info. Systems
NIST SP 800-53 R5 Security & Privacy Controls for Federal Information Systems
NIST SP 800-53A R5 Assessing Security & Privacy Controls in Fed. Info. Systems & Orgs.
NIST SP 800-61, R2 Computer Security Incident Handling Guide
NIST SP 800-124, R1 Guidelines for Managing the Security of Mobile Devices in the Enterprise
NIST SP 800-128 Guide for Security-Focused Configuration Mgt of Info Systems
NIST SP 800-163, R1 Vetting the Security of Mobile Applications
NIST SP 1800-26 Data Integrity: Detecting & Responding to Ransomware
CNSSI-1011 Implementing Host-Based Security Capabilities on NSS
CNSSI-1013 Network Intrusion Detection Sys & Intrusion Prevention Sys (IDS/IPS)
CNSSI-1253 Security Categorization and Control Selection for Nat'l Security Systems
CNSSI-1253F, Atchs 1-5 Security Overlays
CNSSAM IA 1-10, Reducing Risk of Removable Media in NSS
DoDI 5000.90, Cybersecurity for Acquisition Decision Authorities and Program Managers
DoDI 5200.39 CPI Identification and Protection within RDT&E
DoDI 5205.83 DoD Insider Threat and Management and Analysis Center
DoDI 8530.01, Cybersecurity Activities Support to DoD Information Network Operations
DoDI 8531.01, DoD Vulnerability Management
DoDI 8551.01 Ports, Protocols, and Services Management (PPSM)
DoD O-8530.1-M (CAC req'd) CND Service Provider Certification and Accreditation Program
DoDM 5105.21V1, SCI Admin Security Manual: Info and Info Sys Security
DTM 17-007, Ch. 2, Defense Support to Cyber Incident Response
CJCSI 6510.01F Information Assurance (IA) and Computer Network Defense (CND)
CJCSM 6510.01B Cyber Incident Handling Program
CJCSM 6510.02 IA Vulnerability Mgt Program

ABOUT THIS CHART

- This chart organizes cybersecurity policies and guidance by Strategic Goal and Office of Primary Responsibility (see Color Key). Double-clicking* on the box directs users to the most authoritative publicly accessible source.
- *Policies in italics indicate the document is marked for limited distribution or no authoritative public-facing hyperlink is currently available.*
- The linked sites are not controlled by the developers of this chart. We regularly check the integrity of the links, but you may occasionally experience an error message due to problems at the source site or the site's decision to move the document. Please let us know if you believe the link is no longer valid.
- CNSS policies link only to the CNSS site.
- Boxes with red borders reflect recent updates.
- *Note: It is best to open this PDF directly in a browser. However, if you are unable to open the links directly from this PDF document, place your cursor over the target box and right-click to copy the link location. Open a web browser and paste the copied link into the address bar.
- For the latest version of this chart or email alerts to updates go to https://dodiac.dtic.mil/dod-cybersecurity-policy-chart/

Distribution Statement A: Approved for Public Release. Distribution is unlimited.

PREPARE

Develop and Maintain Trust

CNSSP-12 National IA Policy for Space Systems Used to Support NSS
CNSSP-21 National IA Policy on Enterprise Architectures for NSS
NIST 800-160, vol.1, Systems Security Engineering: … Engineering of Trustworthy Secure Systems
CNSSI-5002, Telephony Isolation Used for Unified Comms. Implementations w/ in Physically Protected Spaces
DoDD 3020.40 Mission Assurance
DoDD 3100.10 Space Policy

Strengthen Cyber Readiness

NIST SP 800-207 Zero Trust Architecture
NIST SP 800-18, R1 Guide for Developing Security Plans for Federal Information Systems
NIST SP 800-30, R1 Guide for Conducting Risk Assessments
NIST SP 800-39 Managing Information Security Risk
NIST SP 800-126, R3 SCAP Ver. 1.3
NIST SP 1800-25 Data Integrity: Identifying and Protecting Assets Against Ransomware
NIST SP 800-213 IoT Device Cybersecurity Guidance for the Federal Government
CNSSP-32 Cloud Security for National Security Systems
CNSSD-505 Supply Chain Risk Management
CNSSD-520 The Use of Mobile Devices to Process National Security Information Outside…
DoDD 3700.01 DoD Command and Control (C2) Enabling Capabilities
DoDD S-3710.01 National Leadership Command Capability
DoDI 8140.02 Identification, Tracking, And Reporting of Cyberspace Workforce Requirements
DoDD 5101.21E Unified Platform and Joint Cyber Command and Control (JCC2)
DoDI 8500.01 Cybersecurity
DoDI 8560.01 COMSEC Monitoring

Sustain Missions

NIST SP 800-34, R1 Contingency Planning Guide for Federal Information Systems
NIST SP 800-82, R2 Guide to Industrial Control Systems (ICS) Security
CNSSP-18 National Policy on Classified Information Spillage
CNSSP-22, IA Risk Management Policy for National Security Systems
CNSSP-300 National Policy on Control of Compromising Emanations
CNSSI-1001 National Instruction on Classified Information Spillage
CNSSI-4004.1, Destruction and Emergency Protection Procedures for COMSEC and Class. Material
CNSSI-4007 Communications Security (COMSEC) Utility Program
CNSSI-7000 TEMPEST Countermeasures for Facilities
NSTISSI-7001 NONSTOP Countermeasures
DoDD 3020.26 DoD Continuity Policy
DoDD 3020.44 Defense Crisis Management
DoDD 5144.02 DoD Chief Information Officer
DoDD 8000.01 Management of the DOD Information Enterprise
DoDI 5000.83 Technology & Program Protection to Maintain Technological Advantage
DoDI 8410.02 NetOps for the Global Information Grid (GIG)
ICD 503 IT Systems Security Risk Management and C&A
UFC 4-010-06, Cybersecurity of Facility-Related Control Systems
NSA IA Directorate (IAD) Management Directive MD-110 Cryptographic Key Protection
Defense Acquisition Guidebook Program Protection

Color Key - OPRs

▨	DOD CIO	▨	NIST	▨	USD(I&S)
▨	CNSS/NSTISS	▨	NSA	▨	USD(P)
▨	DISA	■	OSD	□	USD(P&R)
▨	DNI	▨	CYBERCOM	□	Other Agencies
□	JCS	■	USD(A&S)	□	Recently updated policy and/or link
■	NIAP	▨	USD(C)	□	Expired, Update pending

AUTHORITIES

Title 10, US Code Armed Forces (§§2224, 3013(b), 5013(b), 8013(b))
Title 14, US Code Cooperation With Other Agencies (Ch. 7)
Title 32, US Code National Guard (§102)
Title 40, US Code Public Buildings, Property, and Works (Ch. 113: §§11302, 11315, 11331)
Title 44, US Code Federal Information Security Mod. Act, (Chapter 35)
Title 50. US Code War and National Defense (§§3002, 1801)
Clinger-Cohen Act, Pub. L. 104-106
UCP Unified Command Plan (US Constitution Art II, Title 10 & 50)

NATIONAL / FEDERAL

Computer Fraud and Abuse Act Title 18 (§1030)
Federal Wiretap Act Title 18 (§2510 et seq.)
Stored Communications Act Title 18 (§2701 et seq.)
Pen Registers and Trap and Trace Devices Title 18 (§3121 et seq.)
Foreign Intelligence Surveillance Act Title 50 (§1801 et seq)
Executive Order 13231 as Amended by EO 13286 - Critical Infrastructure Protection in the Info Age
Executive Order 13526 Classified National Security Information
Executive Order 13587 Structural Reforms To Improve Classified Nets
Executive Order 13691 Promoting Private Sector Cybersecurity Information Sharing
EO 13636: Improving Critical Infrastructure Cybersecurity
EO 13800: Strengthening Cybersecurity of Fed Nets and CI
NSD 42, National Policy for the Security of Nat'l Security Telecom and Information Systems
EO 13873: Securing the Information and Communications Technology and Services Supply Chain
EO 14028: Improving the Nation's Cybersecurity
NSPD 54 / HSPD 23 Computer Security and Monitoring
PPD 21: Critical Infrastructure Security and Resilience
PPD 41: United States Cyber Incident Coordination
PPD 28, Signals Intelligence Activities
FAR Federal Acquisition Regulation
A-130, Management of Fed Info Resources
Ethics Regulations
Joint Special Access Program (SAP) Implementation Guide (JSIG)
NIST Special Publication 800-Series
NIST SP 800-63 series Digital Identity Guidelines
NIST SP 800-88, R1,Guidelines for Media Sanitization
NIST SP 800-101, R1 Guidelines on Mobile Device Forensics
NIST SP 800-125A, R1, Security Recommendations for Hypervisor Platforms
NIST SP 800-137 Continuous Monitoring
NIST SP 800-209 Security Guidelines for Storage Infrastructure
NISTIR 7298, R3, Glossary of Key Information Security Terms
CNSSD-502 National Directive On Security of National Security Systems
CNSSD-901 Nat'l Security Telecomm's and Info Sys Security (CNSS) Issuance System
CNSSD-900, Governing Procedures of the Committee on National Security Systems
CNSSI-4009 Cmte on National Security Systems Glossary
DoD Information Technology Environment Strategic Plan

OPERATIONAL/SUBORDINATE POLICY

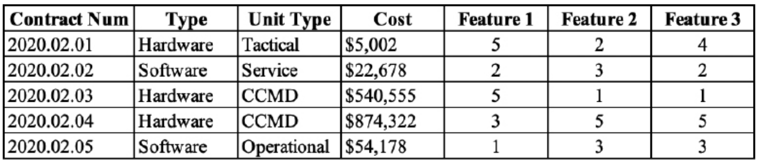
CYBERCOM Orders
JFHQ-DODIN Orders
Security Configuration Guides (SCGs)
Component-level Policy (Directives, Instructions, Publications, Memoranda)
NSA IA Guidance
Security Technical Implementation Guides (STIGs)

Figure 1. Cybersecurity policies and issuances for the DoD.[4]

user to take an action.[6] In human-on-the-loop (HOTL) operations, the machine decides and acts on its own, but a human user supervises its operations and can intervene if necessary.[7] In human-out-of-the-loop (HOOTL) operations, the machine decides and acts on its own, and the human user cannot intervene in a timely fashion.[8] The risk associated with the degrees of autonomy vary and should be carefully weighed based on the intended applications of the machine, the chances of faulty actions to occur, and the severity caused by faulty actions. Given that the purpose of this project is to reduce the risk associated with DoD cyber and IT contracting, we propose that AI recommended contracting clauses and risk determination require HITL acceptance both in modifying contracting language during the contract support process as well as involving commanders to accept contracts of considerable risk with or without language modification. Once implemented, CARE augments, rather than replaces, the human decision-making process.

To develop DoD end user trust in AI, CARE does not remove human involvement and instead harnesses the efficiency of intelligent automation to best inform the human decision-maker.[9] Trust builds as users throughout the contracting chain see tangible benefits from CARE-assisted contracting compared to the standard human-only contracting process.

ML requires data to improve model performance. DoD contracts in document format cannot provide the necessary data to begin training ML algorithms. Natural language processors combined with numerical scoring of contract features must be developed, and contract scoring does not currently exist. Feature engineering is the determination of the appropriate data variables necessary for ML algorithms to assess what the user requires.[10] In other words, poor feature engineering results in subpar model performance. Prior to any data collection for CARE development, DoD contract stakeholders throughout the contracting process with proper AI education must carefully determine the features that will create the contracting data necessary for ML algorithms to work and with the least amount of data bias (Figure 2).



Contract Num	Type	Unit Type	Cost	Feature 1	Feature 2	Feature 3
2020.02.01	Hardware	Tactical	$5,002	5	2	4
2020.02.02	Software	Service	$22,678	2	3	2
2020.02.03	Hardware	CCMD	$540,555	5	1	1
2020.02.04	Hardware	CCMD	$874,322	3	5	5
2020.02.05	Software	Operational	$54,178	1	3	3

Figure 2. Feature engineering example

Development and Operational Concept

In a case study on Army contracting analytic capabilities, the RAND Corporation piloted an effort to make unstructured historical contract data machine readable to forecast a contract's likelihood to have unliquidated obligations.[11] We propose to utilize similar methodologies as RAND in accessing and scoring cyber and IT contracts over a set number of fiscal years with the inclusion of contract performance and contract closeout reports. Contracts would be analyzed by trained cyber and contracting experts and scored on features developed during feature engineering for the data. We seek to score cyber and IT specific contractual language in a tabular format. Proposed feature categories include, but are not limited to, contract duration, contract language, contract outcome, contract performance, adversarial incursion, DoD cyber response, and contract barriers. Close collaboration with data scientists during contract scoring will reduce introducing biased data into the dataset. While RAND utilized over 300,000 contracts with 150 features over three fiscal years, we are unsure how many Army-specific cyber and IT contracts exist at this time.[12] A period of discovery should be included in the CARE development timeline.

Upon completion of contract scoring, developers perform exploratory data analysis to ensure quality data, build and work with predictive models, evaluate models and receive predictions, and refine outputs. CARE determines a contract's risk to DoD and outputs a risk percentage and recommended changes to reduce the risk. A lower risk means that the contract's language provides DoD with favorable execution outcomes. A higher risk percentage suggests that DoD will potentially meet resistance from contractors in response to adverse security events. CARE will recommend specific contractual language modifications and inform end users where that language should go in the contract. Users explore how CARE recommended modifications affect risk, whereby as modifications are selected in the user interface, the contract would be reassessed and the net result displayed in a live risk meter. Users could choose all recommendations or select recommendations, with selections based on the requiring activity's desired combination of potential cost, time, and scope as considerations for risk acceptance. As a HITL system, CARE must rely upon the contracting officer to accept modifications. Cyber and IT contracts continue to be generated by requiring activities, and CARE will be further refined in the future as new data, including CARE augmented contracts, are introduced into the model.

CARE would be a web-portal ML platform with a file upload and document review user interface (Figure 3). Contracting officers upload draft contracts for analysis and interact with recommendations for decision-making analysis only. To reduce the cost and complexity of developing and maintaining CARE, contracting officers transfer recommendations manually into the original document creation software, most likely Microsoft Word or Adobe Acrobat, prior to contract fulfillment. CARE is decision augmentation only. Contracting officers should consult with the requiring activity before accepting any CARE modifications, and risk scores above a certain percentage would require both the requiring activity and contracting commanders to concur. CARE enables commanders to analyze risk, considering risk to the force and risk to the mission against the perceived benefit of the contract.[13]

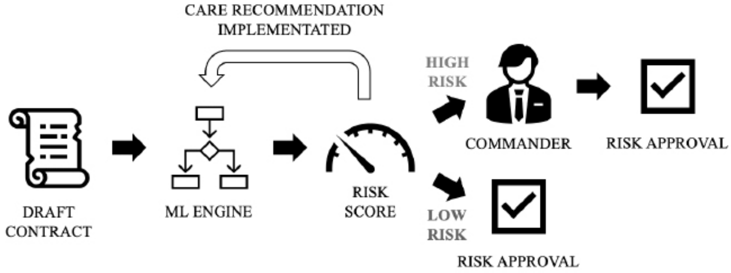


Figure 3. CARE use case

Based upon current development timelines from ML projects being piloted at U.S. Army Forces Command (FORSCOM), we believe that CARE can be rapidly developed with the involvement of data scientists, contract specialists, and cyber security experts in under three months (Figure 4) utilizing the collaborative framework of DevSecOps and agile delivery. We anticipate an additional six to nine months to complete Authorization-To-Operate (ATO) requirements as necessary, working through ML Ops challenges to deploy and maintain models reliably in the production environment, user interface design, and policy decisions. By developing a narrow scope that precisely targets the problem that CARE solves, DoD can responsibly and rapidly prototype and field a platform that decreases contracting risk with immediate and tangible benefits. However, we do acknowledge the risk of the "valley of death" that a successful model development does not guarantee inclusion into a program of record for further sustainment and adoption.

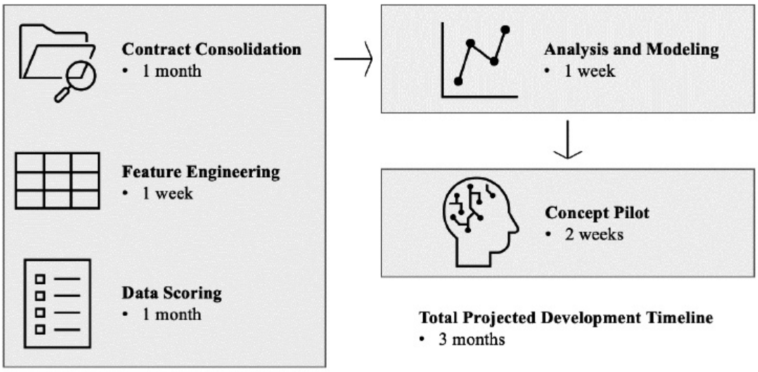


Figure 4. Projected CARE development timeline

CONCLUSION

Cyber-attacks by foreign adversaries and criminal organizations have revealed how the American people and the economy rely on the cyberspace domain. As more DoD operations migrate to the cloud with as-a-service contracting and as DoD activities contract for capabilities to enable a competitive edge in training and in combat, reducing the cybersecurity risk of these contracts is paramount for DoD to defend against and respond to adversarial cyber operations. We recommend that the U.S. Army Materiel Command, assisted by, in coordination with, and potentially developed through the DoD Chief Digital and Artificial Intelligence Office (CDAO), funds and develops CARE. Upon successful pilot testing, it would mandate all cyber and IT contracts to adopt CARE as a critical component in the contract approval process. DoD cannot allow contracting language to cripple America's national security interests. Developing and implementing CARE for DoD cyber contracting will create a more resilient DoD cyber supply chain with the necessary contractual safeguards for DoD to prevent, monitor, and respond to cyber and IT related adversarial events.

NOTES

[1] National Security Commission on Artificial Intelligence, Final Report: National Security Commission on Artificial Intelligence (Washington, DC, 2021), 50.

[2] Paul G. Craft, personal communication, April 20, 2021.

[3] National Institute of Standards and Technology, Information and Communications Technology Supply Chain Risk Management, (Washington, DC: Department of Commerce, 2021), https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Managements/documents/nist_ict-scrm_fact-sheet.pdf.

[4] "Build and Operate a Trusted DoDIN," Defense Technical Information Center, 2022, https://dodiac.dtic.mil/wp-content/uploads/2022/07/2022-06-24-csiac-dod-cybersecurity-policy-chart.pdf.

[5] Dan G. Cox, "Artificial Intelligence and Multi-Domain Operations: A Whole-of-Nation Approach to Success," *Military Review*, 101, no. 3 (May-June 2021): 76-91, https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MJ-21/MJ21-Whole-Book-2.pdf.

[6] Paul Scharre, *Army of None* (New York: Norton, 2018), 29.

[7] Ibid., 29.

[8] Ibid., 30.

[9] Ge Wang, "Humans in the Loop: The Design of Interactive AI Systems," Stanford University, 2019, https://hai.stanford.edu/news/humans-loop-design-interactive-ai-systems.

[10] "Feature Engineering," DataRobot, 2021, https://www.datarobot.com/wiki/feature-engineering/.

[11] William Marcellino et al., *Army Analytic Capabilities: A Case Study Within Army Contracting Command and Its Implications*, RR-A106-1 (Santa Monica, CA: Rand, 2021), 1, https://www.rand.org/pubs/research_reports/RRA106-1.html.

[12] Ibid., 5.

[13] Department of the Army, *Mission Command: Command and Control of Army Forces*, ADP 6-0 (Washington, DC: Department of the Army, 2019), 1-13.

Leveraging the Ontology of the Operational Cyber Mission Stack (OCMS)

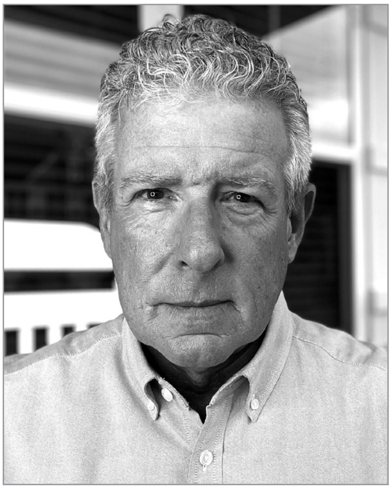
Colonel (Ret.) Jeffrey A. Voice

ABSTRACT

This article aims to identify and clarify a hierarchical construct used by defensive cyberspace planners and operators to aid in mission decomposition, assurance, and terrain mapping. The model enables the visualization of complex relationships and equities between cyberspace assets, resources, and warfighting missions.

At a time when so many Department of Defense mission-essential tasks and functions are cyber enabled, it is more critical now than ever that we strive to model the highly complex cyberspace operational environment in an understandable and useful way. Modeling is a practical means to take logical components of cyberspace, tether them to physical assets, and illuminate how they ultimately support missions. We can then prioritize mission-critical systems and capabilities, organize the defense of those cyberspace elements, and gain confidence we are defending the right things at the right time. While this model is conceptual, it represents a first step toward automating cyberspace terrain mapping that will enable defensive cyber planners and DODIN Cyberspace Forces to respond to the dynamic, man-made terrain that makes up the cyber operational environment.

> "On-tol-o-gy" (computer science) "A structure of concepts or entities within a domain, organized by relationships; a system model."
> – Houghton Mifflin 2016



COL (Ret.) Jeffrey Voice received his commission in the Army Infantry branch after completing studies at Villanova University in 1988. He has served as a Company Commander, Detachment Commander (deployed), Deputy Brigade Commander, S-3, Special Functions Officer, and Plans Team Chief in the special operations community. He also served as a Small Group Leader at the Command and General Staff College (CGSC), Ft Leavenworth, KS, and guest lecturer at the Naval Post-Graduate School (NPS) in Monterey, California where he also studied the Rule of Law and Security, Stability and Development in Complex Operations. During breaks in service, he worked in IT security and technical sales for Qwest Communications while still serving in the U.S. Army Reserve. He currently serves as a Functional Manager and Principal Defensive Cyberspace Warfare Planner for Leidos Corporation at Joint Force Headquarters – Department of Defense Information Networks (JFHQ-DODIN), J35 Future Operations division. jalanvoice@gmail.com

INTRODUCTION

In the progressively complex and dynamic cyberspace environment where, like a submarine commander, we can only perceive our operational environment through a lens of sensor data, it is difficult to connect cyber terrain and assets, to essential tasks and functions supporting warfighter missions. The Operational Cyber Mission Stack (OCMS) applies a conceptual and visual construct to Department of Defense Information Network (DODIN) cyberspace to assist defensive cyberspace planners, asset and mission owners, as well as Cyberspace Operations Forces (COF),[1(1)] identify, map, and understand the environment's operational and digital dependencies.

A significant amount of literature has been dedicated to the network mapping of physical and digital network components and logical protocols, using various models. The most common is the Open Systems Interconnection (OSI) model,[2(2,3)] which standardizes and describes the communication functions of computer systems to visualize network pathways. However, neither the OSI model nor the DoD conceived Transport Communication Protocol/Internet Protocol (TCP/IP)[(4)] model (a construct used to understand Internet protocol relationships) bridges the gap between the physical and logical elements of military cyberspace operations. The OCMS enables a commander to visualize, prioritize, and defend cyber-related elements to achieve mission accomplishment.

What is OCMS?

In Joint Publication (JP) 3-12, Cyberspace Operations, OCMS is characterized as "The ability to visualize cyber terrain, capabilities, and mission essential tasks and

[1] Cyberspace Operations Forces (COF) include all maneuver forces principally tasked with Defensive Cyberspace Operations-Internal Defense Measures (DCO-IDM) and DODIN Operations (DODIN Ops), including but not limited to Cyber Protection Teams (CPTs), Cyber Security Service Providers (CSSPs), Incident/Emergency Response Teams, et al.

[2] Hubert Zimmermann, "OSI Reference Model- The ISO Model of Architecture for Open System Interconnection" IEEE transaction on communications, vol.28, issue 4, April 1980. Zimmermann et al., proposed a model for architecture for Opens Systems interconnection developed by SC16. He gave some indications on initial sets of protocols that have now been developed in the OSI reference model.

[3] Michael Scheidell, "Three Undocumented Layers of the OSI Model and Their Impact on Security," SECNAP Network Security Corporation.

[4] Microsoft," TCP/IP protocol architecture" 2007.

objectives, facilitates cyberspace operations' primary purpose, which is to achieve objectives in or through cyberspace." The OCMS is a conceptual hierarchy and tool that enables visualization thereby revealing and clarifying relationships between the physical and logical layers of cyberspace.

Toward understanding

Joint Force Headquarters-Department of Defense Information Networks (JFHQ-DODIN) Subordinate Campaign Plan's (SCP) first Line of Effort is "Understand." This is further defined in three Supporting Lines of Effort (SLOEs), the first of which is the environment.[4] Operational planners, Area of Operations Commanders/Directors (CDRs/DIRs), and Mission-based/Functional Sector CDRs/DIRs seeking a greater understanding of their environment must employ a conceptual hierarchy to gain a better appreciation of the inherent vulnerabilities and relationships in the joint cyberspace operating environment.

Visualizing and mapping these mission elements up (or down) OCMS reveals which cyber terrain and assets are required to support a particular mission and how they relate to one another. This holistic analysis aids the identification of logical elements and physical nodes or assets necessary to support mission assurance.

A typical cyber mission stack is shown in Figure 1, supporting a notional Maritime Logistics mission. This example shows the Line of Separation (shown as a horizontal dotted line) represents the demarcation between physical cyberspace elements such as Mission Relevant Terrain-Cyber (MRT-C), nodes or assets (below the line), and logical operational elements such as capabilities, mission essential tasks/functions (METs/MEFs), and objectives listed above the line.[(5)]

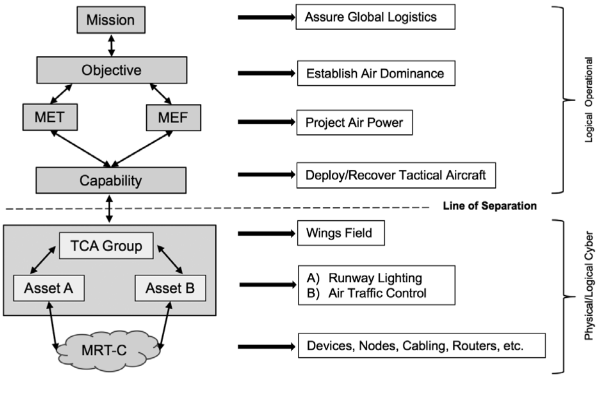


Figure 1. Typical Cyber Mission Supporting a Notional Maritime Logistics Mission.

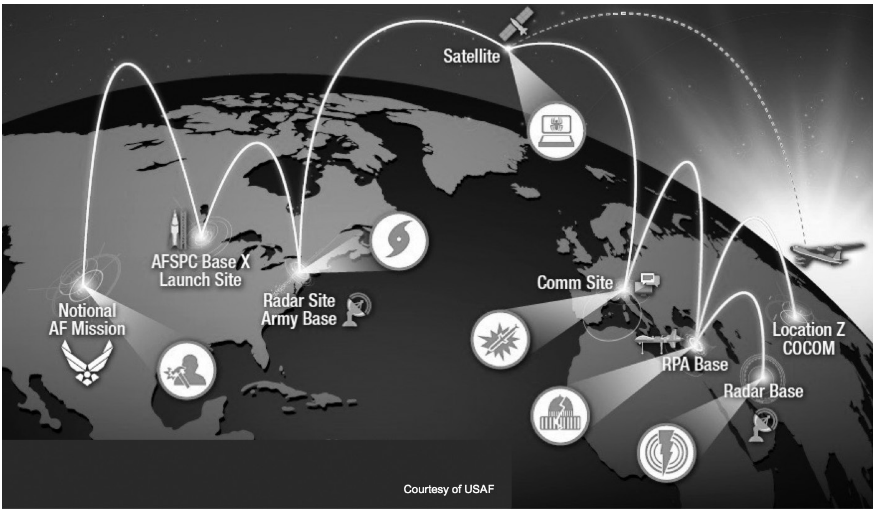
It is important to recognize that Defensive Cyberspace Operations-Internal Defensive Measures (DCO-IDM)[5] and DODIN Ops planners focus on friendly (Blue) cyberspace to enumerate

[5] It is important to note that in accordance with JP-5 Joint Planning, "Tasks direct friendly actions to create desired effect(s). These are the discrete activities directed in the campaign plan used to influence the OE. The execution of a task will result in an effect." For simplicity in illustrating the model, "effects" are omitted herein.

Assets deemed critical to a Commander's mission are referred to as Task Critical Assets or "TCAs." Where they are critical to strategic missions, they are referred to as Defense Critical Assets or "DCAs."

assets and capabilities which enable or create effects in cyberspace (and occasionally physical domains) to protect and defend them. Conversely, offensive cyberspace planners look beyond the DODIN boundary into neutral (Grey) or adversary (Red) cyberspace terrain to develop Cyberspace Effects Operations (CEO) based on a commander's objectives.

What is significant about these divergent organizational approaches is that in planning and executing defensive actions in friendly cyberspace, COF need to look inward to accurately *identify and prioritize* which cyberspace elements are most essential and most vulnerable according to mission imperatives and phases of operation[6] rather than merely executing threat agnostic contiguous defense measures.



Courtesy of USAF

Figure 2. Example of Geographic Distribution of Assets.

What does it do?

The stack enables visualization, prioritization and integration of equities, dependencies, and assets with operational capabilities, tasks, and objectives through a logical mission thread.[7] For instance, elements necessary to carry out a notional Air Force mission like the one depicted in Figure 2[8] may be diverse and distributed geographically around the globe. Their nature and distribution may obfuscate the equities and dependencies the OCMS model endeavors to clarify.

The cyber portion of the mission thread associates two of the three layers of cyberspace (the logical network layer and the physical network layer,[6] with operational warfighting imperatives or elements. It does so by modeling the operational cyber environment to allow the viewer to identify and connect cyberspace entities (physical and logical) supporting a mission. It further

[6] Phases of military operations typically begin with OPLAN approval. Operations ideally begin and end with Phase 0/Shape. Execution of the EXORD or OPORD activation begins the remaining phases. These phases consist of the following: Phase 1/Deter, Phase 2/Seize Initiative, Phase 3/Dominate, Phase 4/Stabilize, and Phase 5/Enable Civil Authority.

[7] A "mission thread" is an operational and technical description of the end-to-end set of activities and systems that accomplish the execution of a joint mission.

[8] Courtesy of United States Air Force, Mission Thread Analysis Overview, A.F. Energy Assurance, safie.hq.af.mil/Installation Energy.

informs the interoperability and dependency of diverse critical assets and cyber terrain supporting one or more critical capabilities.

Why do we need a model?

The ability to deconstruct and understand the interrelation of dependencies increases in complexity and importance as we widen the lens through which we visualize mission composition. The widening of that lens reveals a complex lattice of supporting and supported relationships.

Dependencies and equities become more intricate as cyberspace elements support multiple assets, capabilities, METs/MEFs, missions, etc. For example, the unshaded area in Figure 3(i) shows two task-critical assets (TCAs) supported by common MRT-C. In Figure 3(ii), we

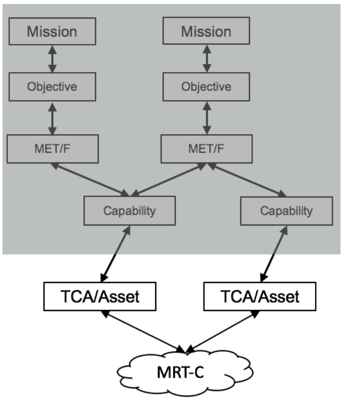


Figure 3 (i). MRTC Supporting Two Task Critical Assets/Assets.

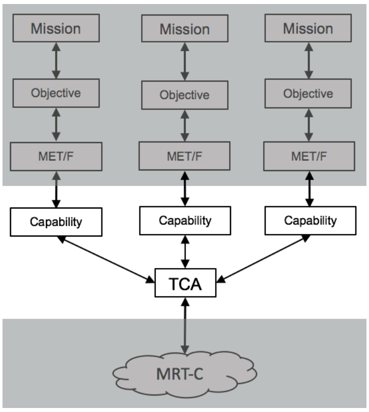


Figure 3 (ii). TCA/Asset Supporting Multiple Capabilities.

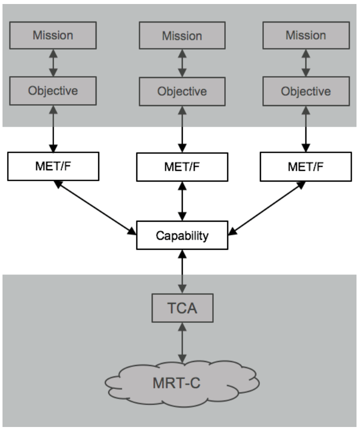


Figure 3 (iii). Capability Supporting Multiple Mets/Mefs.

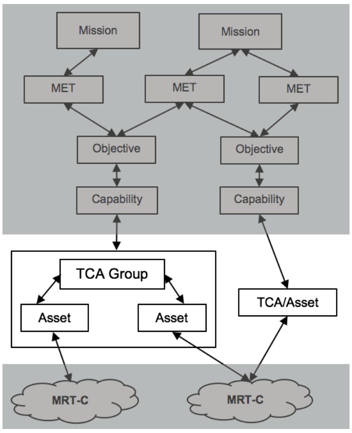
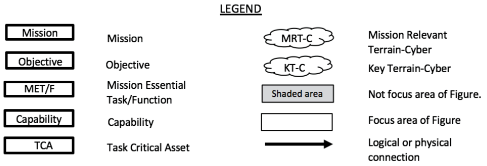


Figure 3 (iv). Multiple Assets Supporting Diverse Capabilities.



see a single TCA supporting multiple capabilities. Figure 3(iii) shows a single capability supporting multiple mission essential tasks or functions (MET/MEF). Finally, in Figure 3(iv), we can see multiple assets supporting diverse capabilities.

Where a series of critical assets are required to enable a capability, they are referred to as a TCA or Asset Group.[7] TCA Groups can be particularly problematic for mission decomposition since it is the aggregate of the assets that enable a capability. A failure of any of the supporting assets can disable the capability. An example might be a Terminal High Altitude Area Defense (THAAD) system, which requires an interceptor, launch vehicle, radar, and fire control system. Each of those elements may be identified as an asset supporting a TCA.

Figure 4 further widens the lens and shows a Mission Owner (also referred to as a Sector Commander [CDR] or Director [DIR])[(9)] supporting multiple Lines of Effort (LOEs) that may include multiple missions. Using OCMS, we can see that the relationship between objectives, tasks, capabilities, and assets increases exponentially. Increasing these elements means increasing the complexity of the supporting and supported relationships to be considered as well.

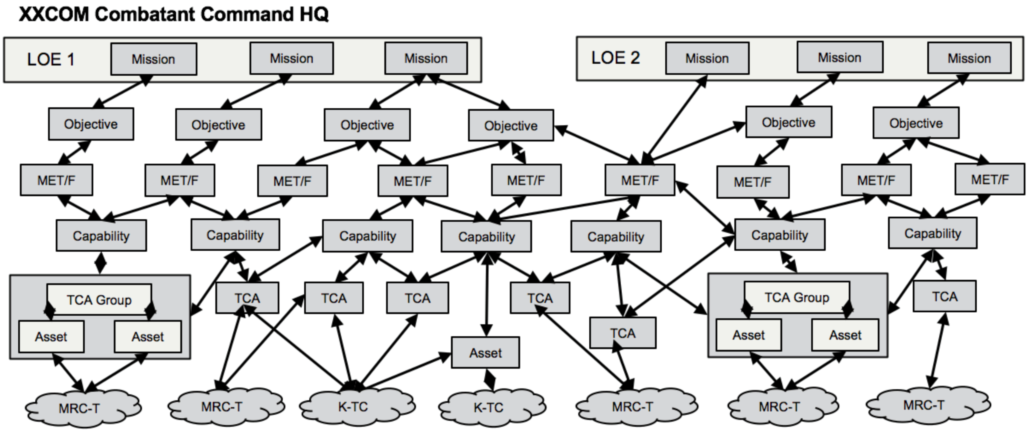


Figure 4. EOCMS Supporting Multiple Loes/Loos.

As the perception aperture continues to widen and becomes more inclusive during mission decomposition, we can see in Figure 5 that a contingency or campaign plan may involve multiple components (DODIN Sector CDRs/DIRs), each supporting multiple LOEs. Their missions are in turn supported by multiple assets provided by DODIN Area of Operation (DAO) CDRs/DIRs (asset owners or resource providers).

It is important to understand that while Mission Owners (such as Combatant Commanders [CCDRs]) are responsible for mission assurance and accomplishment, they are at the same time dependent on multiple assets provided by DAO CDRs/DIRs to accomplish those missions. They are also concurrently acting as DAO CDRs/DIRs providing capabilities to support their own missions and those of others.

[9] The DODIN Area of Operation (AO) and Sector construct is discussed briefly later in this article.

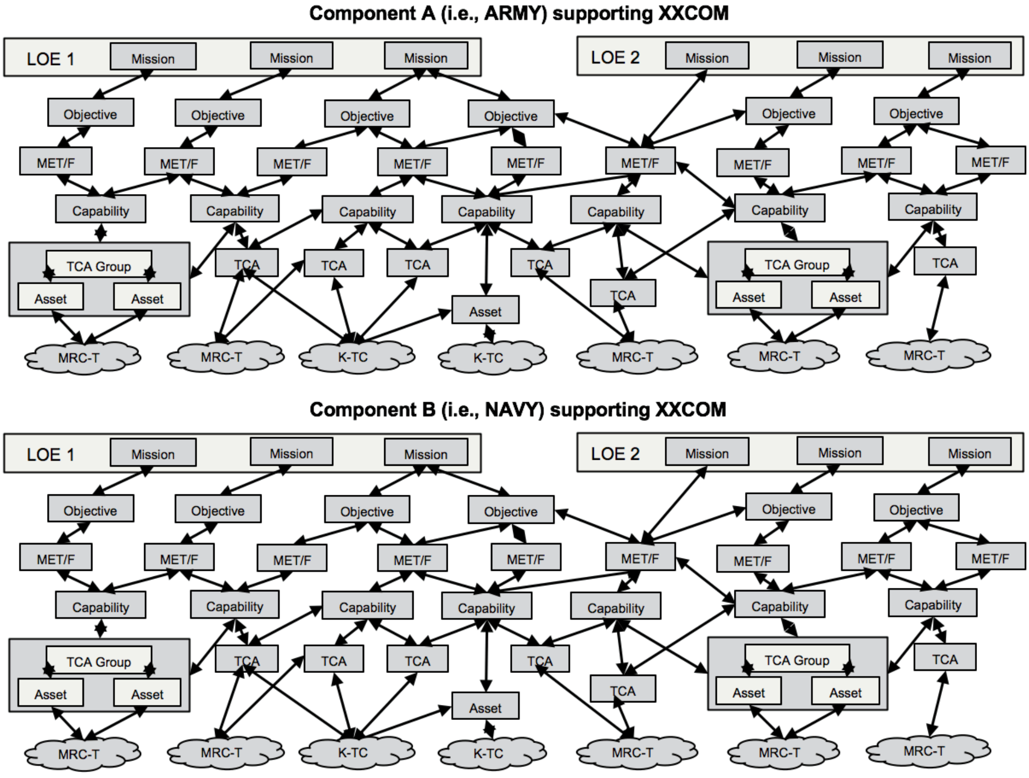


Figure 5. OCMS Supporting Multiple Components Each Supporting Multiple Loes/Loos.

If we accept that DoD Components, such as military service components or other CCMDs, may be acting as a Sector CDR/DIR (Mission Owner) while also acting as a DODIN AO CDR (a resource or asset provider facilitating a variety of capabilities by way of their own assets), then we must also accept that the task of identifying, tracking, and managing those equities and relationships becomes massive and daunting. As a result, because cyber equities and relationships are so entwined and complex, a method or construct like the OCMS is helpful if not imperative.

In support of the concept of Battlespace Awareness, U.S. Cyber Command (USCYBERCOM) Operational Guidance 3-2, "Defensive Cyberspace Operations," cites the six joint functions which underpin the execution of operations in all warfighting domains. The Command-and-Control section discusses the importance of this awareness and states that "visualization must encompass all layers of cyberspace, providing functional mapping of cyberspace objects to the objectives they support; as well as the disposition and status of friendly and adversary forces within the terrain."[8]

OCMS supports the concept of battlespace awareness as it promotes functional and operational identification and mapping of cyberspace objects, such as MRT-C and assets, to the objectives and missions they ultimately support. The increased awareness of the defensive cyber battlespace also facilitates a commander's and COF's ability to prioritize assets and terrain in support of mission assurance by revealing relevant, key or decisive terrain.

KEY TERRAIN-CYBER (KT-C)

KT-C—cyber terrain that affords a marked advantage to the combatant who holds or controls it—can be identified using the OCMS model to unpack, analyze, and understand operational requirements, mission objectives, and vulnerabilities (i.e., single points of failure). It is important to note that KT-C, much like key terrain in other warfighting domains, can change as operations or campaigns mature.

For example, because we are essentially a commuter military, cyber terrain that enables Global Logistics may be more critical and nuanced during Phase I: Deter as forces are being built up than during Phase III: Dominate when demands may decrease as commanders might seek solely to sustain forces. As DoD COF strive to maneuver and defend KT-C, it is wise to be mindful that "unlike maneuver[ing] in the physical world, it will sometimes take place at machine and network speeds on terrain that constantly shifts."[9]

THE OPERATIONAL ENVIRONMENT (OE)

It is essential to recognize that cognizance of the fidelity of situational awareness is proportionate to the speed at which the cyberspace operational environment evolves: "Understanding the relationship of terrain to mission is critical in the development of Defensive Preparation of the Operational Environment" (DPOE).[10] This is principally because, unlike other domains that are bound by more significant corporeal restrictions, like the first law of motion that can dictate how fast a missile may fly or how far a tank may fire, cyberspace's fundamental and foundational physical restriction within the domain is the speed of light. The effects of executed capabilities can, in some cases, be delivered in nanoseconds. Further, those effects can be delivered at that speed globally.

Because cyber effects may be delivered instantly anywhere on the globe (or in Earth's atmosphere), defending the DODIN is a global responsibility. This responsibility was formally tasked to JFHQ-DODIN by USSTRATCOM as recently as 2016. Specifically, the Commander of JFHQ-DODIN was ordered to "plan, execute, direct, coordinate, and assess the execution of global DODIN operations and DCO-IDM in coordination with affected combatant commands (CCMDs) and DoD Components."[11] This codified and operationalized the global responsibility for the defense of friendly cyberspace (DODIN) and all it encompasses.

This global responsibility is reinforced and confirmed by the now Unified Functional Combatant Command, USCYBERCOM, in its 2019 Campaign Order. The order states: "USCYBERCOM and its components (JFHQ-DODIN among them) will operate in a global domain within the information environment consisting of the interdependent networks of information technology (IT)...USCYBERCOM designates JFHQ-DODIN as the main effort for the protection of the DODIN."[12]

Therefore, because cyberspace is unlike other warfighting domains and JFHQ-DODIN maintains global reach and responsibility for defense of the DODIN, it is important to recognize "the nature of cyberspace dictates that the area of operations, influence, or interest are not constrained by geographic or political boundaries, and this may lead to rapid expansion or contraction of these areas."[13] This defines cyberspace as truly dynamic.

AO/SECTOR CONSTRUCT

The OCMS hierarchy supports Intermediate Military Objective One (IMO 1) articulated in JFHQ-DODIN's "Operation Gladiator Shield 2017"[14] which directed Combatant Commanders, Service Components, Agencies, and Field Activities to organize the cyber battlespace according to the DODIN AO and DODIN Sector construct.[15] This objective represented a major step toward structuring a manageable and defendable DODIN battlespace.

While AO is used in the construct to mean "Area of Operations," it can also almost interchangeably represent "Asset Owners" since it is the DODIN AO CDRs/DIRs that usually purchase, operate, maintain, and protect critical assets. An excerpt from USCYBERCOM FRAGORD 1 to OPORD 17-0114 states, "an Area of Operation (AO) when established within the DODIN, is defined by the commander's or director's authority to direct DCO-IDM and DODIN Ops."[16] Since we know that DODIN AO CDRs and DIRs are asset owners, this illustrates an orientation toward the assets and terrain which reside below the line of separation (Figure 1) on the OCMS. As previously alluded to, this is an inward orientation to cyberspace operations.

A subsequent passage from the same order states, "Sectors are established to reference DoD core functions and the corresponding commands, agencies, and field activities that are supported and/or impacted by a cyberspace incident or event."[17] This illustrates a focus on functions, tasks, and capabilities that enable a mission above the Line of Separation on the OCMS. The DODIN AO/Sector construct, and its orientation to assets or functions, becomes evident when using OCMS and thereby enables the decomposition of a mission and identification of which assets are supporting which capabilities.

The Need for Automation

Because the relationships among elements are so complex, the dependence of METs and MEFs on cyber is so great, and because the terrain is subject to morphing at the speed of fiber optics, there is a clear need for an automated platform or technology to aggregate and make network visualization available across all Sectors and DAOs. The Mission Assurance Decision Support System (MADSS) has been designated by the Chairman of the Joint Chiefs of Staff as the program of record for mapping DODIN cyber terrain and assets that support operational warfighting requirements. The implementation of that mission assurance platform was further ordered by CDRUSCYBERCOM in January of 2017.[18]

However, the current input of data into MADSS is a painstakingly manual process. Because cyber terrain can change so rapidly in ways that may have unexpected consequences, it is important that a fully automated strategy be implemented as soon as possible. Regardless of which platform is used, it is important to remember that because cyberspace is a man-made warfighting domain which "adds global reach, often at nearly instantaneous speeds,"[19] and because its terrain evolves and changes constantly, some form of advanced automation if not artificial intelligence will ultimately be necessary to deliver a real-time accurate visualization of the cyberspace operational environment. This automation will add immeasurably to a commander's ability to establish and maintain a cyberspace common operating picture (COP).

CONCLUSION

Because of the complexity of the cyberspace warfighting domain, it is necessary to have a mechanism or model (like OCMS) to unpack and visualize the myriad physical and logical connections and dependencies between all cyberspace elements represented in OCMS, to identify and protect operational elements supporting warfighters conducting kinetic or cyberspace operations. As stated earlier, understanding the relationship of objects in the hierarchy of the Operational Cyber Mission Stack is essential in decomposing and assuring a mission.

The model advanced in this article helps cyber planners, defenders, and mission commanders visualize and define the friendly cyberspace environment. This visualization allows the user to better track and prioritize physical and logical elements of cyberspace, going from micro to macro views of the OE as it evolves and changes on a global scale.

NOTES

1. Joint Force Headquarters – Department of Defense Information Networks (U) "OPORD 19.0005 Fight the DODIN," *Operation Order Gladiator Shield 2019*, Ft Meade: Department of Defense, February 8, 2019.
2. Hubert Zimmerman, "OSI Reference Model- The OSI Model of Architecture for Open Systems Interconnection," *IEEE Transactions on Communication*, IEEE, April, 1980.
3. Chairman of the Joint Chiefs of Staff, "(U) JP 3-12," *Cyberspace Operations*, Washington, D.C.: U.S. Department of Defense, June 8, 2018.
4. United States Cyber Command, "(U//FOUO) DODIN Operations and DCO-IDM." *Subordinate Campaign Plan*, Ft Meade, MD: United States Cyber Command, December 11, 2017.
5. United States Cyber Command, "(U) Doctrine for Cyberspace Operations." *Publication 1.* Ft Meade, MD: USCYBERCOM, June 15, 2016.
6. Chairman of the Joint Chiefs of Staff, "(U) JP 3-12." *Cyberspace Operations,* Washington, D.C.: U.S. Department of Defense, June 8, 2018.
7. Joint Force Headquarters – Department of Defense Information Networks, "(U) Asset Defense Plan/ Resource Document," Ft Meade, MD: Dept of Defense, June 2019.
8. United States Cyber Command, (U) "Operational Guidance," *Defensive Cyber Operations*, Ft Meade, Maryland: United States Strategic Command/United States Cyber Command, March 2017.
9. Gregory Conti and David Raymond, *On Cyber: Towards an Operational Art for Cyber Conflict,* Kopidion Press, 2017, 88.
10. United States Cyber Command, (U) "Operational Guidance," *Defensive Cyber Operations.*
11. United States Strategic Command, "USSTRATCOM EXORD." (U) *EXORD 16-04,* Department of Defense, February 10, 2016.
12. United States Cyber Command, (U) "*Campaign Operation Order 8500-19 Base Order,*" Ft. Meade, MD: Department of Defense, 2019.
13. United States Cyber Command, (U) "*Operational Guidance, Defensive Cyber Operations 3.2.*"
14. Joint Force Headquarters – Department of Defense Information Networks "(U//FOUO) OPORD 17-0318," *Operation Gladiator Shield Implementation*, Ft Meade, MD: Department of Defense, December 20, 2017.
15. Joint Force Headquarters – Department of Defense Information Networks "(U//FOUO) OPORD 17-0318."
16. USCYBERCOM, "(U) FRAGO 01 to *OPORD 17-0114," Designation of Named Areas of Operation*, Ft Meade, MD: Department of Defense, July 2018.
17. USCYBERCOM, "(U) FRAGO 01 to *OPORD 17-0114," Designation of Named Areas of Operation*, Ft Meade, MD: Department of Defense, July 2018.
18. (U) USCYBERCOM "(U) TASKORD 17-0008" *Mission Assurance Decision Supprot System (MADSS) Capabilities*, Ft Meade, MD: Department of Defense, January 10, 2017.
19. Conti and Raymond, *On Cyber: Towards an Operational Art for Cyber Conflict*.

The Cyber Defense Review

◇ Research Articles ◇

The UN Cyber Norms: *How Do They Guide the Responsible Development and Use of Offensive Cyber Capabilities?*

Bart Hogeveen

ABSTRACT

In this article, I review how the international cybersecurity norms, agreed to in 2015 and reaffirmed in 2021 by the member countries of the United Nations (UN), provide guidance to states on their possession and use of offensive cyber capabilities. This is an important exploration given that UN negotiations have reached a provisional climax, and that more states, ranging from major cyber powers to developing cyber nations, are getting involved with offensive cyber activities. I consider the 11 UN norms and extract the specific guidance they offer both to states that conduct offensive cyber operations and to states who have been attacked by offensive cyber activities. Then, I consider the various types of cyber operations that could affect international peace and security before looking at ways through which governments, international bodies and communities of non-governmental organizations can support observance of the UN norms. Finally, I assert that responsible forms of offensive cyber will not be for all states, and that raising the bar – including through the UN norms – benefits all major cyber powers.

At the informal intersessional consultative meeting of the UN Open-ended Working Group (OEWG) on information and communications technology (ICT) security in December 2019, Microsoft's vice-president for Customer Security and Trust, Tom Burt, wanted to send a strong message to the assembled representatives of UN member countries: the security, safety, and stability of cyberspace is in imminent danger and, to prevent further escalation, countries should stop misusing

Bart Hogeveen is the Head of Cyber Capacity Building at the Australian Strategic Policy Institute. In this role, he focuses on international peace and security, international aid, and national security aspects of cyber and digital issues in the Indo-Pacific region. Together with ASEAN-based think tank partners, he authored the Sydney Recommendations on Practical Futures on Cyber Confidence Building in the ASEAN region (2018). With support from the UK Foreign, Commonwealth and Development Office and the Australian Department of Foreign Affairs and Trade, Bart directed a multiyear capacity-building effort supporting the implementation of the UN cyber norms in the ASEAN region between 2019 and 2021. His report, "The UN norms of responsible state behaviour in cyberspace. Guidance on Implementation for Member States of ASEAN," was published in March 2022.

cyberspace for offensive operations.[1] In the accompanying written submission, Microsoft stated that it was analyzing "trillions of signals" in an effort to "identify sophisticated threats and protect our customers from a diverse and growing number of nation-state actors."[2]

In 2018, the UN General Assembly established this OEWG to further develop norms for states' responsible cyber behavior, explore ways to implement them, and, when necessary, introduce changes or additional rules of behavior.[3] After two years of negotiations, the working group concluded in 2021 with a reaffirmation of 11 voluntary and non-binding norms that were first agreed in 2015.

The 11 UN cyber norms set out eight positive steps that states should take, and three actions states should avoid.[4] States are recommended to implement the following actions:

- Cooperate to increase stability and security in cyberspace
- Consider all relevant information when attributing cyber incidents
- Prevent criminal and terrorist use of information and communications technologies
- Respect human rights—including privacy—online
- Take appropriate measures to protect critical infrastructure from cybersecurity threats
- Respond to reasonable requests for assistance from another state
- Take steps to protect the integrity of supply chains for ICT products, and
- Report ICT vulnerabilities in a responsible manner

And states should refrain from the following actions:

- Knowingly allow their territory to be used to commit internationally wrongful acts using cyber tools

- Conduct cyber activities that damage the delivery of essential services by critical infrastructure in another country
- Harm another country's Computer Emergency Response Team (CERT) or use their national CERT to engage in malicious cyber activity

Throughout the tenure of the OEWG negotiations, between 2019 and 2021, the message from industry, civil society organizations and thinktanks was that governments should act in a more diligent, forthcoming, and sincere way in complying with their self-agreed norms.[5] This is a challenge when compliance is based on political and moral grounds and detailed guidance, case-studies and verification methods are absent.

As more states (both major cyber powers as well as developing cyber nations) add offensive tools to their portfolio of cyber capabilities, so should the accountability and reassurance measures. Therefore, the main question that I intend to answer in this article is: How does the existing set of UN norms provide relevant guidance for states in their efforts to responsibly develop, possess, and deploy offensive cyber capabilities?

Competition and conflict among states and their use of cyber tools as levers of political, military, and economic coercion are generally regarded as threats that can potentially destabilize the integrity of cyberspace and societies that rely on trust and confidence in the digital environment.[6] Since 2015, the number of state-sponsored cyber operations and significant cyber incidents that have become publicly recorded or acknowledged has grown significantly (See figure 1).

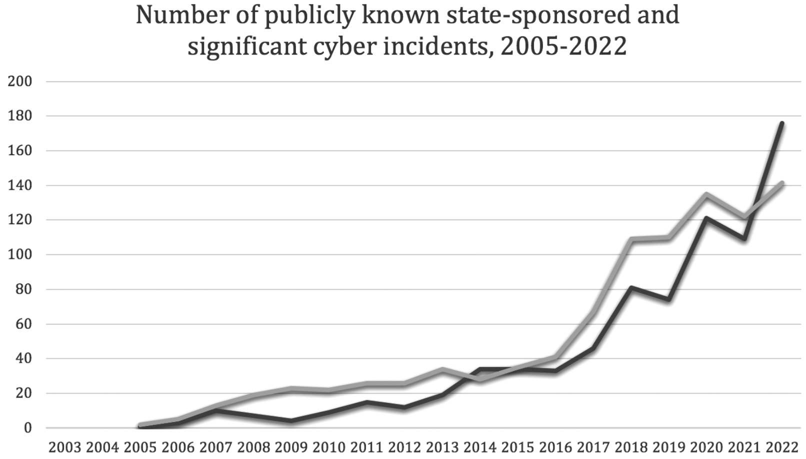


Figure 1. Based on number of entries per year from Council on Foreign Relations' Cyber Operations Tracker (black line) and the Centre for Strategic and International Studies' List of Significant Cyber Incidents (gray line).

Specifically, the governments of Russia, China, North Korea, and Iran have attracted the ire of western states for sponsoring offensive cyber operations. In July 2021, a grand coalition of the US, UK, Australia, Canada, New Zealand, Japan, the EU, and NATO called out the Chinese government for a prolonged campaign of espionage that sought commercial and personal profit,[7] discovered and exploited zero-day vulnerabilities in Microsoft Exchange servers[8] and aided "the widespread and reckless sharing of the vulnerability."[9]

The public statements accompanying the attribution refer to internationally agreed norms of responsible state behavior.[10] In this case, among other things, China was called upon to honor its commitment not to "knowingly allowing its territory to be used for internationally wrongful acts using ICTs" (UN norm #3). After being notified, China should have taken "reasonable steps within its capacity to end the on-going activity in its territory," which it declined. Moreover, should Beijing lack the capacity to address these issues, norm #8 suggests it should have considered seeking outside assistance, which it did not.

There are, however, commitments that the attributing states had to uphold as well. UN norm #2, for instance, recommends that states "consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment, and the nature and extent of the consequences."[11] They should also keep in mind that "an ICT incident emanating from the territory or the infrastructure of a third state does not, of itself, imply responsibility of that state for the incident."[12]

Overall, the practice of publicly attributing acts of offensive cyber appears a bit one-sided. All documented attributions have originated from western governments, dominated by Five Eyes nations, which have declared their own possession of offensive cyber capabilities and a willingness to use them. In fact, the US, UK, Australia, as well as the Netherlands, Denmark, and Sweden have confirmed they have conducted offensive operations.[13]

Despite ample public evidence to the contrary,[14] officials representing the governments of China, Russia, and Iran have continued to deny their country's possession, and use of offensive cyber capabilities.[15] In international forums, Beijing, Moscow, and Tehran have gone to great lengths to object to any language that would normalize what they call the militarization of cyberspace.[16] They capitalize on sentiments expressed by developing cyber nations, such as through the Non-Aligned Movement, which feel overwhelmed by the capabilities of major cyber powers.[17]

This case illustrates how the UN norms can be used to guide state practice. There are certain rules, principles, or norms—either explicit or implied—that determine a 'zone of acceptable behaviour' when it comes to the possession and use of offensive cyber capabilities and any state's (counter)responses. At the same time, today ample latitude remains for states to deny or circumvent their responsibilities and dodge accountability.

Are the 2015 UN Norms Relevant for the Future of Offensive Cyber?

Efforts to build an international regime for managing inter-state cybersecurity issues started as early as 1998. One of the milestones has been the endorsement by the UN General Assembly of Resolution 70/237 in 2015, which calls on all states to use the UN framework for responsible state behavior. This framework is based on the recognition that international law applies to state behavior in the cyber domain and is further complemented by 11 voluntary and non-binding norms; various confidence-building measures, particularly to strengthen transparency, predictability, and stability, and; a commitment to global capacity building.[18]

The set of 11 norms probably provides the most practical guidance regarding what is expected of states in their use of ICTs.

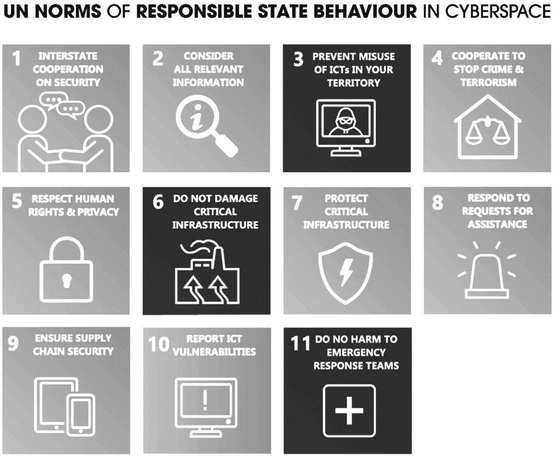

UN NORMS OF RESPONSIBLE STATE BEHAVIOUR IN CYBERSPACE
1 INTERSTATE COOPERATION ON SECURITY
2 CONSIDER ALL RELEVANT INFORMATION
3 PREVENT MISUSE OF ICTs IN YOUR TERRITORY
4 COOPERATE TO STOP CRIME & TERRORISM
5 RESPECT HUMAN RIGHTS & PRIVACY
6 DO NOT DAMAGE CRITICAL INFRASTRUCTURE
7 PROTECT CRITICAL INFRASTRUCTURE
8 RESPOND TO REQUESTS FOR ASSISTANCE
9 ENSURE SUPPLY CHAIN SECURITY
10 REPORT ICT VULNERABILITIES
11 DO NO HARM TO EMERGENCY RESPONSE TEAMS

Figure 2 The UN norms of responsible state behaviour in cyberspace. Source: https://www.aspi.org.au/cybernorms.

Since 2015, three more rounds of negotiation have taken place. A setback was encountered when the Group of Governmental Experts (GGE) 2016-17 failed to reach a consensus. Disagreements remained over the application of international law, the right to self-defense, the principle of state responsibility, and legal bases for countermeasures in response to a cyber incident.[19] The latest two rounds, the Open-ended Working Group and sixth GGE which occurred in parallel in 2019-21, were successfully concluded. This reestablishment of consensus among the OEWG and GGE members has been hailed as a diplomatic triumph.[20]

Negotiators were able to add references to cybersecurity threats affecting electoral processes and health infrastructure,[21] and to rebut claims that "the consensus of the past is not the consensus of the present."[22] Besides this, however, the national delegations were only able to agree to a reconfirmation of the previous agreement from 2015. Therefore, it is reasonable to assume that negotiations have now reached their provisional climax, and the reach and breadth of the framework will not be expanded in the near future.

At this point in time, the UN framework of responsible state behavior in cyberspace is the only globally recognized point of reference to assess what is and what is not responsible state use of cyber tools in the context of international peace and security. Hence, negotiators have shifted their attention to deepening their understanding of the practical implications of the current framework, in particular the norms.[23] These could include guidance on responsible use of offensive cyber capabilities, requirements for oversight and accountability, and recommended operational policies, skills and safeguards a state should be able to demonstrably possess—now and into the future. There may also be certain monitoring and reporting roles that could be taken up by academia, civil society organizations, and industry to increase transparency, accountability, and strengthen collective reassurance.

For this article, offensive cyber capabilities refer to a state "possessing the resources, skills, knowledge, operational concepts and procedures" to conduct offensive cyber operations which are "operations to manipulate, deny, disrupt, degrade, or destroy targeted computers, information systems or networks."[24] As I am focusing on international peace and security, I consider a cross-jurisdictional element as a factor in offensive cyber operations.

There is no implied suggestion that states should develop offensive cyber capabilities or consider their use, let alone that this would be a positive development for international peace and security. However, it is taken as a matter of fact that states are increasingly working on developing sophisticated offensive cyber capabilities and that more states, for different reasons, will get involved with offensive cyber capabilities in the future.

Can the Future of Offensive Cyber be Assessed through the UN Norms?

With the agreed upon UN cyber norms, the activities, intentions, and policies of states can be subjected to assessments.[25] States can be complimented for their response to an incident, or national practices can be heralded as global good practice. Also, states can be reprimanded if they have not done enough to prevent an incident, or that they have used cyber capabilities in an irresponsible manner.[26]

The language reflected in the current text of the norms is a result of concerns and opinions following cyber and information security incidents that occurred up to 2015 such as the 1999 wars in Kosovo and Chechnya,[27] the Olympic Games/Stuxnet[28] operation against Iran, and the Snowden revelations.[29] Since then, there have been attempts to introduce additional norms, notably the idea of protecting the "core of the internet" (promoted by the Netherlands), to prohibit cyber-enabled theft of intellectual property for commercial purposes (promoted by the US) and including the application of international humanitarian law (IHL); spearheaded by the International Committee of the Red Cross (ICRC). Although the GGE in 2021 agreed to note that IHL applies as well as the applicability of its underpinning legal principles,[30] neither the GGE 2016-17 nor the two 2019-21 groups succeeded to expand the original 11 norms.

There have also been proposals from civil society organizations and the IT industry to expand the remit of the UN norms and make them apply to issues of digital rights, cybercrime, and digital development. However, UN member states have rebuked this sentiment and maintain that the norms should focus on cybersecurity issues *that affect inter-state relations*.[31] While recognizing the multi-stakeholder nature of the cyber domain, in particular ownership of key tenets of infrastructure by the private sector, governments also held on to their primary responsibility to ensure safety and security in inter-state cyber relations.[32]

The norms are seen as a means for states to prevent and mitigate the worst of all cyber incidents, i.e., those intentionally or inadvertently perpetrated by governments in the context of political-military tensions or economic conflicts. Offensive cyber falls squarely within this context. Additionally, the UN norms serve as a foundational source from where to deduce specific guidance on responsible state use of ICTs and should be used to assess current state behavior and draw red lines for future reference. In fact, the 2021 reports of both the OEWG and GGE introduced a line calling on states "to avoid and refrain from the use of ICTs not in line with the norms of responsible State behaviour."[33]

How do the UN Norms Examine Offensive Cyber?

The UN working groups that were established to consider international cybersecurity were, among other things, instructed to provide an assessment of existing, emerging, and potential threats. Since 2004, none of the reports that have been published makes explicit reference to offensive use of cyber capabilities.[34] Instead, UN member countries simply acknowledge that "a number of States are developing capabilities for military purposes"[35] and observe activities by "persistent threat actors, including states" as well as the use by states of "ICT-enabled covert information campaigns."[36]

These rather unspecified acknowledgments reflect observations that cyber operations tend to be mostly conducted in "the grey zone," which characterizes many of today's conflicts, tensions and strategic competition.[37] Within this zone, we see blurred lines between intelligence and offensive cyber operations; between cyber and information operations; in the use of proxies for cyber operations; and the absence of a distinction between operations of a criminal or inter-state (political-military, offensive) nature.

The UN norms, however, do refer to certain cyber capabilities that states possess and use that are potentially of an offensive nature. These terms are laid out in Table 1.

Table 1: Terms related to offensive cyber included in the UN norms lexicon.

Norm	Terminology
#1	ICTs, ICT networks, and ICT practices that are harmful or that may pose threats to the maintenance of international peace and security
#2	Malicious ICT incidents
#3	Internationally wrongful act
#6	ICT activity contrary to obligations under international law
#6	ICT activities conducted or supported by a state that may impact the critical infrastructure of or the delivery of essential public services in another state
#8	Malicious ICT acts
#9	Malicious ICT tools and techniques
#9	Use of harmful hidden functions, including backdoors
#10	The exploitation of vulnerabilities that compromise the confidentiality, integrity, and availability of systems and networks
#11	Malicious international activities

The used terminology suggests that the international community intends to distinguish between the malicious and benevolent use of cyber capabilities. This may imply that offensive cyber operations are acknowledged in situations where acts, tools, techniques, and activities are or are becoming “malicious.” This leads to questions about what is considered “malicious” and who makes that determination.

The potential consequences of offensive use of cyber capabilities seem to be recognized with the adjective clauses “acknowledged to be harmful” and “pose a threat to international peace and security.” Finally, the terms note the use of hidden functions in software and/or the exploitation of known or yet unknown vulnerabilities. These are tools, tactics, and techniques—or enablers—that commonly form a part of offensive cyber operations. Clearly, the UN norms do not dismiss the existence of a state’s offensive cyber repertoire although precise definitions and intended meanings are absent.

What Guidance Can be Deduced from the UN Norms on Offensive Cyber?

A next step is to look closely at the text of each of the individual norms and establish how they address the pertinent issues such as the development of offensive cyber capabilities, command and control over cyber tools in possession; use of cyber capabilities; and response measures after becoming a victim of the development, control, and/or use of capabilities by other states. This is greatly aided by the “additional layer of understanding”[38] that is offered in the GGE 2021 report.

An initial observation in considering the eleven norms is the balance between responsibilities of the victim of a cyber operation and those of the author. This is most evident in the combination of norms 6 and 7. While norm 6 prohibits the targeting of critical infrastructure in another state, norm 7 imposes a responsibility to make sure one’s own critical infrastructure is sufficiently cyber secure. This should create an environment where (innocent and civilian) systems are not inadvertently affected while offering offensive cyber operators the opportunity to be distinct and proportional in their actions.

That same mutuality can be found when considering the norms on offensive cyber. There are responsibilities for states that possess and use cyber capabilities as well as for states who believe they have been attacked by other states’ offensive cyber activities. The different pieces of guidance that can be found in the set of eleven norms are presented in Tables 2 and 3 respectively, with a distinction between encouraging and constraining actions.

The do’s and don'ts outlined in Table 2 show that the current UN norms assign a range of responsibilities to any state involved in offensive cyber.

For instance, the UN norms constrain the use of offensive cyber by requiring operations to be targeted and to exclude effects on other states’ critical infrastructure and CERTs, including through second- and third-order effects. The norms also require that tools and techniques need to be used in such a way that they do not proliferate any further, and vulnerabilities

Table 2: Guidance from the UN norms on responsibilities to states involved in offensive cyber.

Individual States should apply the following actions:

- Take reasonable steps within their capacity to end the ongoing activity in its territory.[39] (to prevent a potential internationally wrongful act[40]).
- Respect and protect human rights and fundamental freedoms, in particular the freedom of expression which includes the freedom to seek, receive, and impart information regardless of borders and through any media.[41]
- Put in place relevant policy and legislative measures at the national level to ensure that state-sponsored ICT activities that may impact the critical infrastructure or delivery of essential public services in another state conducted in accordance with international law and subject to comprehensive review and oversight.[42]
- Prevent the proliferation of malicious ICT tools and techniques.[43]
- Introduce measures that prohibit the introduction of harmful hidden functions and the exploitation of vulnerabilities in ICT products that may compromise the confidentiality, integrity, and availability of systems and networks.[44]
- Put in place legal frameworks, policies, and programs to guide decision-making on the handling of ICT vulnerabilities and curb their commercial distribution.[45]
- Distinguish their national CERT(s) from other arms of government.[46]

Individual States should refrain from the following actions:

- Carry out activities that threaten international peace and security or are harmful.[47]
- Practice arbitrary or unlawful mass surveillance.[48]
- Intentionally damage critical infrastructure or otherwise impair the use and operation of critical infrastructure to provide services to the public, including cascading domestic, regional, and global effects.[49]
- Conduct or knowingly support activity to harm the IT systems of CERT in recognition of their unique responsibilities and functions in managing and resolving ICT incidents.[50]
- Use their national CERT(s) to engage in international malicious activity.[51]

should not be used in a way that additionally compromise the confidentiality, integrity, and availability of ICT products. Also, the state authoring the operation should be able to end the activity once it appears to be threatening international peace and security and/or amounts to an internationally wrongful act.

The UN norms further state that the possession of offensive cyber capabilities comes with the responsibility to follow adequate policy and legislative measures to ensure that no operation will breach obligations under international law and to guarantee a form of review and oversight. They also set out the responsibility to not engage a state's national CERT in offensive cyber operations and to ensure a separation of staff, tools, and command and control.

The development of offensive cyber capabilities or attempts to acquire or procure access to third-party capabilities do not seem to be guided by the UN norms. In other words, states are currently free to pursue these assets.

The norms also extend duties to states that believe they have been attacked by an offensive cyber operation. They need to contact, consult, and inform the other states concerned, including the presumed author. They also have to make sure they have done their own due diligence regarding cybersecurity measures and incident response mechanisms. Finally, the norms indicate an affected state should "take a deep breath" and respond proportionally and in an informed manner.

Table 3: Guidance from the UN norms on responsibilities to states who fall victim to another state's offensive cyber.

States should:

- Consult among relevant competent authorities between the states concerned.[52]
- Consider all relevant aspects in their assessment of the incident. This can include the incident's technical attributes; its scope, scale, and impact; and the wider context, including the incident's bearing on international peace and security.[53]
- Take all appropriate and reasonably feasible steps to detect, investigate, and address the situation.[54]
- Notify the state from which the activity is emanating.[55]
- Take appropriate measures to protect its critical infrastructure and designate infrastructure and sectors it deems critical.[56]
- Classify ICT incidents in terms of their scale and seriousness.[57]
- Authorize national CERT(s) and put in place a national ICT-security incident management framework.[58]
- Respect and protect human rights and fundamental freedoms, in particular the freedom of expression which includes the freedom to seek, receive and impart information regardless of frontiers and through any media.[59]

States should not:

- Monitor all ICT activities within their territory.[60]

How each state fulfils these responsibilities is a matter of national policy and sovereign decision-making. It will differ among states based on factors such as political-military culture, national cyber and security context, and institutional arrangements of government. The UK and Australia, for instance, will have special duties to reassure friends and foes of their responsible conduct of operations given the integration of the national CERT and National Cyber Security Centre into, respectively, Government Communications Headquarters (GCHQ) and the Australian Signals Directorate (ASD). In Australia, ASD has the national mandate for developing tools, techniques, and procedures of offensive cyber that they then "offer" to Defense or a respective military command.[61] In the UK, together with the Ministry of Defence, Secret Intelligence Service, and Defence Science and Technology Laboratory, GCHQ coordinates the National Cyber Force, which is the only recognized body to conduct offensive cyber operations.[62]

Different Types of Offensive Cyber Operations in the Context of International Security

The UN cyber norms are a relevant mechanism to assess offensive cyber. They provide distinct guidance to states on their use of and any responses to the use of offensive cyber by others. The next thing to consider is the context in which offensive cyber capabilities are deployed, in particular situations that may constitute a threat to the maintenance of international peace and security.

Different perspectives address the strategic value of offensive cyber operations. Based on anecdotal evidence that is surfacing from past cyber operations, it appears that the cyber domain is a treasure trove for intelligence-collection activities such as intercepting communications and data, stealing high-value intellectual property, and pre-positioning for any potential future acts.

While debates continue as to whether cyber espionage meets the criteria of offensive cyber, in most cases state capabilities and agencies mandated with foreign (cyber) espionage are the same as, or closely connected to, those for offensive (military) cyber operations. In diplomatic practice, however, the use of cyber tools for intelligence purposes does not appear controversial or discouraged.[63] Intelligence operations have only become problematic in situations in which they were discovered, exceeded a distinct political-military (information) purpose, for instance, in the case of cyber-enabled theft of intellectual property or created unintended physical effects.

Another use case is cyber operations that are part of a wider campaign of authorized military operations; they are one of the many "weapons"[64] that can be deployed both in the intelligence preparation of the battlefield[65] and for tactical operations. A well-known example of the latter is the cyber operation by the US, UK, and Australia against the Islamic State's propaganda network in 2016.[66] Also, recent Russian cyber operations as part of the military campaign against Ukraine, and earlier, in 2008 against Georgia, fit this category.

In the similar military context, there are several examples of standalone offensive cyber operations. The Olympic Games/Stuxnet operation attributed to the US and Israel against Iran's nuclear capabilities is an example that fits this label as does the use of offensive cyber capabilities to combat cybercrime and prevent terrorist use of the internet. The Australian government, for example, has declared a willingness to deploy their offensive capabilities to pursue overseas cyber criminals,[67] and the US conducted operations "to impose costs" on Russian-based ransomware groups.[68]

The last category of offensive cyber operations to carefully consider in the context of international peace and security is the use of cyber capabilities by security and intelligence agencies under domestic law and for national (public) security purposes.[69] In efforts to stem discontent, surveil political opposition, demoralize insurgency groups and control the flow of information and data in and out of the country, security agencies have imposed crude tactics that wouldn't be out of place in an inter-state conflict. Furthermore, states will be challenged in any claims of sole domestic effects of the use of cyber capabilities given the character of the networks and almost inevitable cascading effects outside their sovereign borders.

In these four situations, states make use of their offensive cyber capabilities in the pursuit of what can be legitimate national interests. In doing so, however, they may exceed the boundaries of responsible behaviour and create a threat to international stability. This then leads to the final question of how the UN norms can be applied. This requires a more detailed understanding of what tools, techniques, activities, and impact are out of bounds, and through which means and mechanisms offensive cyber acts can be verified.

Applying the UN Norms in Maintaining International Peace and Security

In conventional warfighting and peacekeeping, international legal concepts, thresholds of peace and conflict, and rules of engagement are relatively clear and established. The UN Security Council typically acts as the premier body to discuss issues related to the maintenance of international peace and security, including investigations into international disputes, recommendations to resolve tensions, and the determination of the existence of a threat or acts of aggression. The Council can also decide to impose sanctions or authorize military responses.[70]

Through these functions, the Council has been applying rules of international law alongside a wide variety of norms of responsible state behavior, such as committing to the responsibility of humanitarian intervention and mandates around the protection of civilians. The UN General Assembly, where all international cybersecurity debates have so far taken place, can only make non-binding recommendations and, in practice, the nature of the General Assembly's First Committee deliberations have been largely conceptual and legalistic rather than issue- or incident-specific.

During its non-permanent term on the UNSC in 2020-21, Estonia has been fronting a series of so-called Arria formula meetings.[71] These are informal sessions intended to engage stakeholders outside of the UN system or to raise issues that have not yet found their way to the formal agenda of the Security Council. These are valuable steppingstones to arrive at a future situation where an international body such as the Security Council will express an opinion about an act of offensive cyber in terms of its legality and legitimacy. For now, Russia, China, and their allies do not see a role for the UN Security Council on international cyber matters.[72] This aligns with their effort to prevent the acknowledgment of "the militarisation of cyberspace."

For the purpose of arms control, disarmament, and conflict prevention, the UN and various regional organizations have mechanisms in place for states to report on their military capabilities, doctrines, and decision-making, which are monitored by international secretariats, civil society organizations, and academia.[73] Similar activities have started to emerge for cyber capabilities that may jeopardize international peace and security including offensive cyber operations. Examples include the cyber operations[74] and significant cyber incident[75] trackers, cyber power, and capability indices,[76] and assessments of nations' international cyber strategies.[77] Yet, these have not yet reached a level of maturity to consequently affect national decision-making and offer a robust form of international accountability.[78]

The non-tangible and yet-too-difficult-to-verify character of cyber operations is a significant hindering factor in this accountability effort. Also, the dominant roles of intelligence agencies and the use of proxy actors add to the level of secrecy surrounding state cyber capabilities. Nonetheless, a gradually growing body of public government documentation is emerging that allows assessments to be made. These include cybersecurity strategies, operational concepts for cyber commands, and military cyber-related Standard Operation Procedures (cyber-SOPs). Confidence-building measures promoted by the UN, as well as several regional organizations, are promoting the sharing of official, but unclassified documents like these.

There is a pivotal role for Track Two actors such as academia, think tanks and civil society organizations to keep pushing states at the national and operational level to exercise greater transparency and to expose and report on real-life incidents, compare these with public documents, and offer informed assessments of the responsible and irresponsible nature of specific offensive cyber activities.

CONCLUSION

The UN norms of responsible state behaviour in cyberspace do not discourage, let alone stop, states from developing or procuring cyber capabilities. In fact, it is most likely that more states will pursue national cyber capabilities for either domestic security purposes or in light of geo-economic competition.

However, this does not necessarily lead to an offensive future. Ever since international ICT security was put on the UN agenda as a topic in 1998, the world's major cyber powers, including the US, Russia, and China, have shown an interest in developing and committing to certain basic minimum rules.

The UN norms provide relevant guidance to states in terms of their responsible possession and use of offensive cyber capabilities. While they are anything but complete and unambiguous, collectively the current set of 11 norms provides a distinct direction. It shows what activities, effects, and practices the international community does not want to see occurring.

While norms are occasionally violated, the general applicability of the 11 UN norms is not disputed. Further work is required to marry UN language around "maliciousness" with offensive cyber, develop operational guidance, and find mechanisms to assess states' on-going observance.

Responsible forms of offensive cyber will not be recognized by or achievable for everyone and most likely remain the business of a limited group of states that show a political interest in projecting power in cyberspace, have a digital and tech-enabled economy and can employ operators with sophisticated technical skillsets. More fundamentally, these frontrunners will benefit from setting the bar of responsible state behavior high as their own capabilities grow and professionalize.

An elevated bar for states to responsibly possess and use offensive cyber capabilities should create an environment where states can use these tools and assets for legitimate national interests but without jeopardizing international peace and security, and societal trust and confidence in ICTs and the digital domain.

APPENDIX

The full text of the UN norms of responsible state behavior in cyberspace, as contained in UN General Assembly Resolution 70/237 (2015).

(a) Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security;

(b) In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences;

(c) States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;

(d) States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect;

(e) States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression;

(f) A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public;

(g) States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions;

(h) States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty;

(i) States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions;

(j) States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure;

(k) States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.

NOTES

1. Statement made plus author's conversation with Microsoft's global diplomacy team.
2. Microsoft, Protecting people in cyberspace: The Vital Role of the United Nations in 2020, 2, https://www.un.org/disarmament/wp-content/uploads/2019/12/protecting-people-in-cyberspace-december-2019.pdf.
3. UN General Assembly, Resolution 73/27, operative clause 5, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/418/04/PDF/N1841804.pdf?OpenElement.
4. Australian Strategic Policy Institute, The UN norms of responsible state behaviour in cyberspace, explainer video,https://ad-aspi.s3-ap-southeast-2.amazonaws.com/2020-09/cybernorms_ENGLISH.mp4.
5. UNOEWG (2021), Summary report of the informal intersessional consultative meeting, December 2-4, 2019, https://front.un-arm.org/wp-content/uploads/2020/01/200128-OEWG-Chairs-letter-on-the-summary-report-of-the-informal-intersessional-consultative-meeting-from-2-4-December-2019.pdf.
6. See for example: Jim Lewis, Toward a More Coercive Cyber Strategy: Remarks to U.S. Cyber Command Legal Conference, March 4, 2021 https://www.csis.org/analysis/toward-more-coercive-cyber-strategy; Ciaran Martin, Cyber 'Deterrence': A Brexit Analogy, January 15, 2021, https://www.lawfareblog.com/cyber-deterrence-brexit-analogy; Global Commission on the Stability of Cyberspace, Advancing Cyberstability; Final report, November 2019, https://www.whitehouse. gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/, see chapter 2 for a definition of cyberstability as intended here.
7. Government of the United States, The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China, July 19, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/.
8. Ibid.
9. Government of New Zealand, New Zealand condemns malicious cyber activity by Chinese state-sponsored actors, July 19, 2021, https://www.beehive.govt.nz/release/new-zealand-condemns-malicious-cyber-activity-chinese-state-sponsored-actors.
10. US ("The PRC's pattern of irresponsible behavior in cyberspace is inconsistent with its stated objective of being seen as a responsible leader in the world" https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/); UK ("The UK is calling on China to reaffirm the commitment made to the UK in 2015 and as part of the G20 not to conduct or support cyber-enabled theft of intellectual property of trade secrets" link); Australia ("Australia calls on all countries – including China – to act responsibly in cyberspace. China must adhere to the commitments it has made in the G20 and, bilaterally, to refrain from cyber-enabled theft of intellectual property, trade secrets and confidential business information with the intent of obtaining competitive advantage," https://www.foreignminister.gov.au/minister/marise-payne/media-release/australia-joins-international-partners-attribution-malicious-cyber-activity-china); EU ("We continue to urge the Chinese authorities to adhere to these norms and not allow its territory to be used for malicious cyber activities, and take all appropriate measures and reasonably available and feasible steps to detect, investigate and address the situation," https://www.consilium.europa.eu/en/press/press-releases/2021/07/19/declaration-by-the-high-representative-on-behalf-of-the-eu-urging-china-to-take-action-against-malicious-cyber-activities-undertaken-from-its-territory/; NATO ("we call on all States, including China, to uphold their international commitments and obligations and to act responsibly in the international system, including in cyberspace," NATO - News: Statement by the North Atlantic Council in solidarity with those affected by recent malicious cyber activities including the Microsoft Exchange Server compromise, 19-Jul.-2021).
11. UN General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2015), A/70/174, paragraph 13(b), https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf?OpenElement.
12. UN General Assembly, Group of Governmental Experts on advancing responsible state behaviour in cyberspace in the context of international security (2021), paragraph 30(d).
13. Tom Uren, Bart Hogeveen, and Ferus Hanson, Defining offensive cyber capabilities, ASPI. Memo for the Global Commission for the Stability in Cyberspace, July 2018, https://www.aspi.org.au/report/defining-offensive-cyber-capabilities.

NOTES

14. For Russia, see for instance, Janne Hakala and Jazlyn Melnychuk, Russia's strategy in cyberspace. NATO Strategic Communications Centre of Excellence, June 2021, https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_15-06-2021. pdf; for China, see for instance: The Guardian, Experts say China's low-level cyberwar is becoming severe threat, September 23, 2021, https://www.theguardian.com/world/2021/sep/23/experts-china-low-level-cyber-war-severe-threat; for Iran, see for instance, US Congressional Research Service, Iranian offensive cyber-attack capabilities, January 2020, https://sgp. fas. org/crs/mideast/IF11406.pdf.
15. For instance, see, Josh Gold, A cyberspace FIFA to set rules of the game? UN states disagree at second meeting. CfR Net Politics, March 2, 2020, https://www.cfr.org/blog/cyberspace-fifa-set-rules-game-un-states-disagree-second-meeting.
16. ASPI-ICRC workshop with Australian government representatives, September 2021, Report forthcoming.
17. Statement by the delegation of the Republic of Indonesia on behalf of the Non-Aligned Movement, First Substantive Session of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security, September 9, 2019, PERMANENT MISSION OF THE REPUBLIC OF INDONESIA, TO THE UNITED NATIONS, NEW YORK (kemlu.go.id).
18. Bart Hogeveen, *The UN norms of responsible state behaviour in cyberspace. Guidance on implementation for member states of ASEAN*, Australian Strategic Policy Institute, March 2022, https://www.aspi.org.au/report/un-norms-responsible-state-behaviour-cyberspace.
19. Elaine Korzak, UN GGE on Cybersecurity: The end of an era? *The Diplomat*, July 31, 2017, https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/.
20. Bart Hogeveen, Six years in the making: UN reaches global cyberspace consensus, *ASPI Strategist*, March 26, 2021, https://www.aspistrategist.org.au/six-years-in-the-making-un-reaches-global-cyberspace-consensus/.
21. Josh Gold, Unexpectedly all UN countries agreed on a cybersecurity report. So what? *Council for Foreign Relations,* March 18, 2021, https://www.cfr.org/blog/unexpectedly-all-un-countries-agreed-cybersecurity-report-so-what.
22. Hogeveen, Six years in the making: UN reaches global cyberspace consensus.
23. UN General Assembly Resolution 75/240, January 4, 2021, operative clause 1, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/000/25/PDF/N2100025.pdf?OpenElement.
24. Uren, Hogeveen, and Hanson, Defining offensive cyber capabilities.
25. UN General Assembly, Resolution 70/237.
26. Bart Hogeveen, The UN norms of responsible state behaviour in cyberspace. Guidance on implementation for member states of ASEAN, Australian Strategic Policy Institute, forthcoming.
27. During the 1999 NATO intervention in Kosovo, NATO networks were targeted through a Denial-of-Service attack (Christine Hegenbart, Semantics matter. NATO, cyberspace and future threats, NATO research paper, July 2014, https://www.ndc.nato.int/news/news.php?icode=701#) and the US military reportedly considered hacking into Serbia's central bank and degrading Serbia's financial systems (Julian Border, Pentagon kept the lid on cyberwar in Kosovo, *The Guardian,* November 9, 1999, https://www.theguardian.com/world/1999/nov/09/balkans); During the second Chechen war, the Russian military sought to disrupt websites and information databases of its opponents (Kenneth Geers, Cyberspace and the changing nature of warfare, NATO CCDCOE, keynote speech, https://csl.armywarcollege.edu/SLET/mccd/CyberSpace-Pubs/Cyberspace%20and%20the%20Changing%20Nature%20of%20Warfare.pdf; and Timothy L. Thomas, Information warfare in the second (1999-present) Chechen war: Motivator for military reform? 2003, https://community.apan. org/cfs-file/__key/docpreview-s/00-00-08-52-36/2002_2D00_01_2D00_01-Information-Warfare-in-the-Second- _2800_1999_2D00_Present_2900_-Chechen-War-_2800_Thomas_2900_.pdf.
28. Allegedly, the US government's NSA and CIA together with Israeli intelligence services developed the Stuxnet virus to degrade the industrial control systems of Iran's nuclear facility in Natanz (Mariusz Antoni Kaminski, Operation Olympic Games. Cyber-sabotage as a tool of American intelligence aimed at counteracting the development of Iran's nuclear programme, in: Security and Defence Quarterly, 2020:29(2): 63-71, https://securityanddefence.pl/Operation-Olympic-Games-nCyber-sabotage-as-a-tool-of-American-nintelligence-aimed,121974,0,2.html.
29. This refers to leaked documents by former NSA contractor Edward Snowden on the US NSA's surveillance activities. They disclosed the tools and techniques that were being used targeted systems, internet providers, and other platforms and encryption keys they had managed to break; *Lawfare*, Snowden revelations, https://www.lawfareblog.com/ snowden-revelations.

NOTES

30. UNGGE (2021), paragraph 71 (f).
31. UNOEWG (2021), Summary report of the informal intersessional consultative meeting, December 2-4, 2019, LetterF702. dot XP (un-arm.org)
32. Bart Hogeveen, “Which practices help us maintain a secure cyberspace in the Asia Pacific?” APNIC blog, November 26, 2020, https://blog.apnic.net/2020/11/26/which-practices-help-maintain-secure-cyberspace-asia-pacific/.
33. GGE report, para 18.
34. A scan of the 2021 reports (which includes relevant passages of previously agreed text) do not show terms that explicitly relate to “offensive” and “offensive cyber operations” or “capabilities.”
35. UNGGE (2021) and UNOEWG (2021).
36. UNGGE (2021) and UNOEWG (2021).
37. Lesley Seebeck, Grey zone strike means cyber war, in *Australian Financial Review*, June 24, 2020, https://www.afr.com/policy/foreign-affairs/grey-zone-strike-means-cyber-war-20200623-p5556b.
38. UNGGE (2021), paragraph 18.
39. UNGGE (2021), paragraph 30(a)
40. An Internationally Wrongful Act is an act that is (a) attributable to a state, and (b) a breach of a rule of international law. See: Francois Delerue, Cyber operations and international law, 2020, chapter 5: Internationally wrongful acts: cyber operations breaching norms of international law.
41. UNGGE (2021), paragraph 13(e).
42. UNGGE (2021), paragraph 46.
43. UNGGE (2021), norm 13(i), paragraph 56.
44. UNGGE (2021), paragraph 58(c).
45. UNGGE (2021), paragraph 62.
46. UNGGE (2021), paragraph 68.
47. UNGGE (2021), paragraph 20.
48. UNGGE (2021), paragraph 37.
49. UNGGE (2021), paragraph 42.
50. UNGGE (2021), paragraph 65.
51. UNGGE (2021), paragraph 67.
52. UNGGE (2021), paragraphs 23 and 24.
53. UNGGE (2021), paragraph 24.
54. UNGGE (2021), paragraph 29.
55. UNGGE (2021), paragraph 30(c).
56. UNGGE (2021), paragraph 48.
57. UNGGE (2021), paragraph 50.
58. UNGGE (2021), paragraph 68.
59. UNGGE (2021), norm 13(e).
60. UNGGE (2021), paragraph 30(a).
61. Australian Signals Directorate, Annual Report 2019-20, chapter 3: offensive cyber operations – performance analysis, Offensive cyber operations - performance analysis | Transparency Portal.
62. UK government, National Cyber Force explainer, December 2021, Microsoft Word - Force Explainer 20211213 FINAL. docx (publishing.service.gov.uk).
63. For instance, see: Russell Buchan and Inaki Navarrete, Cyber espionage. Oxford bibliographies, Cyber Espionage - International Law - Oxford Bibliographies; Ilina Georgieva, The unexpected norm-setters: Intelligence agencies in cyberspace, in Contemporary Security Policy, vol. 41, 2020, issue 1, https://www.tandfonline.com/doi/full/10.1080/13523260.2019.1677389.

NOTES

64. For an overview of offensive cyber capabilities that nation states might deploy, see: Ciaran Martin, Cyber-weapons are called viruses for a reason: Statecraft and security in the digital age. Inaugural lecture, King's College London, November 2020, https://s26304.pcdn.co/wp-content/uploads/Cyber-weapons-are-called-viruses-for-a-reason-v2-1.pdf.
65. See, for instance, U.S. Army, Army Technical Publication 2-01.3, *Intelligence Preparation of the Battlefield*, March 1, 2019, appendix D: IPB Cyberspace Considerations, https://home.army.mil/wood/application/files/8915/5751/8365/ATP_2-01.3_Intelligence_Preparation_of_the_Battlefield.pdf.
66. Stephanie Borys, Australian cyber soldiers hacked Islamic state and crippled its propaganda unit – here's what we know, ABC News, December 18, 2019, https://www.abc.net.au/news/2019-12-18/inside-the-secret-hack-on-islamic-state-propaganda-network/11809426.
67. Australian Minister of Defence, Australia continues to combat foreign cybercriminals, media release, December 2, 2020, https://www.minister.defence.gov.au/minister/lreynolds/media-releases/australia-continues-combat-foreign-cybercriminals.
68. Julian E. Barnes, US military has acted against ransomware groups, General acknowledges, *The New York Times*, December 5, 2021, https://www.nytimes.com/2021/12/05/us/politics/us-military-ransomware-cyber-command.html.
69. For instance, see Dien Nguyen An Luong, How the Vietnamese state uses cyber troops to shape online discourse, in ISEAS Perspective 2021/22, March 3, 2021, https://www.iseas.edu.sg/articles-commentaries/iseas-perspective/2021-22-how-the-vietnamese-state-uses-cyber-troops-to-shape-online-discourse-by-dien-nguyen-an-luong/.
70. UN Security Council, Functions and Powers, Functions and Powers | United Nations Security Council.
71. ERR, UN Security Council reaffirms important of cyberstability, May 23, 2020, https://news.err.ee/1093658/un-security-council-reaffirms-importance-of-cyberstability.
72. What's in blue: Arria-formula meeting on "preventing civilian impact of malicious cyber activities," Security Council report, December 19, 2021,UN Security Council reaffirms importance of cyberstability | News | ERR.
73. For example, one can look at the work of SIPRI (SIPRI yearbook) and Crisis Group.
74. Council on Foreign Relations, Cyber operations tracker, https://www.cfr.org/cyber-operations/.
75. Centre for Strategic and International Studies, Significant cyber incidents, Significant Cyber Incidents | Center for Strategic and International Studies (csis.org).
76. For instance, see Belfer Center, National Cyber Power Index 2020, https://www.belfercenter.org/publication/national-cyber-power-index-2020; IISS, Cyber capabilities and national power, June 28, 2021, https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power.
77. For instance, see the Cyber Diplomacy research papers on China, Russia, India, Latin America, and Southeast Asia from the EU Cyber Direct (Cyber Diplomacy) project, https://eucyberdirect.eu/research?category=research-papers.
78. ASPI and ICRC, Report on workshop, forthcoming.

Why the United States Must Win the Artificial Intelligence (AI) Race

Alfred D. Hull
Dr. Jim Kyung-Soo Liew
Kristian T. Palaoro
Dr. Mark Grzegorzewski
Dr. Michael Klipstein
Dr. Pablo Breuer
Dr. Michael Spencer

The AI Race Winner Will Control AI Impacts on Society

An increasingly urgent debate rages in many circles about the "Artificial Intelligence (AI) Arms Race" rapidly progressing on a global scale. Among many unanswered questions, one is of particular interest to the United States (US) government: Where does the US stand in this race relative to China? This question is critical because the AI Arms Race "winner" will dominate how AI impacts myriad aspects of human society worldwide. For the US to lead the AI race, it will require a conscious partnership among public, private, and academic sectors, and a strategic alignment with our allies. Our relative position as a world leader, our relative position as an economic leader, and our standing as a moral force for all people's good and ethical treatment are at risk.

The sheer breadth that AI poses, both to improve and degrade human life, deeply troubles many. A common naysayer vision of AI in the future poses a bleak dystopian picture dominated by terminators and bad actors. The high-profile Elon Musk has cast our rapid pursuit of developing AI technology as **summoning the demon**.[1] Others on the other side of this debate think AI is going to open a new global chapter in which we try to understand ourselves better than the outside world.[2] Which prophetic vision of AI is most accurate is unknown, but what is clear is that AI technology continues to progress. Recently, Google announced that its AI model has over one and a half trillion parameters, ousting the previously most advanced AI, which was Open AI's 175 billion parameterized GPT-3 model.[3] The AI industry dazzles with its breakthroughs, which are being driven more and more by national governments and private companies due to AI's potential for paradigm advances in national security and corporate efficacy.

Russian President Vladimir Putin dramatically but correctly stated that whichever nation wins the AI race will rule the world. The stakes have never been higher. Imagine a world where China wins the AI Arms Race and US citizens become as marginalized as the Uighur Muslims now are, forcefully held in re-education camps under extreme AI digital surveillance. Are we ready to have a "social credit" system[4] instilled for the next generation of Americans, where they will have their digital data crumbs captured from birth and fed into a national AI engine to predict the probability of dissidence? To Elon Musk's point of view of AI as a source of untold and unimaginable power for the countries that harness it, the US winning the AI race is inescapable.

As much of US AI competition resides in China and received their AI basic training in North America, we unwittingly have, in fact, armed our AI adversary. Even though the US may still hold the advantage as the launching pad for the next generation of AI scientist-soldiers, and we are able to stem the brain-drain, the question remains: is that alone enough for us to prevail?

The National Security Commission on AI (NSCAI) lists steps[5] the US should take to overcome the challenge. It also observes that the AI revolution is not a strategic surprise and that time is running out. China has, for years, been investing heavily through Venture Capitalists, Angels, and Accelerators across Silicon Valley and the Bay area. In addition to poaching talent from America's AI armories, we must work together with Venture Capitalists in China, like Kai-Fu Lee,[6] a Taiwanese-born American computer scientist who obtained his Ph.D. from Carnegie Mellon and previously worked at Apple, Microsoft, and Google. Kai-Fu now runs Sinovation Ventures with over $2 billion in assets under management, investing aggressively in the China-based AI unicorn companies. China's continued heavy investments in AI all aims to make China the world's dominant AI player by 2030. This resolve is formally etched into the Chinese Communist Party's (CCP's) proposal—approved at the Fifth Plenum of the 19th CCP Central Committee in late October 2020.[7]

And what is the US response to this marker? How can we effectively strengthen our trifecta partnerships across domestic technology companies, academic institutions, and military agencies? Large federal agencies can help spur on a tremendous amount of economic activity, but we must coordinate ourselves properly. How do we enact AI-trifecta policies to unleash a flood of federal AI investments and thus catalyze economic development within the US? How do we convince professors to work much more collaboratively with leaders from both industry and defense agency leaders? How can we better weave AI postdoctoral researchers and Ph.D. students into the fabric of our entrepreneurial culture and reinvigorate the American dream? How do we balance AI academic freedom to publish and share breakthroughs without unduly compromising intellectual property?

Finally, how can we provide ramps for any American to embark on the AI knowledge journey? Some have proposed ways to make AI training widely accessible by all in the federal government (see ACT-IAC's AI *Federal Workforce Certification*).[8] Finding, training, and keeping the next generation of AI work- force talent within the US will help build our AI workforce, thereby protecting our national AI competitive advantage. With this backdrop in mind, the solution to how the US can win the AI race becomes clearer. Allies are critical to winning the AI race. From a pure numbers game, which country can match China's over one billion people and speak English? The answer is, not surprisingly, India. Additionally, imagine if the US included our European allies and Mexico? Strategic AI relationships built to have our partners overseas and nearshore will mark a significant step in augmenting the US in the AI Race.

The US should aggressively foster strategic AI relationships with its allies: India, Mexico, Canada, Ghana, and the Europe Union, to co-develop AI training, tools, and solutions, and to co-host AI summits. Needless to say, no one will call a timeout while the US figures out what it wants to do, least of all China, which enjoys the strength, talent, and aspiration to challenge US technological leadership, military establishments, and global position, as evidenced by China's citizen surveillance and social credit scoring systems.[9] Thus one key to victory in the AI race is recognizing the benefits of establishing and nurturing alliances among state actors, industry, academia, and free societies. The ingredients for success currently exist, but they remain in urgent need of being further strengthened and coordinated. The AI race will not be won unless the US acts swiftly to cultivate and resource these synergies. The time *to strike first, strike hard, with no AI mercy*, is now. To do that, we must first understand the spectrum of technologies and discipline that fall under the AI umbrella.

AI Goal – Computers that Mimic Human Intelligence

The AI ecosystem of fields facilitates several tools, such as Generative Adversarial Networks. Some compare AI's field with building artificial animals or persons, or at least something similar.[10] While there is some contention regarding where to draw the outer boundaries around AI is still debated, but most agree that the nucleus of AI is to cause computers to mimic human intelligence. AI researchers since the 1950's have been using the principles that are now known as "Machine Learning" well before they were integrated into the AI ecosystem. After decades of remaining idle, the more recent and exponential growth in the development and use of AI technology today is due to three key factors: (1) cheap computational power (e.g., GPUs) to run Machine Learning, (2) Deep Learning algorithms, and (3) heaps of Big Data, a.k.a. the Data Deluge, to churn through the models for training and validation purposes.

The keys to winning the AI Arms Race will be a sound grasp of the current AI ecosystem and use of AI tools to promote education and address misconceptions. Educational efforts are especially critical to assemble diverse groups of thought and opinions and create a culture of inclusivity. Diversity is essential because, while AI algorithms are superb at finding patterns within high-dimensional vectors of data, and the map f(), AI cannot yet ascribe meaning to these maps. Academically trained humans are needed to be "in the loop" to create, monitor, and be held responsible for clarifying the value and the importance of these AI tools. The following categories will help explain where AI is in its Capability Maturity Model (CMM):

1. **Artificial Narrow Intelligence (ANI):** Machines' ability to accomplish specified tasks
2. **Artificial General Intelligence (AGI):** Machines perform previously undefined general tasks
3. **Artificial Super Intelligence (ASI)/The Singularity:** Machines have AGI capabilities and have achieved self-awareness.

Another reason for the urgent calls to invest in AI education is that the AI Arms Race cannot be won solely by the nation with the most advanced AI technology. NSCAI's publication Technical ***Talent in Government***, reports that "the Department of Defense (DoD) and the Intelligence Community (I.C.) both face an alarming talent deficit.[11] *This problem is the greatest impediment to the U.S. being AI- ready by 2025.*" This AI talent deficit can only be addressed by aggressively recruiting, training, employing, and retaining the most technically savvy and diverse talent. Thus, our competitive advantage largely will be driven by our ability to identify, nurture, train, integrate, collaborate with, cultivate, and sustain the next generation of human capital technical talent. Since we already see AI innovations across all industries, such as healthcare, education, finance, science, smart cities, and space, building an educated populace around this technology will enable us to move effectively to and govern AGI while vigilantly preventing ASI. An ASI reality is the point at which the US could lose control of AI from technology outpacing and outgrowing what benefits humans. Better understanding AI-related disciplines and research obviously includes a rudimentary understanding of the inherent dangers in poorly executed AI. Few other technologies for good can affects more catastrophic than poorly implemented AI.

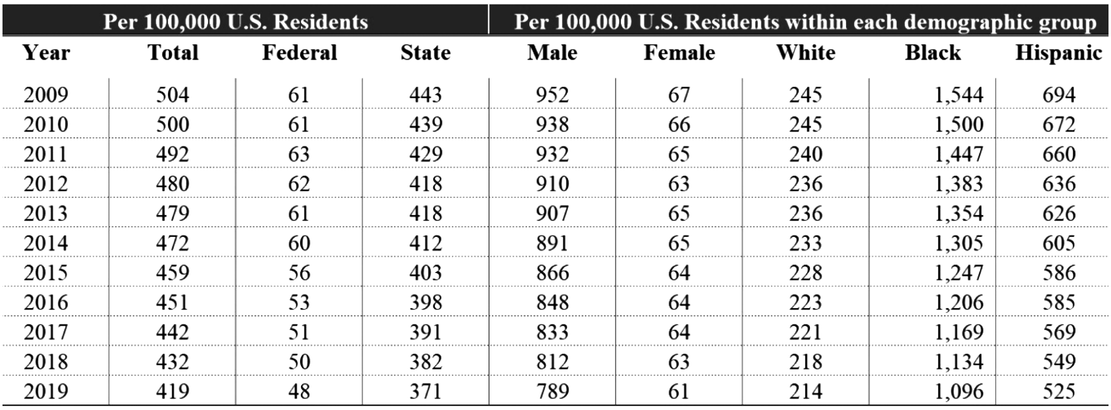
Misguided View That AI Will Explicitly Marginalize People

To better understand AI requires us to examine how it shapes society through the lens of the Internet of Things (IoT). Items like wearable computers, smart refrigerators, digital helpers, and myriad other sensors integrate our personal data into the Internet. Our data is continuously being captured, monitored, and analyzed, and thereby perpetually fuels the next generations of AI and algorithms. This in turn is accelerating the pace of the AI Arms Race, often with little regards for how this process is being adequately vetted to prevent bias and other inaccuracies.

Society's embrace of AI is no surprise, as researchers worked for the last sixty years, driven by the vision of more efficient decision-making machines. With the increase of computational power, the utility, sophistication, and prevalence of AI tools have increased exponentially, but this progress also has a dark side. In 2009, the Nikon Corporation grappled with this issue when its AI-powered digital camera took a picture of an Asian person's face and asked the photographer if the subject had blinked. In 2015, Google suffered a very public outcry when it discovered that its facial recognition AI tool had mislabeled a black person as a gorilla.[12] Although these respective companies have made efforts to address these biases in their AI technology, and other companies have taken these incidents to heart, many problems still exist, especially concerning the data used in AI training.

In 2014, Amazon developed an AI tool to automate the evaluation of job applications and identify optimal candidates. After a year of using this tool, Amazon realized that women were being excluded from hiring results due to the training data. The training data used included technology job applications over the past 10 years, most of which were by men, leading the AI tool to exclude resumes including the word "women." Amazon subsequently abandoned this AI-based application process in 2017.[13] MIT researcher and founder of the Algorithmic Justice League Dr. J. Buolamwini highlighted the dangers of facial recognition AI bias.[14]

Considering the examples provided by Dr. J. Buolamwini of AI's shortcomings in producing accurate or equitable results, we approach law enforcement applications of AI with wariness. Presently, within law enforcement, AI is most used for predictive policing and identification of demographics of likely offenders.[15] The Bureau of Justice compiled incarceration rates by demographic in October 2020; the results were stark, with White incarceration rates shown to be one-third of Hispanics and one-fifth of Blacks.



	Per 100,000 U.S. Residents			Per 100,000 U.S. Residents within each demographic group				
Year	Total	Federal	State	Male	Female	White	Black	Hispanic
2009	504	61	443	952	67	245	1,544	694
2010	500	61	439	938	66	245	1,500	672
2011	492	63	429	932	65	240	1,447	660
2012	480	62	418	910	63	236	1,383	636
2013	479	61	418	907	65	236	1,354	626
2014	472	60	412	891	65	233	1,305	605
2015	459	56	403	866	64	228	1,247	586
2016	451	53	398	848	64	223	1,206	585
2017	442	51	391	833	64	221	1,169	569
2018	432	50	382	812	63	218	1,134	549
2019	419	48	371	789	61	214	1,096	525

Figure. Sentenced prisoners under the jurisdiction of state or federal correctional authorities, by jurisdiction, sex, and race or ethnicity 2009-2019[15]

Suppose these results are used as training data for predictive policing, without context or accounting for variables of extraneous circumstances. In that case, law enforcement will inevitably target minority males, which is, inarguably, unjust. What further diminishes the efficacy of crime prediction models is the law enforcement community's lack of education in understanding its models.[16]

US educational systems must incorporate AI and critical thinking into its curricula, just as cybersecurity has been a recent addition. As an example, in May 2017, the Trump administration, through the Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, tasked the Departments of Commerce and Homeland Security to submit a report on findings and recommendations to educate and train the American cybersecurity workforce, including cybersecurity-related education curricula, training, and apprenticeship programs, from primary through higher education.[17] The Departments' joint response outlined several recommendations for reskilling the existing workforce and aligning education and training to employers' requirements. However, the Departments' educational proposals focused on collegiate level education instead of elementary education. Similar challenges exist for the AI talent pool; more foundational education, ideally in elementary school, must occur to win the upcoming Arms Race in AI development and application. Gamification of critical thinking skills and logic construction facilitate early childhood learning which, in turn, should continue through secondary education. This also will optimize opportunities to cultivate interest in the STEM fields, with reduced anxiety that often accompanies these studies.

Furthermore, leveraging, expanding, and promoting existing programs, such as Scholarship for Service (SFS), will further incentivize pursuit of AI as a career choice.[18] Another cybersecurity lesson learned is the need to retrain the current workforce. The earlier-referenced executive order incentivized existing government employee volunteers to develop new skills by guaranteeing job placement in the cyber workforce, which should grow a strong AI workforce more quickly. With proper implementation and training, AI can and should help reliably execute decisions within design parameters.

However, concern still exists. Presently, the bias of the algorithm creator or environment ultimately encroaches into the AI, knowingly or unknowingly. "Real world" applications of AI involve some people or groups winning while others lose, as happens now with a person making decisions. We see this in the judicial system, workplace adjudication of conflict, and in other locations. However, some tasks should never be assigned to AI, and many believe that researchers should not only ask, "can we?" but also, "should we?" Ethics are a very personal set of beliefs, honed by the individual's education and experience, and other factors such as religious faith, social community, and focus on assigned goals. Leaving ethical decisions to AI will always include a bias and will always result in someone losing.

If this paradigm remains unchecked, then an uneducated, misguided, and ham-fisted application of AI in the US will, at best, result in the unequal distribution of AI's benefits among the populace and, at worst, explicitly marginalize groups of people. Our adversaries welcome the opportunity to capitalize on our society's resultant divisions and sow further division for political purposes. As seen in the 2016 US Presidential election, the selective presentation of information as "facts" distorted views of reality and quickly reinforced individuals' confirmation bias. This example portends future problems if AI remains unharnessed and considered a panacea for problems. However, AI, with its promise comes with threats and problems difficult to predict, exasperated by invalid or incomplete data or inappropriate questions asked of the data.

AI Researchers Must Consider the Ethical Implications of Their Products

According to *Merriam-Webster,* ethics is "the discipline dealing with what is good and bad and with moral duty and obligation."[19] The myriad tools of the AI ecosystem present a vast array of ethics issues, including everything from bias and fairness to safety and job losses, and civil rights abuses. Resolving to comprehensively win the AI race will also require careful consideration of the ethical implications relating to AI technology before, not after implementation. Failure to do that means China very likely will fill the ethical vacuum with its own AI standards and ethical frameworks. Among the questions AI policymakers should ask is how AI implementers can ensure accuracy of its the training data? How does the AI technology account for missing data? What assumptions are baked into the AI model? In other words, how does the creator's own ethical framework influences these assumptions? Taking all of these together, hat is the AI prediction quality?

Autocratic governments are less answerable to these questions than pluralistic, democratic societies must be, and care less about unfavorable outcomes for their people derived from AI solutions. Their priority is societal order, which they attain by suppressing free speech and open discourse. Such nations will not hesitate to use AI data to acculturate their population effectively, even if such data is inaccurate. Both politically and technologically, their aim is not to be broadly representative of the people they govern; it is to homogenize. Thus, technology will be used to enable such political-cultural homogenization.

All societies, which aim to be free and open while striving to provide equal access for all, can potentially benefit from optimally deployed AI. It also is incumbent on democratic societies to heed lessons learned from instances of misapplied AI to avoid disastrous results. One example was a report of police deploying a pre-cog-like AI causing sheriffs to arrive at homes before a predicted crime would occur.[20] Another example entailed AI researchers developing RealTalk, using deep fake technology to replicate a person's voice convincingly. This AI technology will undoubtedly have nefarious applications in the information sphere. The anecdote demonstrates how the private sector excels in answering "Can we?" without first asking "Should we?" As a threshold matter, advancing AI technology should always include a threshold consideration as to (a) how the new technology could be misused, and (b) what, if any, rudimentary guardrails are needed to minimize such misuse.

Put another way, AI innovators must consider the ethical implications of their products. If their product can be used in a harmful manner, should it proceed to market? Users must ask, what type of bias, and historical, measurement does this AI tech rely upon, and are we replicating bias society-wide by using it? As AI technology continues to permeate daily life, understanding how AI technology decisions are made is important. Simply because AI technology recommends a particular action, how can the user guarantee that the AI incorporated guiding principles such as proportionality and does no harm to safety and security?[21] No matter how sophisticated AI technology becomes in regards to statistical (or any other parameter of) accuracy, it can never substitute a user's ethics. This, and trusting technology efficacy, raise questions for leaders in open societies to answer and be held accountable. Wholly apart from the technical experts and duly elected leaders, every American eligible to vote plays a role in responsibly bringing AI to market, implementing safe AI solutions, and understanding how the AI tools we use enhance or detract from the just and equitable type of society we hold sacred.

Elements of DoD are already thinking about these questions and discussing the importance of creating AI tools with ethical considerations addressed on the front end.[22] This may require creators to first consider potential harm, precedent, setting into motion nefarious adversary responses, etc., and setting parameters contemplating when an AI solution may violate specific ethical parameters. The Defense Innovation Board studied and released ethical considerations for DoD AI adoption, including the AI must be responsible, equitable, traceable, reliable, and governable. Given DoD's immense buying power, each of these ethical principles will impact how AI creators build and market their products and how users interact with those products.

Lastly, the US has a unique strength compared to its competitors: we are diverse, respect the enforcement of the rule of law, and value our open, flexible society. An open, transparent society can evaluate evidence, absorb feedback, and make changes critically. It is an open system where information—including ethical judgments—is not closed off. That is not to say that our competitors have no ethical guidelines. In a closed society, the regime does not receive critical feedback and insularly defines its own ethics and accountability. This arrangement for closed regimes works until it cannot absorb any more shocks, eventually collapsing. Incorporating unethical AI into their systems will hasten the fall of these closed regimes. If adequately implemented with ethical considerations for the US open system, it may lead to unforeseen prosperity vis-a-vis our competitors and a healthier political system.

AI's Dual-Use Capabilities Provide Both Positive and Negative Potentials

> "If soldiers are not to cross international boundaries, goods must do so. Unless the shackles can be dropped from trade, bombs will be dropped from the sky."[23]

The AI race is a product of a broader science and technology (S&T) rivalry between the US and China that is quickly developing into a technology war.[24] China's ascendency in global economic power, its rapid technological growth, and the CCP Vision of Victory seeks to position China as the world innovation leader and dominant force in emerging key technologies all combine to threaten US technological superiority.[25] The CCP's restricted, centralized approach gives China an unprecedented advantage to expedite S&T policy creation, allowing state-owned enterprises (SOEs) and commercial sector businesses the unfair advantage of easy access to incentives and funding in opposition to the national security and foreign policy interests of the US. In response to business initiatives taken by China, the US has implemented counterbalancing measures through use of the Department of Commerce's Entity

Lists which targets Chinese digital technology companies.[26] This was done under the auspices of protecting US commercial interests, slowing the pace of China's digital technologies development, and providing the US time to better develop its own S&T initiatives and AI strategies.

According to the US founding principles heavily influenced by the philosophers Sidney[27] and Locke,[28] the US regards the development of AI in accordance with democratic principles: limited representative government, individual freedoms, private property, and authority derived from the electorate. Internationally, the US uses its economic and technological dominance to promote democracy, free markets, and the current international order.[29] China's objectives, in contrast, are primarily to ensure the CCP's regime survival. For the CCP, technological sovereignty is needed to grow a high-tech economy, modernize the PLA, and spread its commercial and geopolitical influence throughout the world. China aims to use AI to suppress individual liberties using surveillance, repressive controls, and predictive analytics. These are not conditions most Western democracies prefer to be subject to or live under.[30]

AI's dual-use capabilities provide both far-reaching positives and negatives. AI's commercial integrative capacity is expected to be an economic boom and the primary catalyst for the upcoming fourth industrial revolution with an additional global economic value more than $13 trillion by 2030.[31] International cooperation in an open-source environment can use AI to solve real-world problems such as food security, clean water, reliable and sustainable energy, affordable health care, and pollution mitigation. Therefore, competition between autocratic and democratic governments and their world views need not result in a zero-sum game.

States invariably take self-serving actions when they believe their survival is at stake, so AI will be integrated almost certainly into military weapons systems, intelligence collection, and other uses deemed essential. The US and partner nations must account for AI's dual-use capabilities representing threats to economic and national security interests. Measures need to be taken following the NSTC AI R&D Strategic Plan and the NSCAI Final Report.[32, 33]

The US can win the AI race. Primary recommendations include dedicating funding for long-term AI investment, developing safe and dependable AI systems, strengthening military-academia-industrial complex collaborations, hardening US cybersecurity, and governing the integration of AI into national security interests. These strategies and recommendations should be the foundation that ensures the US will remain the AI technology leader. We win by taking bold, transparent actions for the collective good, to lift the human condition by providing "responsible, equitable, traceable, reliable, and governable" AI.[34] At the same time we must protect US technological supremacy, intellectual property, technology transfers, and national security.[35] To remain a shining beacon of ethics and humanity, the US must continue to champion humans-in-the-loop and systems free of ignorance and bigotry while preserving and embodying the liberties and values of a free society.

CONCLUSION

If having read this article, you find yourself more curious about and invested in the US winning the AI Arms Race, then there is legitimate hope that this race can be won with our democratic principles intact. The odds of the US establishing itself not only as the leader of the free world, but also as leader of the development and use of AI in pushing human progress forward for citizens the world over, grow as more Americans recognize this to be an all-hands-on-deck situation. To prevail over the competition will require national resolve and all of us going all-in to win this AI race. Doing this will undoubtedly build the necessary momentum to get the US to the next stage of ramping up a national AI strategy, including immediate and significant government investments with more robust partnerships across the spectrum, particularly with academia, private industry, and our allies.

Equally important, our national AI strategy must be girded on the foundation of education and training, which will require dramatic realignment of education to our technology goals, perhaps even using AI learning tools themselves, to include customized instruction for each learner. Moreover, the access to AI education and training must be equitable for everyone to ensure that AI tools going forward minimize biases.

As the US stands at this critical juncture, let it make the bold choices that will allow the nation, decades from now, to look lback proudly. As with all the challenges that the US has faced before and will face in the future, it wins this AI Arms Race by applying America's unique combination of ambition, talent, rigor, diversity, the highest level of ethical standards, transparency, and ingenuity. And when the world notes that the US won this difficult AI race, it also will note that it is the US that continues to protect the inalienable rights of life, liberty, and the pursuit of happiness for all.

BIOS

Mr. Alfred Hull is the HQDA Data Policy & Governance Branch Chief/Senior Data Scientist, and previously led Artificial Intelligence & Machine Learning efforts for the Navy Program Executive Office Manpower, Logistics, and Business Solutions. He earlier led Data Science, Engineering, and Systems Development & Sustainment teams at Naval Information Warfare Command, supporting PMW150: Business Management Systems Portfolio. He spent seven years in fortune 500 companies doing Operations Research and Decision Science work at Amazon.com, Target Corporation, and Dollar Tree Corporate Headquarters. Alfred holds an MBA from George Washington University and two undergraduate degrees in Decision Science and Maritime & Supply Chain Management from Old Dominion University.

Dr. Jim Kyung-Soo Liew is President and Founder of SoKat.com, and Associate Professor of Finance at Johns Hopkins Carey Business School. He has published pioneering research at the intersection of social media and big data, cryptos/blockchain, and financial markets. He currently teaches Big Data and Artificial Intelligence: Extracting Business Value, Crypto-Currencies and Blockchain, and Leading Entrepreneurship and Innovation at the Johns Hopkins Carey Business School. He also serves as ACT-IAC's Co-Chair of the AI Curriculum Committee and Chair of the Data Readiness for AI Committee.

Mr. Kris Palaoro is a NAVWAR systems engineer who works across engineering and logistics, focusing in data engineering and analytics on the ADVANA Jupiter platform. He holds an MBA with a concentration in finance, an MS in International Relations with a concentration in national security affairs, an ME in systems engineering, and four other undergraduate degrees. He is DAWIA level 3 in engineering, level 3 in logistics, level 2 in program management, and is certified as a PMP and CSWF advanced master.

Dr. Mark Grzegorzewski is Resident Senior Fellow in the Department of Strategic Intelligence and Emerging Technology at Joint Special Operations University. His publications include: ″Technology Adoption in Unconventional Warfare", and he authored the chapter: "Why Silicon Valley is a Poorly Suited Model for SOF" in the "Big Data for Generals … and Everyone Else over 40." He also recently published with the Modern War Institute on "Incorporating the Cyberspace Domain: How Russia And China Exploit Asymmetric Advantages in Great Power Competition."

Dr. Michael Klipstein has worked on national cyber topics for over a decade, ranging from USCYBERCOM continuity of government networks, the National Security Agency hard targets, leading a Cyber National Mission Team, and building two Nation Cyber Protection Teams. He taught at Columbia University, created curricula for the Joint Staff for international partner nations in cyberspace, and served as Director of International Cybersecurity Policy for the National Security Council.

Dr. Pablo Breuer is a non-resident senior fellow of the Atlantic Council's GeoTech Center and twenty-two-year veteran of the U.S. Navy with tours including military director of U.S. Special Operations Command Donovan Group and senior military advisor and innovation officer to SOFWERX, the National Security Agency, and U.S. Cyber Command as well as serving as Director of C4 at U.S. Naval Forces Central Command. A DoD Cyber Cup and Defcon Black Badge winner, he has served as faculty at the Naval Postgraduate School, National University, California State University Monterey Bay, and was a Visiting Scientist at Carnegie Mellon CERT/SEI. Pablo is also a co-founder of the Cognitive Security Collaborative and coauthor of the Adversarial Misinformation and Influence Tactics and Techniques (AMITT) framework.

Dr. Michael Spencer is the founder and a Board of Director for the Halcyon Institute, a technology-based research and policy analysis think tank dedicated to the development and integration of dual use digital technologies such as AI, big data, cloud networks, 5G, ICT, cybersecurity, advanced semiconductors, quantum computing, IOT, etc. He is also currently an adjunct professor at Saint Leo University where he teaches courses in Democracy, Democratic Institutions, and Historical Immigration.

SPECIAL THANKS TO TECHNICAL EDITORS

Susan An Esq., Chief Executive Officer, Sokat.com

Alka Patel, Chief, Responsible AI, DOD Joint Artificial Intelligence Center (JAIC)

Sam Gunter, Johns Hopkins University

NOTES

1. M. McFarland, October 24, 2014, Elon Musk: "With artificial intelligence we are summoning the demon." *The Washington Post*, https://www.washingtonpost.com/news/innovations/wp/2014/10/24/elon-musk-with-artificial-intelligence-we-are-summoning-the-demon/.
2. Sanchita Dash, "Elon Musk and Jack Ma Fight about AI and Mars, but Agree That 'Love Is the Answer,'" *Business Insider*, August 29, 2019, www.businessinsider.in/elon-musk-and-jack-ma-fight-about-ai-and-mars-but-agree-that-love-is-the-answer/articleshow/70892426.cms, accessed February 5, 2022.
3. Will Heaven, "OpenAI's New Language Generator GPT-3 Is Shockingly Good—and Completely Mindless," MIT Technology Review, July 20, 2020, www.technologyreview.com/2020/07/20/1005454/openai-machine-learning-language-generator-gpt-3-nlp/.
4. A. Lee, August 9, 2020, What is China's social credit system and why is it controversial? *South China Morning Post,* https://www.scmp.com/economy/china-economy/article/3096090/what-chinas-social-credit-system-and-why-it-controversial.
5. National Commission on AI, "NSCAI Submits First Quarter Recommendations to Congress," NSCAI, April 1, 2020, www.nscai.gov/2020/04/01/nscai-submits-first-quarter-recommendations-to-congress-2/#:~:text=NSCAI%20recommended%20steps%20to%3A%20increase%20funding%20for%20non-defense, accessed February 5, 2022.
6. Dr. Lee, K.-F. (2021), Founder - Sinovation Ventures, Sinovationventures.com, https://sinovationventures.com/index.php/home/aboutus/teams.html
7. Proposal of the Central Committee of the Chinese Communist Party on Drawing Up the 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2030, December 2, 2020, Center for Security and Emerging Technology, https://cset.georgetown.edu/research/proposal-of-the-central-committee-of-the-chinese-communist-party-on-drawing-up-the-14th-five-year-plan- for-national-economic-and-social-development-and-long-range-objectives-for-2030/.
8. ACT-IAC AI Working Group, 2020, ARTIFICIAL INTELLIGENCE FEDERAL WORKFORCE CERTIFICATION EMERGING TECHNOLOGY COMMUNITY OF INTEREST Artificial Intelligence Working Group, In ACT-IAC Accelerating Government, https://www.actiac.org/system/files/AI%20Knowledge%20Certification_2.pdf.
9. A. Lee, August 9, 2020, What is China's social credit system and why is it controversial? South China Morning Post, https://www.scmp.com/economy/china-economy/article/3096090/what-chinas-social-credit-system-and-why-it-controversial.
10. S. Bringsjord and N.S. Govindarajulu, 2018, Artificial Intelligence, *Stanford Encyclopedia of Philosophy,* Stanford University, https://plato.stanford.edu/entries/artificial-intelligence/.
11. E. Schmidt, R. Work, C. Catz, E. Horvitz, S. Chien, A. Jassy, M. Clyburn, G. Louie, C. Darby, W. Mark, K. Ford, J. Matheny, M. Griffiths, K. McFarland, and A. Moore, 2021, Final Report National Security Commission on Artificial Intelligence, https://www.nscai.gov/wp- content/uploads/2021/03/Full-Report-Digital-1.pdf.
12. Vincent, James, "Google 'Fixed' Its Racist Algorithm by Removing Gorillas from Its Image-Labeling Tech," The Verge, The Verge, January 12, 2018, www.theverge.com/2018/1/12/16882408/google-racist-gorillas-photo-recognition-algorithm-ai.
13. J. Dastin, October 10, 2018, Amazon scraps secret AI recruiting tool that showed bias against women, Reuters, https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G.
14. J. Buolamwini, T. Gebru, S. Friedler, and C. Wilson, 2018, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, Proceedings of Machine Learning Research, 81, 1-15, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.
15. Bureau of Justice Statistics, Report title: Prisoners in 2019 NCJ 255115, October 22, 2020, accessed March 3, 2021, https://www.bjs.gov/index.cfm?ty=tp&tid=1.
16. C. O'Neil, WEAPONS OF MATH DESTRUCTION: How big data increases inequality and threatens democracy, New York: Broadway Books, 2017.
17. Executive Office of the President, May 16, 2017, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, *Federal Register,* https://www.federalregister.gov/documents/2017/05/16/2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical- infrastructure.
18. CyberCorps. (n.d.). SFS. Www.sfs.opm.gov, retrieved February 5, 2022, https://www.sfs.opm.gov/
19. *Merriam-Webster,* 2019, Definition of ETHIC, https://www.merriam-webster.com/dictionary/ethic.

NOTES

20. K. McGrory and N. Bedi, September 3, 2020, Target, *Tampa Bay Times,* https://projects.tampabay.com/projects/2020/investigations/police-pasco-sheriff-targeted/intelligence-led-policing/.
21. United Nations Educational, Scientific and Cultural Organization, November 24, 2021, Recommendation on the Ethics of Artificial Intelligence, https://unesdoc.unesco.org/ark:/48223/pf0000380455.
22. J. Barnett, November 17, 2021, DOD organizations plot implementation of ethical AI in new guidance, Fedscoop, https://www.fedscoop.com/diu-ai-ethics-guidance-for-contractors/.
23. Otto Mallery, "Economic Union and Enduring Peace," Annals 216 (July 1941): 125-126.
24. David Lynch, "How the U.S.-China Trade War Became a Conflict over the Future of Tech," *The Washington Post*: Business, May 22, 2019, accessed November 24, 2019; Gavekal Research, "What's Really at Stake in the US-China Rivalry," Gavekal, May 9, 2018, http://web.gavekal.com/article/whats- really-stake-us-china-rivalry; Elsa Kania, "Innovation in the New Era of Chinese Military Power: What to Make of The New Chinese Defense White Paper, The First Since 2015," *The Diplomat*, July 25, 2019, accessed October 13, 2019, https://thediplomat.com/2019/07/innovation-in-the-new-era-of-chinese- military-power/.
25. Gavekal Research, "What's Really at Stake in the US-China Rivalry."
26. R. Ashooh, 2019, Addition of Entities to the Entity List and Revision of an Entry on the Entity List. In Department of Commerce. Bureau of Industry and Security, https://s3.amazonaws.com/public-inspection.federalregister.gov/2019-13245.pdf.
27. Discourses concerning government by Sidney, Algernon, 1622-1683; John Adams Library (Boston Public Library), BRL; Filmer, Robert, Sir, d. 1653; Sidney, Algernon, 1622-1683; Adams, John, 1735-1826, former owner.
28. Locke's Two Treatises on Government and Essay Concerning Human Understanding.
29. Elsa Kania, "Innovation in the New Era of Chinese Military Power: What to Make of The New Chinese Defense White Paper, The First Since 2015," *The Diplomat*, July 25, 2019, accessed October 13, 2019.
30. Schmidt, Work, Catz, Horvitz, Chien, Jassy, Clyburn, Louie, Darby, Mark, Ford, Matheny, Griffiths, McFarland, and Moore, Final Report National Security Commission on Artificial Intelligence.
31. J. Bughin, J. Seong, J. Manyika, M. Chui, and R. Joshi, 2019, https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Artificial%20Intelligence/Notes%20from%20the%20frontier%20Modeling%20the%20impact%20of%20AI%20on%20the%20world%20economy/MGI-Notes-from-the-AI-frontier-Modeling-the-impact-of-AI-on-the-world-economy-September-2018.ashx.
32. NSTC, 2019, "The National Artificial Intelligence Research and Development Strategic Plan: 2019 Update." Whitehouse.gov., National Science and Technology Council: Select Committee on Artificial Intelligence, June 2019, accessed January 22, 2020, 1-42. https://trumpwhitehouse.archives.gov/wp-content/uploads/2019/06/National-AI-Research-and-Development-Strategic-Plan-2019-Update-June- 2019.pdf.
33. Schmidt, Work, Catz, Horvitz, Chien, Jassy, Clyburn, Louie, Darby, Mark, Ford, Matheny, Griffiths, McFarland, Moore, Final Report: National Security Commission on Artificial Intelligence.
34. JAIC Public Affairs, 2021. "AI Ethical Principles – Highlighting the Progress and Future of Responsible AI in the DoD". AI in Defense. March 26, 2021, accessed March 12, 2021. https://www.ai.mil/blog_02_26_21-ai_ethics_principles- highlighting_the_progress_and_future_of_responsible_ai.html.
35. Gavekal Research, "What's Really at Stake in the US-China Rivalry."

How China's Cyber Operations During the COVID-19 Pandemic Worsened the United States Biodefense and National Security

Lieutenant Colonel Regan F. Lyon

INTRODUCTION

Until 2020, biological warfare seemed like a remote threat to military operations and national security. Then, in March 2020, the novel SARS-associated coronavirus (SARS-CoV2) emerged and forced the world, including the Department of Defense (DoD), to acknowledge the calamitous potential of deadly virus pandemics.

The United States 2018 National Biodefense Strategy (NBS) warns of the need to enhance biological threat responses to prevent such detrimental effects.[1] It highlights the natural, isolated outbreaks of Systemic Acute Respiratory Syndrome (SARS), Ebola, and Zika viruses as potential agents on which clandestine bioweapon programs or terrorist groups seeking such programs could capitalize.[2] The NBS outlines a plan to prevent, detect, and respond to biological threats, providing defense and deterrence strategies to avert bioweapon use on American civilians or military personnel.[3] A nation with a strong biological defense decreases its population's vulnerability to pathogens with aggressive exposure mitigation and effective treatment measures, which thereby increase the nation's resiliency to public health crises. Such defense capabilities change an adversary's cost-benefit balance so that it avoids initiating a biological attack, providing deterrence from future threats. The success of these response strategies requires cooperation among government, medical, public health personnel, and the general population.

Lt. Col. Regan F. Lyon is an emergency medicine physician and a recent graduate of the Defense Analysis master's program at the Naval Postgraduate School in Monterey, CA. Lt. Col. Lyon was commissioned after graduation from Texas A&M University in 2006, completed medical school through the Uniformed Services University of the Health Sciences (USUHS), and graduated from the Emergency Medicine Residency at Brooke Army Medical Center. In 2014, she deployed as the medical director of the 83rd Rescue Squadron at Bagram Airfield, Afghanistan. She deployed in support of Operation INHERENT RESOLVE as the Special Operations Surgical Team's emergency medicine physician in 2017 and Team Leader in 2019. Lt. Col. Lyon has specific interests in the employment of battlefield medicine and its impact on operations. In recognition of her academic contributions, she was appointed to an Assistant Professorship at the USUHS Department of Military and Emergency Medicine.

SARS-CoV2's high transmission rate, long incubation period, airborne transmission, and significant morbidity/mortality are the ideal qualities for biological weapons.[4] Just two years after the NBS's publication, the COVID-19 pandemic put it to the test, thus providing an excellent opportunity to evaluate US bioterrorism defense and deterrence strategies.

Cyber-enabled information operations, conducted largely through social media, created confusion, skepticism, resistance, and division within the US population, and thus negatively impacted the US response to the COVID-19 pandemic.[5] A poor pandemic response from the US created an opportunity for China to improve its international reputation and power, consistent with its proclaimed national strategy.[6] This article describes how Chinese cyber-enabled information operations during the pandemic threatened our national security by increasing China's perceived power and undermining democracy.[7] It will also examine the effects of these operations on US' NBS and our increased vulnerability to future biological attacks.

BIOWARFARE AND ITS DEFENSE AND DETERRENCE

The psychological and physical impacts of biological weapons on civilians and military units have been exploited by adversaries throughout history. One of the first recounted biological warfare attacks was the siege of Caffa in 1346.[8] During this conflict, the invading Tartar army fell victim to the plague and sustained numerous casualties as a result. Recognizing the infectious nature of the disease, the Tartars tossed the infected cadavers over the city wall, initiating an outbreak, causing panic in the city, and forcing the opposing force to flee. More recently, the US saw the use of bioweapons in the wake of the September 11, 2001, terrorist attacks on the World Trade Center. The following week, several media outlets and Congressional offices received anthrax spores through the mail in an attempt to capitalize on and further increase the heightened stress within the US. The overwhelming fear and psychological impact on the US populace underscore bioterrorism's potential for severe disruption even when casualties are limited.[9]

Biological weapons are considered weapons of mass destruction and are prohibited by the 1972 UN Biological Weapons Convention (BWC).[10] Unfortunately, not all potential adversaries adhere to these standards. Terrorists and other non-state actors are also not part of such agreements, and nation states that did ratify the treaty could potentially enlist covert operations or non-state proxies to use bioweapons. While there have been no intentional large-scale attacks by adversarial nation states to date, terrorist groups and covert operations have utilized biological weapons for small operations.[11] To prevent the use of biological weapons and limit their effectiveness when used, the biological defense and deterrence measures outlined in the NBS must be credible and effective.

More commonly used in nuclear warfare strategy, the concepts of defense and deterrence involve protection and security from offensive operations, including biological weapons, by an adversary.[12] Defense refers to the ability of a target to prevent or minimize damage sustained from an adversary action, decreasing the effectiveness of the attack and imposing a high cost-to-benefit burden on the adversary.[13] In the case of bioterrorism, adequate medical responses decreasing the transmissibility, disease severity, and mortality negate the overall weapon effectiveness. Deterrence attempts to prevent an adversary from taking harmful actions. One of the methods to achieve deterrence is deterrence by denial in which mechanisms are already in place that would mitigate an action taken by an adversary.[14] In the case of biological warfare, vaccines prevent susceptibility to a microbe, making the weapon useless against those vaccinated. The challenge with deterrence through vaccination is that a biological agent must be identified and determined to be a threat prior to developing a vaccine against it. An efficient defense response can also provide deterrence of future attacks because the effectiveness of previous attacks was low.

The linchpin for the NBS to be successfully employed is that the public receive reliable and objective communication.[15] Public distrust in the government causes multiple breakdowns in the NBS as it hinders communication to the public, inter-agency cooperation, and compliance with public health measures. Disseminating information regarding an outbreak, infection characteristics, response protocols, and public health measures relies on effective communication between the government and citizens. A lack of trust in the government breeds suspicion of the validity of information and fosters non-compliance, or even resistance, to protective measures. Furthermore, medical professionals skeptical of the government's actions or motivations during an outbreak will not likely reinforce and support the public service announcements. This lack of reinforcement from subject matter experts worsens public skepticism and non-compliance.

The misinformation campaigns that emerged during the COVID pandemic impaired the US' response to the public health crisis, thereby worsening the nation's bioterrorism deterrence and defense strategies. Adversaries, including China, have employed cyber operations against the US during the pandemic to cause chaos and confusion and used these operations to increase distrust in the U.S. Government (USG).[16] As the fruits of their labor have played out, however, third- and fourth-order effects of these misinformation campaigns are shaping a narrative to the world regarding US bioterrorism vulnerability.

CHINA'S CYBER OPERATIONS COVID-19 CASE STUDY

While likely not an original goal of China's cyber operations, the public health crisis and pandemonium that followed the SARS-CoV2 outbreak have highlighted our nation's bioweapon vulnerabilities to the world and may have caused unintended serious national security consequences. Any uncertainty adversaries may have had regarding our biodefense capabilities and weaknesses, which deterred employment of biological weapons prior to the pandemic, no longer exists. This section utilizes the COVID-19 pandemic as a case study to provide examples of China's cyber operations' effects on our bioterror defense and deterrence.

China's status as a reliable global power was called into question because of its initial cover-up of the outbreak in December 2019 and erroneous accusations of accidental release from research laboratories. Chinese misinformation and propaganda campaigns began in February 2020 with two primary objectives: shift blame for the pandemic from China and create dissonance within the finger-pointing democracies to worsen their pandemic management and control.[17]

Official statements, news reports, and social media campaigns attempted to turn speculations of COVID-19's origin outside Chinese borders.[18] Over a year later, China has continued to change the origin narrative through Facebook posts and peer-reviewed medical journals, despite substantiating evidence, to off-load the blame for the catastrophic infection numbers.[19] Through tools such as the Great Cannon, Chinese media highlighted their international humanitarian aid to nations experiencing medical supply shortages, underscoring their superior crisis response capability.[20]

Sowing Distrust

To destabilize democracies, specifically the US, cyber misinformation operations were employed to create domestic division, sow distrust and panic, and further deteriorate outbreak control.[21] Since the first case of COVID-19 was reported in the US on January 19, 2020,[22] Americans have anxiously watched if the government's response would prevent a nation-wide crisis. Case numbers grew over the next few weeks, and with stories of lockdowns across the world filling newsfeeds, concern grew as to how severely the US would restrict its citizens to control virus transmission. Internationally, nations began casting blame on China for downplaying the outbreak, which began the largest global health and economic crisis in recent history.

The reputational damage triggered China's plummet from its recent rise in power, leading Beijing to shift blame and portray its strong, heroic role relative to floundering democratic states.

One of China's cyber operations aimed at discrediting the USG's COVID response occurred almost simultaneously with the "viral origin" propaganda early in the pandemic. Chinese cyber forces amplified a fake news rumor of the White House implementing the Stafford Act and ordering a nation-wide shutdown.[23] In a national crisis, the Robert T. Stafford Disaster Relief and Emergency Assistance Act authorizes the President to mobilize an emergency federal government response, institute rules and regulations, and to utilize Department of Defense assets to assist state and local governments.[24] Martial Law, which is separate from the Stafford Act, refers to military control over domestic populations during wartime or natural disaster. Conspiracists conflated the two terms and speculated President Trump would invoke the Stafford Act for a national lockdown and utilize military force to ensure compliance. While officials do not believe Chinese cyber personnel started these theories, evidence points to China utilizing social media bots to proliferate and highlight them on media platforms to create division and distrust among the US population.[25]

US citizens were significantly confused, discouraged, and fearful when China executed a cyber-enabled information operation to capitalize on the instability. On March 13, 2020, social media posts began circulating that warned of a National Guard deployment to enforce an impending Stafford Act implementation by the White House.[26] No clear evidence suggests the original posts were the result of a cyber-enabled information operation. However, Chinese social media bots spreading these messages attributed the information to close contacts within reputable organizations like the National Guard, Department of Homeland Security, the State Department, FBI, etc., and encouraged wider sharing of the messages.[27] The results reinforced fears of the pandemic's severity and beliefs that the administration was about to exceed its authority. Warnings of a nationwide shutdown supported concerned citizens' speculation of officials minimizing the virus's severity. For citizens already dissatisfied with the current administration, rumors of enacting the Stafford Act deepened their distrust in the government. These two extreme divergent reactions began a chain reaction which demonstrated how China's cyber operations undermined democratic power and increased our bioterror vulnerability.

Most analysts believe that China's primary objective in this campaign was to increase Americans' anti-government sentiments, worsening stability.[28] The threat of invoking a nationwide lockdown with deployed National Guard personnel for enforcement sparked public concern of an abuse of power by the Trump administration and violation of citizens' rights. The social media posts and text messages referencing sources linked to reputable government agencies exploited people's trust in their network and strengthened these allegations. Such civil unrest begins to undermine democratic institutions, worsens other nations' perceptions of our stability, threatens national security, and advances the communist government's argument of superiority.

Defense Breakdown

When the Stafford Act social media posts began to circulate, serious concerns spread that the virus was more dangerous than originally reported. The US public flooded stores to stock up on "essential items" in preparation for a lockdown. In addition to the infamous toilet paper shortage, shelves and online outlets were soon devoid of masks, gloves, and sanitizers, including within healthcare supply chains. Once it was discovered that N95 masks, used to prevent medical personnel from contracting airborne pathogens, were effective against SARS-CoV2, the situation worsened.[29] Demand quickly exceeded supply, leaving frontline medical personnel without the appropriate personal protective equipment (PPE) required to care for infected patients.[30] Healthcare workers began openly complaining of the nation-wide PPE shortage and the risk it brought to their lives.

The strained PPE supply chain exacerbated by the public hoarding caused a ripple effect within the healthcare system. Hospitals began instituting resource conservation policies to extend the life of supplies intended for one-time use since these items were on indefinite back-order. Concurrently, these measures also helped to alleviate costs since hospitals were generating less revenue from the Stay-at-Home campaign. Healthcare workers interpreted these PPE conservation measures as the hospitals jeopardizing their safety and initiated lobbying for government involvement.

The saturation of stories showing pandemic mismanagement by democratic nations and exaggerated success stories of containment at home boosted China's legitimacy on the global stage. US media was swarmed with accounts of disgruntled healthcare workers risking their lives daily due to a lack of PPE. Beijing capitalized on these news reports and recirculated them through the Great Cannon as propaganda illustrating how China was gaining control of viral spread and protecting their healthcare workers better than the western democracies.[31] Chinese cyber accounts and media sources discovered and broadcasted pictures of healthcare workers using garbage bags as PPE.[32] Such stories accused the ill-prepared countries of ignoring the needs of their medical personnel and putting additional lives at risk. Although these claims were mere speculation at the time, prospective studies have since reported healthcare workers with inadequate PPE had a statistically significant increase of COVID-19 infection compared to those with adequate PPE.[33] This Chinese cyber strategy was employed domestically to reinforce the long-time message to citizens that "socialism is good, democracy is bad."

The 2018 NBS mandates robustly mobilizing PPE for frontline healthcare workers and establishing a communication plan on preventive health measures for the public in the event of an attack.[34] The ability to provide adequate PPE for medical personnel is a vital defense tactic, as it increases the efficiency of the healthcare system to treat casualties in response to a biological outbreak. Having the ability to mobilize these resources to hospitals strengthens bioterror deterrence by demonstrating to a potential adversary that a bioterror attack would have a limited effect on a population.

The initial US defense measures against SARS-CoV2 were painted as ineffective through reports of public hoarding, inadequate PPE supply chains, and inappropriate PPE conservation measures by hospitals. While Beijing's primary objective was to increase China's international reputation, its cyber operations highlighting the inadequate public health response worsened US national security by undermining our biodefense strategy.

Deterrence Breakdown

Classic nuclear weapon deterrence focuses on retaliation and what has been called mutually assured destruction, but future bioweapon deterrence relies more on past defensive responses to previous biological outbreaks. Increasing the effectiveness of public health and protective measures in decreasing impacts of a biological attack reduces the incentive for adversary use of biological weapons. Non-compliance with these measures reduces their deterrent value.

America's individualistic nature, amplified by the cyber-induced government distrust, led to significant non-compliance with government-implemented public health policies. One survey indicated that 58% of Americans preferred "freedom…without interference from the state," compared to 30-38% of Europeans.[35] This hindered our ability to "flatten the curve" compared to other countries.[36] The US' inadequate public health measures followed by the rapid spread of COVID-19—especially compared to China—signals to adversaries our vulnerability to biological attacks.

Another bioweapon deterrence strategy is vaccination against the biological agent. Because vaccines cannot be developed until after a threat is identified, vaccines deter the use of a specific agent for future attacks. This strategy only works for a nation with access to vaccines and a population willing to be inoculated.

China's attack on Western-developed vaccines started with cyber operations intended to steal SARS-CoV2 vaccine development information. The US identified both Chinese and Russian cyber espionage attacks against vaccine developers, another indication of China borrowing Russia's playbook.[37] This may have strictly been another example of Chinese intellectual property theft, but US officials raised concerns that these cyber actions could sabotage the target's operations to create defects in the product and dissemination delays.[38] Broken promises of vaccination timelines and effectiveness expanded suspicion towards the government, escalated the anti-vax claims, and exacerbated public division. Operation Warp Speed, however, maintained a reasonable timeline, and China turned to other tactics to reinforce their legitimacy, to undermine democracy, and to weaken our national security and biodefense measures.[39]

Past vaccination resistance, such as during the 19th-century UK smallpox epidemic and the 2019 US measles outbreak, highlights a population's vulnerability to anti-vaxxer campaigns. This is even more of a problem when cyber disinformation reinforces doubts.[40] For example, early in the pandemic, COVID-19 anti-vaccine social media posts warned that future coronavirus vaccines could contain toxic chemicals or tracking devices used by the USG.[41]

China fueled the anti-vax movement by discrediting US vaccines through disinformation campaigns.[42] The Wolf Warriors began spreading conspiracy theories regarding the Pfizer and Moderna vaccines even before they were released to the public.[43] These trolling attacks focused on the vaccines' safety and were echoed by Chinese nationalist media and Chinese officials.[44] Other Chinese blogs claimed the efficacy of the mRNA vaccines was only 29%, significantly lower than what the US claimed and what turned out to be true. Simultaneously, cyber campaigns boasted of China-developed vaccines in attempts to increase international demand and bolster their pandemic reputation.[45]

COVID vaccine speculation and conspiracy theories, exacerbated by cyber disinformation campaigns, created significant resistance to receiving a vaccine. Surveys conducted prior to vaccine release estimated one third of Americans, compared to 14% of UK citizens, would refuse vaccination.[46] By summer of 2021, a few months after a vaccine was available to all citizens 12 years of age or older, only 48.5% of the population was fully vaccinated.[47] The unvaccinated population enabled the Delta variant to become the dominating SARS-CoV-2 strain in August 2021, and hospital systems in less-widely vaccinated populations were once again strained.[48] The unvaccinated then facilitated further mutations that led to the highly-transmissible Omicron variant, which emerged in the US in early December 2021.[49] A population that is not vaccinated increases susceptibility to a biological agent and facilitates its propagation, transmission, and mutations, ultimately decreasing deterrence by denial.

CONCLUSION

The SARS-CoV-2 pandemic panic in 2020, exacerbated by China's misinformation cyber campaign, highlighted a critical vulnerability in the most important US defense strategies against bioterrorism: prevention and resilience. The simultaneous reports of inadequate PPE for healthcare workers reduced faith in the government by affected healthcare workers and concerned citizens alike. The collective effort of the US population began to split just when cohesiveness was most needed to flatten the curve of COVID-19 infections, gain control of the pandemic and economic crises, implore Americans to protect themselves with vaccines, and salvage our international political and biodefense image. The growing impact of mis- and disinformation in the twenty-first century not only made the US a target for exploitation but showcased our inadequate pandemic response measures. Ignoring the role of cyber operations in amplifying the effects of bioterrorism compounds our vulnerability to such attacks.

Any signals that biological deterrence or defense mechanisms were weakened because of China's cyber-enabled information operations will play into the adversary cost-to-benefit considerations of bioweapon employment. This confluence of cyber operations, medicine and public health, and national security is unique, unprecedented, and requires a multi-dimensional counter strategy. The medical community must work with the government to evaluate the pandemic response in relation to the NBS, identify NBS weaknesses and systemic failures, and strategically signal the rectification of identified vulnerabilities. Concurrently, this pandemic has highlighted evolving Chinese cyber strategies for the cyber and intelligence communities. It has also taught medical professionals to consider cyber threats beyond personal health information hacking efforts. Recognition of China's brazen tactics will assist the US in developing countermeasures for future cyber information operations and in arming US citizens with the tools to identify and discredit such propaganda. Understanding the role of cyber-enabled information operations on our biodefense strategies will enable further research on countering our weaknesses and protecting our national security.

DISCLAIMER

The views expressed herein are those of the author and do not reflect the official policy or opinion of the Naval Postgraduate School, Department of the Air Force, Special Operations Command, Department of Defense, or the U.S. Government.

NOTES

1. White House, *National Biodefense Strategy of the United States of America (*Washington, DC: White House, 2018), i.
2. Ibid, 2–3.
3. Ibid, 1.
4. Yu Chen and Lanjuan Li, "SARS-CoV-2: Virus Dynamics and Host Response," *The Lancet Infectious Diseases* 20, no. 5 (May 1, 2020): 515–16, https://doi.org/10.1016/S1473-3099(20)30235-8.
5. Julian E. Barnes, Matthew Rosenberg, and Edward Wong, "As Virus Spreads, China and Russia See Openings for Disinformation," *The New York Times*, March 28, 2020, sec. U.S., https://www.nytimes.com/2020/03/28/us/politics/china-russia-coronavirus-disinformation.html.
6. Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China* (Washington, DC: Department of Defense, 2020), https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF.
7. Jessica Brandt and Torrey Taussig, "The Kremlin's Disinformation Playbook Goes to Beijing," Brookings, May 19, 2020, https://www.brookings.edu/blog/order-from-chaos/2020/05/19/the-kremlins-disinformation-playbook-goes-to-beijing/.
8. Stefan Riedel, "Biological Warfare and Bioterrorism: A Historical Review," *Baylor University Medical Center Proceedings* 17, no. 4 (October 2004): 400, https://doi.org/10.1080/08998280.2004.11928002.
9. Robert Roos and Lisa Schnirring, "Public Health Leaders Cite Lessons of 2001 Anthrax Attacks," Center for Infectious Disease Research and Policy, September 1, 2011, https://www.cidrap.umn.edu/news-perspective/2011/09/public-health-leaders-cite-lessons-2001-anthrax-attacks.
10. "Biological Weapons," accessed March 11, 2022, https://www.who.int/westernpacific/health-topics/biological-weapons; Riedel, "Biological Warfare and Bioterrorism."
11. Riedel, "Biological Warfare and Bioterrorism," 404.
12. Glenn Herald Snyder, *Deterrence and Defense* (Princeton University Press, 2015), 3.
13. Ibid, 4.
14. Ibid, 14–15.
15. Abhay B. Kadam and Sachin R. Atre, "Negative Impact of Social Media Panic during the COVID-19 Outbreak in India," *Journal of Travel Medicine* 27, no. 3 (May 18, 2020), https://doi.org/10.1093/jtm/taaa057.
16. Mark Bryan Manantan, "Unleash the Dragon: China's Strategic Narrative during the COVID-19 Pandemic," *The Cyber Defense Review* 6, no. 2 (Spring 2021): 71–89.
17. David Erdahl, Sandy Gitter, and Brock Lu, "China Will Do Anything to Deflect Coronavirus Blame," *Foreign Policy* (blog), accessed September 8, 2020, https://foreignpolicy.com/2020/03/30/beijing-coronavirus-response-see-what-sticks-propaganda-blame-ccp-xi-jinping/.
18. Ibid.
19. Emma Graham-Harrison and Robin McKie, "A Year after Wuhan Alarm, China Seeks to Change Covid Origin Story," *The Guardian*, November 29, 2020, http://www.theguardian.com/world/2020/nov/29/a-year-after-wuhan-alarm-china-seeks-to-change-covid-origin-story.
20. Keith Bradsher and Liz Alderman, "The World Needs Masks. China Makes Them, but Has Been Hoarding Them.," *The New York Times*, March 13, 2020, sec. Business, https://www.nytimes.com/2020/03/13/business/masks-china-coronavirus.html.
21. Brandt and Taussig, "The Kremlin's Disinformation Playbook Goes to Beijing."
22. Michelle L. Holshue et al., "First Case of 2019 Novel Coronavirus in the United States," *New England Journal of Medicine* 382, no. 10 (March 5, 2020): 929–36, https://doi.org/10.1056/NEJMoa2001191.
23. Edward Wong, Matthew Rosenberg, and Julian E. Barnes, "Chinese Agents Helped Spread Messages That Sowed Virus Panic in U.S., Officials Say," *The New York Times*, April 22, 2020, sec. U.S., https://www.nytimes.com/2020/04/22/us/politics/coronavirus-china-disinformation.html.
24. "H.R.2707 - 100th Congress (1987-1988): Major Disaster Relief and Emergency Assistance Amendments of 1987," November 23, 1988, 1987/1988, https://www.congress.gov/bill/100th-congress/house-bill/2707.
25. Wong, Rosenberg, and Barnes, "Chinese Agents Helped Spread Messages That Sowed Virus Panic in U.S., Officials Say."

NOTES

26. Ibid.
27. Ibid.
28. Barnes, Rosenberg, and Wong, “As Virus Spreads, China and Russia See Openings for Disinformation.”
29. Kadam and Atre, “Negative Impact of Social Media Panic during the COVID-19 Outbreak in India.”
30. World Health Organization, “Shortage of Personal Protective Equipment Endangering Health Workers Worldwide,” World Health Organization, March 3, 2020, https://www.who.int/news-room/detail/03-03-2020-shortage-of-personal-protective-equipment-endangering-health-workers-worldwide.
31. Li Yuan, “With Selective Coronavirus Coverage, China Builds a Culture of Hate,” *The New York Times,* April 22, 2020, sec. Business, https://www.nytimes.com/2020/04/22/business/china-coronavirus-propaganda.html.
32. Ibid.
33. Long H Nguyen et al., “Risk of COVID-19 among Front-Line Health-Care Workers and the General Community: A Prospective Cohort Study,” *The Lancet Public Health* 5, no. 9 (September 1, 2020): e475–83, https://doi.org/10.1016/S2468-2667(20)30164-X.
34. White House, *National Biodefense Strategy of the United States of America.*
35. Alex Fitzpatrick, “Why the U.S. Is Losing the War On COVID-19,” *Time*, August 13, 2020, https://time.com/5879086/us-covid-19/.
36. Ibid.
37. Joseph Marks, “The Cybersecurity 202: Russia and China’s Vaccine Hacks Don’t Violate Rules of Road for Cyberspace, Experts Say,” *Washington Post,* July 20, 2020, https://www.washingtonpost.com/politics/2020/07/20/cybersecurity-202-russia-china-vaccine-hacks-dont-violate-rules-road-cyberspace-experts-say/.
38. Julian E. Barnes and Michael Venutolo-Mantovani, “Race for Coronavirus Vaccine Pits Spy Against Spy,” *The New York Times*, September 5, 2020, sec. U.S., https://www.nytimes.com/2020/09/05/us/politics/coronavirus-vaccine-espionage.html.
39. Jon Cohen, “With Global Push for COVID-19 Vaccines, China Aims to Win Friends and Cut Deals,” *Science,* November 25, 2020, https://www.sciencemag.org/news/2020/11/global-push-covid-19-vaccines-china-aims-win-friends-and-cut-deals.
40. Steven King, “Coronavirus Vaccine: Lessons from the 19th-Century Smallpox Anti-Vaxxer Movement,” The Conversation, July 31, 2020, http://theconversation.com/coronavirus-vaccine-lessons-from-the-19th-century-smallpox-anti-vaxxer-movement-143375. Julie Charpentrat, “There’s Another Insidious Side Effect of This Pandemic - More Anti-Vaxxer Activity,” ScienceAlert, July 5, 2020, https://www.sciencealert.com/anti-vaxxers-seize-virus-moment-to-spread-fake-news.
41. Charpentrat, “There’s Another Insidious Side Effect of This Pandemic - More Anti-Vaxxer Activity”; Elizabeth Cohen and Dana Vigue, “US Government Slow to Act as Anti-Vaxxers Spread Lies on Social Media about Coronavirus Vaccine,” *CNN*, August 13, 2020, https://www.cnn.com/2020/08/12/health/anti-vaxxers-covid-19/index.html.
42. Barnes and Venutolo-Mantovani, “Race for Coronavirus Vaccine Pits Spy Against Spy.”
43. Carmen Paun and Susannah Luthi, “What China’s Vax Trolling Adds up to,” *POLITICO*, January 28, 2021, https://politi.co/3oqX66H.
44. Yaqiu Wang, “China’s Dangerous Game Around Covid-19 Vaccines,” Human Rights Watch, March 4, 2021, https://www.hrw.org/news/2021/03/04/chinas-dangerous-game-around-covid-19-vaccines.
45. Paun and Luthi, “What China’s Vax Trolling Adds up to.”
46. Cohen and Vigue, “US Government Slow to Act as Anti-Vaxxers Spread Lies on Social Media about Coronavirus Vaccine.” King, “Coronavirus Vaccine.”
47. Hannah Ritchie et al., “Coronavirus Pandemic (COVID-19) Vaccinations,” Our World in Data, accessed July 14, 2021, https://ourworldindata.org/covid-vaccinations; Cheyenne Haslett, “FDA Authorizes Pfizer Vaccine for 12-15-Year-Olds,” *ABC News,* May 10, 2021, https://abcnews.go.com/Politics/fda-authorizes-pfizer-12-15-year-olds/story?id=77419872.

Seventh Service: Proposal for the United States Cyber Force

Lieutenant Commander Michael G. McLaughlin

ABSTRACT

To fight and win in cyberspace, the United States needs a Cyber Force. During World War II, air power tipped the scale of victory in favor of the allies, as aviation proved to be an indispensable warfighting capability. The creation of the Air Force was predicated on the notion that the effective employment air power is not a matter of choice, but the very condition on which national survival rested. Today, cyber superiority has wider implications for US national security than air superiority had at the close of World War II; however, the federal government is not structured to effectively defend the US national interests. The current division of cyber authorities precludes comprehensive mitigation of cyber-enabled malicious activities. To effectively combat nation-state and non-state actors targeting US and allied interests in cyberspace, the US should establish a Cyber Force modeled on the U.S. Coast Guard with a reserve component modeled on the National Guard. Combining these models would allow for a single force capable of executing military operations, law enforcement activities, and intelligence collection at the direction of the Departments of Defense and Homeland Security, complemented by an expansive reserve component available to both state governors and the federal government.

INTRODUCTION

During World War II, air power tipped the scale of victory in favor of the allies, as aviation proved to be an indispensable warfighting capability.[1] From air-to-air engagements and tactical bombing campaigns to aircraft carrier-centered naval combat and the delivery of nuclear munitions—for the first time in history,

Michael McLaughlin is a cybersecurity attorney in Washington D.C. and research affiliate for the University of Maryland Applied Research Laboratory for Intelligence and Security. He previously served as the Senior Counterintelligence Advisor for United States Cyber Command and Chief of Counterintelligence and Human Intelligence for the Cyber National Mission Force. He holds a Bachelor of Science degree from the US Naval Academy and a Juris Doctorate from the University of Maryland School of Law. Lt. Cmdr. McLaughlin resides in Annapolis, Maryland, with his wife and their two sons.

the air became a significant warfighting domain.[2] Throughout the war, aviation components of the Army and Navy proved the value of complementing land and sea power with air power in every theater of combat.[3] After the war, America's military and political leaders recognized the inefficacy of having all the nation's air power subordinated as components of the Army and Navy.[4] Nearly two years after the end of hostilities, the National Security Act of 1947 officially established the United States Air Force as its own military service within the Department of Defense (DoD).[5]

The creation of the U.S. Air Force was predicated on the notion that a "realistic understanding of the new weapon, of its implications in terms of national security, of its challenge to America, is not a matter of choice," but one of the conditions on which national survival rested.[6] Today, cyber superiority has wider implications for US national security than air superiority had at the close of World War II, as every facet of life in America has become reliant on cyberspace.[7] However, unlike how DoD evolved its structure to meet the new challenges and opportunities of air warfare, no such significant structural change has materialized in the way in which the military resources, trains, and controls its forces for combating threats in the cyber domain. Despite DoD's recognition of cyberspace as a critical warfighting domain, there exists no standalone Cyber Force.[8] This shortcoming places the US at a disadvantage as digital warfare and threats continue to evolve. The US needs a Cyber Force with military, intelligence, and law enforcement authorities sufficient to effectively combat the malicious use of cyberspace.

There exist legal, organizational, and practical impediments to establishing an element with such broad powers. To prevent abuse of government power, the US has developed a system specifically designed to prevent the consolidation of domestic law enforcement, intelligence, and military capabilities.

This is an important division; however, it can also lead to dysfunction. Threats in cyberspace are inherently different from traditional national security threats. Malicious cyber actors recognize neither physical borders nor the distinction between military and non-military targets.[9] Nation-states frequently blend criminal activities, espionage, and military operations to conduct malicious activities and impose costs upon businesses, governments, and individuals.[10] The US considers these types of operations to be traditional military activities, yet the national framework for cyber incident coordination does not include the DoD.[11] To address the novel legal and operational challenges of cyber warfare and cyber-enabled malicious activities, the US needs to move beyond current monolithic military, intelligence, and law enforcement constructs to imagine a new Cyber Force.

Within the United States Code, there are several unique titles that, if combined, would imbue a Cyber Force with authorities commensurate with the evolving threats in cyberspace.[12] While different organizations within the federal government are authorized to conduct various activities under multiple titles, no single organization can leverage all requisite authorities for effectively combating malicious cyber actors and activities.

Within the DoD alone, different organizations and agencies operate in cyberspace under disparate legal frameworks. For example, while Military Department Counterintelligence Organizations (MDCOs)—such as the Naval Criminal Investigative Service (NCIS)—conduct counterintelligence and law enforcement activities, MDCOs are not authorized to conduct military operations.[13] The authority to conduct military operations is derived from orders issued to combatant commanders by the Secretary of Defense through the Chairman of the Joint Chiefs of Staff.[14] Conversely, while the Secretary of Defense (SECDEF) has ordered U.S. Cyber Command (USCYBERCOM) to execute military cyber operations to deter, disrupt, and defeat malicious cyber actors targeting DoD information networks and US critical infrastructure, USCYBERCOM has no authority to conduct counterintelligence or law enforcement activities.[15] However, there are organizations within the federal government whose roles, responsibilities, and authorities enable exceptions under the right circumstances to the separation of military, intelligence, and law enforcement powers—namely, the U.S. Coast Guard and National Guard. The exceptions under which these organizations can operate, and the circumstances under which they are allowable, offer a viable model and framework for designing roles, responsibilities, and authorities for a Cyber Force and corresponding National Guard component.

This article presents shortcomings inherent in both the current construct of DoD's cyber operations forces and the federal government's cyber incident coordination. It contends that the federal government's division of authorities precludes comprehensive mitigation of and response to cyber-enabled malicious activities targeting domestic cyberspace. To combat nation-state and non-state actors targeting US interests in cyberspace effectively, the federal government should establish a Cyber Force modeled on the U.S. Coast Guard with a reserve component modeled on the dual state/federal forces of the National Guard.

Though blending legal authorities in the digital age is a relatively new concept, the Coast Guard serves as a useful model because it has effectively integrated military capabilities and operations with law enforcement and homeland defense authorities for decades, for example in the War on Drugs and the Global War on Terror. Moreover, the National Guard has been extensively leveraged over the past 20 years to respond to natural disasters under state authority and deploy to Iraq and Afghanistan under federal authority. Combining these models would establish a single service capable of executing military operations, law enforcement activities, and intelligence collection at the direction of both DoD and Department of Homeland Security (DHS), complemented by a reserve component available to individual states and to the federal government.

PART I. CURRENT STRUCTURE

Department of Defense Cyber Operations Forces

Within DoD, USCYBERCOM is the unified combatant command whose area of responsibility is the global cyber domain.[16] The Commander of USCYBERCOM is principally charged with defending the DoD Information Network, and, on order, to "defend or secure . . . cyberspace related to critical infrastructure and key resources (CI/KR) of the US."[17] USCYBERCOM comprises 133 teams and over 6,200 cyber operations personnel assigned throughout the headquarters; service cyberspace component commands from the Army, Navy, Air Force, and Marine Corps; Joint Force Headquarters DoD Information Network (JFHQ-DODIN); and the Cyber National Mission Force (CNMF).[18] Each service component of USCYBERCOM executes defensive and offensive cyberspace operations to defend its respective service networks and to engage targets in and through cyberspace.[19] JFHQ-DODIN is the joint component charged with securing, operating, and defending the DoD information technology infrastructure.[20] Furthermore, consisting of over 2,000 personnel from each military service, the CNMF is the joint component responsible for executing the full spectrum of cyberspace operations to deter, disrupt, and defeat malicious cyber actors to defend the United States.[21]

As the DoD's joint force component for national cyber defense, the CNMF conducts cyberspace operations to defeat cyberspace threats to both the DoD Information Network and non-DoD cyberspace.[22] To this end, the CNMF conducts myriad offensive and defensive cyberspace operations external to DoD networks.[23] Since the activation of the CNMF in 2014, the Secretary of Defense has ordered USCYBERCOM to execute numerous cyberspace operations against malicious cyber actors. Frequently, these actors are affiliated with foreign intelligence services or are conducting espionage activities at their behest.[24]

Because the DoD requires the CNMF to execute what would traditionally constitute covert action or counterintelligence activities, Congress authorized the DoD to recharacterize these actors so as permit the CNMF to conduct operations against them.[25] In the 2020 National Defense Authorization Act, Congress reaffirmed that USCYBERCOM may conduct operations in cyberspace against malicious cyber actors as “traditional military activities.”[26] CNMF operations defending against and targeting malicious cyber actors, therefore, do not constitute counterintelligence activities.[27] Despite this limited legal nuance, USCYBERCOM cannot conduct the full range of counterintelligence or law enforcement activities and relies on other government organizations with those authorities to engage with domestic companies and organizations to defend the homeland.[28]

Within DoD, those authorities rest with the cyber elements of the military counterintelligence and law enforcement organizations, which comprise Cyber Crime Investigators from NCIS, the U.S. Army’s Counterintelligence Command and Criminal Investigative Division (CID), and the U.S. Air Force Office of Special Investigations (OSI).[29] These organizations are responsible for the collection, production, and dissemination of military-related counterintelligence, as well as conducting military law enforcement and counterintelligence activities both outside of the US and domestically.[30] Because malicious cyber actors target domestic companies and organizations for intellectual property theft, misappropriation of trade secrets, and other acts of espionage affecting DoD information, military counterintelligence and law enforcement organizations have broad authority to conduct activities on the networks of consenting organizations inside the US in coordination with the Federal Bureau of Investigation (FBI) and the Department of Justice (DOJ).[31] However, these organizations are not authorized to execute military cyber operations against malicious cyber actors; that authority resides solely with USCYBERCOM.[32]

DEPARTMENT OF HOMELAND SECURITY

DHS is responsible for the security of non-DoD federal information networks[33] and the protection of critical infrastructure,[34] as defined by Presidential Policy Directive (PPD) 21.[35] Within DHS, various agencies have sector-specific cyber responsibilities, such as the Coast Guard—responsible for cybersecurity in the maritime sector;[36] the U.S. Secret Service—responsible for investigating fraud and finance-related crimes;[37] the Transportation Security Administration (TSA)—responsible for the security of all modes of transportation, including, inter alia, aviation, shipping, and pipelines;[38] and the Federal Emergency Management Agency (FEMA)—responsible for the activation and support of emergency support functions under the National Response Framework and the National Cyber Incident Response Plan.[39] For the cyber efforts of the various sector-specific agencies within DHS, the dedicated lead is the Cybersecurity and Infrastructure Security Agency (CISA).[40] For significant cyber incidents, CISA also serves as the lead for asset response activities and coordinating field-level activities among DHS’s sector-specific agencies.[41]

FEDERAL GOVERNMENT CYBER INCIDENT RESPONSE

Though DHS serves as the lead agency for protecting and mitigating threats to federal networks and CI/KR, the federal government organizes its response to significant cyber events affecting the homeland through the coordination of field-level activities, national policy, and national operations across multiple agencies.[42] Field-level activities are those conducted at the affected entity, whether a critical infrastructure element, a federal government agency, or another affected entity.[43] National policy coordination consists of support to the National Security Council in the development and implementation of policy and strategy to address "significant cyber incidents affecting the US or its interests abroad."[44] National operational coordination consists of the establishment of a Cyber Unified Coordination Group (UCG) to coordinate responses to significant cyber incidents among federal government agencies.[45]

Within the UCG, there are designated lead agencies to ensure "maximum effectiveness" across three primary lines of effort: threat response, asset response, and intelligence support.[46] For threat response activities, the DOJ, acting through the FBI and the National Cyber Investigative Joint Task Force (NCIJTF), serves as the lead federal agency.[47] Threat response activities include the attribution, pursuit, and disruption of malicious cyber actors and activities.[48] This is done through criminal investigations, federal indictments, and economic sanctions aimed at countering the malicious cyber activity."[49] Asset response, led by the DHS, consists of activities aimed at mitigating network vulnerabilities and protecting assets against malicious cyber actors.[50] DHS does this by providing technical assistance, conducting threat hunting on affected networks, and facilitating information sharing across multiple industries.[51] Intelligence support is led by the Office of the Director of National Intelligence (ODNI), which directs the activities of the US Intelligence Community (IC).[52] Intelligence support activities are intended to identify and build awareness of cyber threats and facilitate information sharing.[53]

While this delineation of roles is intended to "achieve maximum effectiveness in coordinating responses to significant cyber incidents," the DoD and the significant resources and capabilities of the cyber operations forces are notably absent.[54] To compound this ambiguity in the role of the DoD in responding to national cyber incidents, the integration of DoD resources into the federal government's response to cyber events faces other barriers. For example, in 2015, Congress passed the Cybersecurity Information Sharing Act to encourage and facilitate the sharing of threat indicators, defensive measures, and best practices between public and private sector entities.[55] However, in November 2018, the DoD Inspector General (IG) found that the DoD had taken only limited actions to implement the Act's requirements.[56] Federal guidelines direct government agencies to make unclassified cyber threat indicators broadly available to other agencies as well as to non-federal entities as quickly as operationally practicable.[57] The DoD IG found that the DoD did not have the internal controls necessary to meet the Act's requirements for sharing cyber threat indicators and defensive measures.[58]

In addition to the limitations noted above, information silos exist which prevent the integration of different types of intelligence and operational activities that would enable the DoD to assist the federal government in a significant cyber incident and mitigate the risk of compromise by wide-scale cyber aggression. For example, because USCYBERCOM is not a member of the IC, it primarily relies upon tailored signals intelligence (SIGINT) or law enforcement-derived information to execute its missions.[59] As such, it is dependent on Intelligence Community and law enforcement partners that prize and seek to protect this information for their missions.[60] Where competition for resources exists, these information silos and restrictive information-sharing practices can limit or preclude integration and effective whole-of-government response to cyber events.

The exclusion of DoD from the framework for federal responses to cyber incidents is likely due in part to limitations in the manner in which the armed forces are permitted to operate domestically. For instance, using elements of DoD by civilian law enforcement in such a manner as to subject US citizens to a "regulatory, proscriptive, or compulsory" exercise of military power would violate the Posse Comitatus Act.[61] Intelligence elements of DoD are subject to intelligence oversight provisions of Executive Order 12333, prohibiting the intentional collection of information about US persons.[62] Moreover, non-intelligence elements of DoD are beholden to other legal provisions such as the Wiretap Act, which requires consent for government actors to access private networks.[63]

PART I. SUMMARY

Existing legal frameworks and restrictive departmental constructs like those discussed above keep the federal government from effectively integrating the totality of its capabilities and resources. Instead, it is waging an inefficient campaign, fraught with intra-departmental and interagency redundancies, information silos, and inefficient public-private partnerships.[64] "If the United States is to defeat these cyber threats, traditional notions regarding the division between criminal and national security matters must be reevaluated."[65] While the vast majority of cyber events affecting US cyberspace can be managed by individual network defenders and the current federal response construct, increasingly sophisticated nation-state attacks against the private sector "require a unique approach to response efforts."[66]

PART II. MORE EFFECTIVE MODELS

U.S. Coast Guard

The Coast Guard operates at the intersection of homeland defense, law enforcement, intelligence activities, and military operations.[67] It is the only element within the federal government where individual personnel can conduct activities simultaneously under authorities traditionally reserved for individual governmental agencies. The Coast Guard's unique composition offers a particularly good model for addressing the challenges inherent in the dynamic nature of cyberspace, where lines between domestic security, law enforcement, and warfare are often blurred.

Following 9/11, the Homeland Security Act of 2002 transferred the Coast Guard to the Department of Homeland Security.[68] When operating as a part of DHS, the Coast Guard has five homeland security missions: (1) Ports, waterways, and coastal security; (2) drug interdiction; (3) migrant interdiction; (4) defense readiness; and (5) other law enforcement activities.[69] As the agency responsible for the maritime sector within DHS, the Coast Guard maintains broad authority over the navigable waters of the US. These authorities include the ability to prescribe how private and commercial vessels operate,[70] control over the anchorage and movement of vessels to ensure the safety and security of US naval vessels,[71] and the ability to prescribe regulations for the inspection and certification of vessels.[72] Additionally, the Coast Guard may use its personnel, equipment, and facilities to assist federal, state, local, tribal, and territorial agencies when its assets are particularly qualified to perform a specific activity.[73]

To fulfill its role in the maritime domain effectively, the Coast Guard is authorized to operate as a law enforcement organization.[74] Coast Guard personnel have federal law enforcement authorities to board any vessel subject to the jurisdiction of the US, whether on the high seas or on waters over which the US has jurisdiction, to "make inquiries, examinations, inspections, searches, seizures, and arrests for the prevention, detection, and suppression of violations of US laws."[75] Additionally, when the President determines that US national security is endangered, the Coast Guard may enforce regulations within US territorial waters, including vessel seizure and forfeiture, and may fine and imprison the master and crew for noncompliance.[76]

In addition to its role as a sector-specific agency within DHS, the Coast Guard is also "a military service and a branch of the armed forces of the United States at all times."[77] As such, the President may direct elements of the Coast Guard be transferred to the Department of the Navy to execute operations consistent with the authorities of the armed forces.[78] For example, in April 2021, two Coast Guard cutters deployed to the Middle East to operate under the U.S. Navy's Fifth Fleet in Bahrain.[79] The Coast Guard has continuously conducted such military deployments to the US Central Command area of responsibility since 2002.[80]

Among its myriad functions, the Coast Guard also operates as a member of the IC.[81] In this role, the Coast Guard has the authority to "collect, analyze, produce, and disseminate foreign intelligence and counterintelligence" and to "conduct counterintelligence activities" at the direction of the Commandant.[82] Because Coast Guard Intelligence does not operate exclusively as an element of DoD, it is not beholden to many of the restrictions imposed upon the Defense Intelligence Enterprise.[83]

A key area where all the Coast Guard's roles and authorities intersect is in cyberspace. Complementing its traditional maritime role, the Coast Guard also operates Coast Guard Cyber Command both as the maritime sector lead for DHS and as a service cyber component of USCYBERCOM.[84] In its DHS role, Coast Guard Cyber Command serves to facilitate the cybersecurity of maritime ports and shipping and to respond to cyber events affecting the maritime sector.[85] For example, in August 2021, the Coast Guard assisted the Port of Houston in defending its network from a cyberattack by a nation-state actor using a zero-day vulnerability.[86] In its DoD role, Coast Guard Cyber Command is responsible for defending and operating the Coast Guard's portion of the DoD Information Network.[87] Though its current DoD mission is entirely defensive, the Coast Guard's first Combat Mission Team was established in the summer of 2021 to begin growing the service's offensive cyber capabilities.[88] While the Coast Guard's offensive cyber mission remains undefined, it could conceivably execute offensive operations as either a military operation under DoD or as a counterintelligence activity under DHS.

National Guard

Within DoD, there are seven reserve components. Each of the uniformed services, including the Coast Guard, has a reserve.[89] The Army and Air Force also have a National Guard component.[90] While the reserve components of the uniformed services operate exclusively under DoD, elements of the National Guard operate either under the operational control of the governors of individual states and territories or as elements of DoD in federal service when activated by the President.[91] Comprising over half of the total force strength of the reserve elements of the armed forces, the National Guard is a crucial component of both national defense and disaster response and recovery.[92]

There are three ways the National Guard may be activated: state active duty, federal activation, and Title 32 status. State active duty is governed by individual state and territorial laws by which governors can activate members of the National Guard at the governor's discretion.[93] Federal activation occurs in the form of either mobilization[94] or federalization of the National Guard as an organized militia.[95] Title 32 activation is directed by the federal government—and paid for by the federal government—but the command and control of National Guard personnel on Title 32 orders remain with the respective state governors.[96]

During emergencies, a state may use its own National Guard and may leverage the National Guard of other states through the Emergency Management Assistance Compact (EMAC).[97] Depending on the type of emergency, states can also leverage National Guard Civil Support to assist law enforcement.[98] However, the type of activation dictates the types of activities the National Guard can perform. For instance, when National Guard personnel are operating under state active duty or Title 32—either within their home state or in another state under EMAC—they are generally not governed by the Posse Comitatus Act and may perform law enforcement functions.[99] However, when National Guard personnel are activated under Title 10 and perform duties under the control of the President, though they can provide military support to civil authority, they are subject to the Posse Comitatus Act and may not perform law enforcement functions except in specific circumstances enumerated by statute.[100]

Despite the size and broad authorities of the National Guard operating under state authority, it has only been leveraged in limited scope to "prepare for, respond to, and recover from cybersecurity incidents that overwhelm state and local assets."[101] Congress has recognized a lack of standardization and efficient employment of the National Guard for responding to cyber events.[102] In the 2021 National Defense Authorization Act, Congress directed the Secretary of

Defense to evaluate the "statutes, rules, regulations and standards that pertain to the use of the National Guard for the response to and recovery from significant cyber incidents."[103] Congress went on to direct an update to the National Cyber Incident Response Plan to reflect improved employment of the National Guard.[104]

PART II. SUMMARY

Both the Coast Guard and the National Guard have unique characteristics that set each organization apart from traditional government and military entities. The Coast Guard leverages authorities under both DoD and DHS to perform its core functions for national security and homeland defense. Similarly, the National Guard provides both state governments and the federal government with a reserve force capable of executing emergency management and response actions at the state level as well as federal tasking as part of DoD. Because threats in cyberspace span military, law enforcement, homeland defense, and intelligence functional areas, as well as pose substantial risks to CI/KR that could result in significant state-level emergencies, the nation requires a cyber force capable of operating across all of these functional areas and in support of every level of government.

PART III. UNITED STATES CYBER FORCE

The US should establish a Cyber Force with an active component modeled on the Coast Guard and a reserve component modeled on the National Guard. The active component would serve as a sector-specific agency within DHS and "a military service and a branch of the armed forces of the US at all times."[105] The reserve component would be a third National Guard force and would operate alongside each of the 54 current National Guard organizations.

Within DHS, the Cyber Force would be the element responsible for managing DHS contributions in all dimensions of our cybersecurity. This would include defense of federal networks and CI/KR and operational control over the US Computer Emergency Response Team (US-CERT) and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). The Cyber Force would work closely with the Cybersecurity and Infrastructure Security Agency (CISA) in supporting private sector engagement, network monitoring, and threat-hunting activities.

The Cyber Force would be imbued with federal law enforcement authorities for the "prevention, detection, and suppression of violations of laws of the United States" in cyberspace similar to those of the Coast Guard in the maritime domain.[106] To limit a broad interpretation of this authority, the Cyber Force's law enforcement functions could be limited to those unlawful activities that target or affect the federal government or CI/KR networks. Among other law enforcement functions, the Cyber Force could use these authorities and the warrant process to mitigate cyber threats proactively.[107] Law enforcement authorities would also permit the Cyber Force to apply for and serve warrants and subpoenas to domestic entities wittingly or unwittingly used by malicious cyber actors to execute operations against the US. Finally, these authorities would allow the Cyber Force to integrate with and support other federal law enforcement agencies as well as state, local, tribal, and territorial law enforcement elements without violating the Posse Comitatus Act.

Like the Coast Guard, the Cyber Force would also be an individual member of the Intelligence Community. This would enable the training and development of cyber-specific intelligence and counterintelligence collectors, analysts, and operational personnel. The Cyber Force would have the authority to conduct counterintelligence activities, operations, and investigations in direct support of national cyber missions and requirements. As a member of the IC, the Cyber Force would also be able to conduct foreign intelligence liaison relationships and exchange programs with partners to improve the collective cyber defense posture of the US and its allies.

When operating as part of the DoD, the Cyber Force would serve as the force provider for the CNMF. In this role, the Cyber Force would man, train, and equip personnel to conduct full-spectrum cyberspace operations against malicious cyber actors. Under the operational control of USCYBERCOM, Cyber Force personnel would be able to execute offensive and defensive cyber operations targeting malicious cyber actors outside of the US. Rotational assignments would ensure that personnel supporting USCYBERCOM can benefit from the operational experience of performing sector-specific functions for DHS and vice versa. Additionally, mobilization of the Cyber National Guard to support USCYBERCOM and the CNMF would ensure operational experiences are continually shared between state defenders and the active component of DoD. Importantly, the establishment of a Cyber Force would not supplant the cyber components of the other military services. USCYBERCOM's service component commands would maintain their respective offensive and defensive missions in the same way as US Space Command's service component commands carry out appropriate missions despite the existence of the US Space Force.

As the reserve component of the Cyber Force, the Cyber National Guard would serve primarily as a digital militia for individual states and territories, while providing a ready pool of cyber professionals in the event of a national emergency. The establishment of a Cyber National Guard would standardize the training and equipping of a state-level cybersecurity response force. This stand-alone force could be leveraged by governors to respond, using state police powers, to significant cyber incidents affecting state and local governments, CI/KR, and private entities. A Cyber National Guard would also enable the individual states and the federal Cyber Force to tap into the significant talent pool across the private sector by allowing for part-time state and federal service without requiring those individuals to enlist or commission in the regular military.

CONCLUSION

In March 2021, the Government Accountability Office (GAO) found that the federal government "needs to urgently pursue critical actions to address major cybersecurity challenges."[108]

The GAO recommended the federal government establish a comprehensive cybersecurity strategy and perform effective oversight.[109] The segmentation of authorities and capabilities across the federal government makes this difficult if not infeasible. Overcoming this challenge requires establishing a Cyber Force and Cyber National Guard able to leverage the requisite authorities of both the individual states and the federal government and provide a comprehensive array of capabilities to support achievement of the nation's cybersecurity objectives.

DISCLAIMER

The views and opinions expressed in this article are those of the author alone and do not reflect the official policy or position of the Department of Defense (DoD), U.S. Cyber Command, or any agency of the U.S. Government. Any appearance of DoD visual information or reference to its entities herein does not imply or constitute DoD endorsement of this authored work, means of delivery, publication, transmission, or broadcast.

NOTES

1. Arthur W. Tedder, *Air Power in War,* The University of Alabama Press (2010), 87-124.
2. Ibid., 29.
3. Ibid.
4. Alexander P. de Seversky, *Victory Through Air Power*, Simon & Schuster, Inc. (1942), 254.
5. Pub.L. 80-253, 61 Stat. 495, enacted July 26, 1947.
6. de Seversky, *Victory Through Air Power*, 254.
7. The White House, *National Cyber Strategy of the United States of America* (2018) ("America's prosperity and security depend on how we respond to the opportunities and challenges in cyberspace."), 1.
8. Department of Defense Memorandum, "Directing USSTRATCOM's Establishment of a Subordinate Unified Command for Cyber Operations," June 23, 2009, https://nsarchive.gwu.edu/news/cyber-vault/2020-05-11/uscybercom-documents-timeline (accessed October 6, 2021) (Though "the military departments have identified the following organizations to serve as components to USCYBERCOM. . . . (1) ARFORCYBER [Army Cyber Command][,] (2) FLTCYBERCOM [Navy Fleet Cyber Command][;] (3) MARFORCYBER [Marine Forces Cyber Command]; (4) AFCYBER [Air Force Cyber Command]," each military service maintains its own cyber forces.).
9. Daniel, Michael, "Why Is Cybersecurity So Hard?" *Harvard Business Review* (May 22, 2017), https://hbr.org/2017/05/why-is-cybersecurity-so-hard (accessed Oct. 1, 2021) ("[O]ur physical-world mental models simply won't work in cyberspace. For example, in the physical world, we assign the federal government the task of border security. But given the physics of cyberspace, everyone's network is at the border. If everyone lives and works right on the border, how can we assign border security solely to the federal government?").
10. See *United States v. Yuriy Sergeyevich Andrienko, et al.*, No. 20-316 (WDPA) (On October 15, 2020, a grand jury in the Western District of Pennsylvania returned an indictment against six Russian intelligence officers. These officers, members of GRU Military Unit 74455 – more commonly referred to as "Sandworm," were charged with executing a pervasive and continuous destructive malware campaign against nations worldwide since at least 2015.)
11. The White House, "Presidential Policy Directive 41," (July 7, 2016) [hereafter "PPD-41"] (Federal lead agencies for coordinating responses to significant cyber incidents include the Federal Bureau of Investigation and the National Cyber Investigative Joint Task Force for threat response activities, the Department of Homeland Security for asset response activities, and the Office of the Director of National Intelligence for intelligence support.).
12. U.S.C. Title 6. DOMESTIC SECURITY governs the Department of Homeland Security and the Cybersecurity and Infrastructure Security Agency; U.S.C. Title 10. ARMED FORCES governs the military; U.S.C. Title 14. COAST GUARD governs the activities of the U.S. Coast Guard; U.S.C. Title 18. CRIMES AND CRIMINAL PROCEDURE governs law enforcement; U.S.C. Title 32. NATIONAL GUARD governs the functions of the National Guard Bureau; U.S.C. Title 50 WAR AND NATIONAL DEFENSE governs the activities of the U.S. Intelligence Community.
13. See 10 U.S.C. §§ 5013 (authorizes the Secretary of the Navy to control and supervise intelligence activities of the Department of the Navy); see 10 U.S.C. § 7480 (authorizes the Secretary of the Navy to permit NCIS special agents to execute federal arrest warrants); see also 50 U.S.C. §3038 (authorizes the Department of the Navy to collect and produce intelligence).
14. See 10 U.S.C. § 164(c); see also 10 U.S.C. § 167(b)(d).
15. Pub.L. 116-92—December 20, 2019. § 1631 (c); see 10 U.S.C. § 394 (c); see also 50 U.S.C. 3093 (e)(2).
16. U.S. Cyber Command, "Our History," https://www.cybercom.mil/About/History/ (accessed November 6, 2021).
17. See Department of Defense, Joint Publication 3-12, *Cyberspace Operations,* June 8, 2018 [hereafter JP 3-12], 1-4.
18. U.S. Cyber Command Public Affairs, "Cyber Mission Force achieves Full Operational Capability" (May 17, 2018), https://www.cybercom.mil/Media/News/News-Display/Article/1524492/cyber-mission-force-achieves-full-operational-capability/ (accessed November 6, 2021).
19. U.S. Army Cyber Command, "About Us" (June 2020), https://www.arcyber.army.mil/Organization/About-Army-Cyber (accessed October 7, 2021).
20. COL Craft, Paul, "JFHQ-DODIN: Fight the DODIN" (May 2019), https://disa.mil/-/media/Files/DISA/News/Events/Symposium-2019/1---COL-Craft_Fight-the-DODIN_approved-Final.ashx (accessed October 7, 2021).
21. Joint Staff Approval of U.S. Cyber Command Concept for Organization (2012).
22. JP 3-12, I-9.

NOTES

23. See JP 3-12, II-8 to II-9.

24. See The White House, "The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China," Statements and Releases (July 19, 2021) ("As detailed in public charging documents unsealed in October 2018 and July and September 2020, hackers with a history of working for the [People's Republic of China] Ministry of State Security (MSS) have engaged in ransomware attacks, cyber enabled extortion, crypto-jacking, and rank theft from victims around the world, all for financial gain.").

25. See Executive Order 12333, *United States Intelligence Activities* (as amended by Executive Orders 13284 (2003), 13355 (2004), and 13470 (2008)) § 3.5(a), *Federal Register,* Vol. 40, No. 235 (December 8, 1981), [hereafter EO 12333] ("Counterintelligence means information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities."

26. Pub. L. 116-92—December 20, 2019. § 1631 (c); see 10 U.S.C. § 394 (c); see also 50 U.S.C. 3093 (e)(2).

27. Sen. Rpt. 102-85, at 46 (1991) ("'[T]raditional military activities' include activities by military personnel under the direction and control of a United States military commander (whether or not the U.S. sponsorship of such activities is apparent or later to be acknowledged) preceding hostilities which are anticipated (meaning approval has been given by the National Command Authorities for the activities and for operational planning for hostilities) involving U.S. military forces, or where such hostilities are ongoing, where the fact of the U.S. role in the overall operation is apparent or to be acknowledged publicly.").

28. See DoD Instruction S-5240.17, "(U) Counterintelligence Collection Activities (CCA)," March 14, 2014 (MDCOs conduct consent-based monitoring of select domestic private sector networks under Military Department counterintelligence authorities. Because Commander, U.S. Cyber Command, has not been delegated full-spectrum counterintelligence authorities by the Secretary of Defense, counterintelligence agents assigned to the Cyber Mission Force are not authorized to conduct similar network monitoring.).

29. See Cyber Crime Investigator, *Defense Cyber Workforce Framework*, https://public.cyber.mil/dcwf-work-role/cyber-crime-investigator/ (accessed November 27, 2020); see also EO 12333.

30. EO 12333 § 1.12.

31. See, generally, United States v. Li Xiaoyu (a/k/a "Oro0lxy") and Dong Jiaxhi, No. 4:20-CR-6019-SMJ (E.D. Wash. July 7, 2020); see DoDD 5240.02 (DoD policy outlining the conduct of CI); see 18 U.S.C. § 2511(2)(c) (Exception to the Wiretap Act: "It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception. . . ."); see also DoD Manual 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities,* at para. 3.2 Procedure 2: Collection of USPI, August 8, 2016 (DoD policy governing exceptions to the collection of United States Person information, including with valid consent and for the purposes of counterintelligence); see also EO 12333 § 1.11(d) ("CI activities outside the U.S. are conducted in coordination with the Central Intelligence Agency (CIA)[, and] MDCO CI activities inside the U.S. are conducted in coordination with the Federal Bureau of Investigation (FBI).").

32. See 10 U.S.C. §167b; see also 10 U.S.C. §395.

33. Pub. L. 113-283 (Federal Information Security Modernization Act of 2014).

34. Pub. L. 107-296 (Homeland Security Act of 2002); Pub. L. 113-282 (National Cybersecurity Protection Act of 2014); Pub. L. 114-113 (Cybersecurity Act of 2015); Pub. L. 115-278 (Cybersecurity and Infrastructure Security Agency Act of 2018).

35. The White House, Presidential Policy Directive 21 (February 12, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil/ (accessed November 7, 2021) [hereafter "PPD-21"], ("The Secretary of Homeland Security shall provide strategic guidance, promote a national unity of effort, and coordinate the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure." Critical infrastructure sectors include: Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government Facilities; Healthcare and Public Health; Information Technology; Nuclear Reactors, Materials, and Waste; Transportation Systems; and Water and Wastewater Systems.).

36. 46 U.S.C. §70116.

NOTES

37. 18 U.S.C. §3056.
38. 49 U.S.C. §114; see Transportation Security Administration, “DHS announces new cybersecurity requirements for critical pipeline owners and operators” (July 20, 2021), https://www.tsa.gov/news/press/releases/2021/07/20/dhs-announces-new-cybersecurity-requirements-critical-pipeline (accessed November 7, 2021).
39. Department of Homeland Security, “National Response Framework” (4th Ed., October 28, 2019).
40. Pub. L. 115-278.
41. PPD-41, supra note 11.
42. Ibid.
43. Ibid.
44. Ibid.
45. Ibid
46. Ibid.
47. Ibid.
48. Department of Homeland Security, “Cyber Incident Reporting: A Unified Message for Reporting to the Federal Government,” https://www.dhs.gov/sites/default/files/publications/Cyber%20Incident%20Reporting%20United%20Message.pdf (accessed November 9, 2021).
49. PPD-41, supra note 11 (“Threat response activities include conducting appropriate law enforcement and national security investigative activity at the affected entity’s site; collecting evidence and gathering intelligence; providing attribution; linking related incidents; identifying additional affected entities; identifying threat pursuit and disruption opportunities; developing and executing courses of action to mitigate the immediate threat; and facilitating information sharing and operational coordination with asset response.”
50. See PPD-41, supra note 11; see also Department of Homeland Security, “Cyber Incident Reporting: A Unified Message for Reporting to the Federal Government,” https://www.dhs.gov/sites/default/files/publications/Cyber%20Incident%20Reporting%20United%20Message.pdf (accessed November 9, 2021).
51. PPD-41, supra note 11 (“Asset response activities include furnishing technical assistance to affected entities to protect their assets, mitigate vulnerabilities, and reduce impacts of cyber incidents; identifying other entities that may be at risk and assessing their risk to the same or similar vulnerabilities; assessing potential risks to the sector or region, including potential cascading effects, and developing courses of action to mitigate these risks; facilitating information sharing and operational coordination with threat response; and providing guidance on how best to utilize Federal resources and capabilities in a timely, effective manner to speed recovery.”).
52. Ibid.
53. Ibid., “Intelligence support and related activities facilitate the building of situational threat awareness and sharing of related intelligence; the integrated analysis of threat trends and events; the identification of knowledge gaps; and the ability to degrade or mitigate adversary threat capabilities.”.
54. Ibid.
55. Pub.L. 114-113, “Division N—Cybersecurity Act of 2015, Title I—Cybersecurity Information Sharing,” December 18, 2015; 6 U.S.C. § 1502.
56. DODIG-2019-016.
57. Ibid., 11, citing “Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government Under the Cybersecurity Information Sharing Act of 2015," February 16, 2016.
58. DODIG-2019-016 at 5.
59. Office of the Director of National Intelligence, *Members of the IC* (https://www.dni.gov/index.php/what-we-do/members-of-the-ic) (accessed October 25, 2021).
60. Rpt. to Accompany S. Rpt. 116-4049 (2020), Sec. 1639 at 463, https://www.armed-services.senate.gov/imo/media/doc/FY%202021%20NDAA%20-%20Report.pdf.
61. *United States v. McArthur,* 419 F. Supp. 186 (D.N.D. 1976); see 18 U.S.C. 1385.
62. EO 12333.
63. 18 U.S.C. § 2511(2)(c).

NOTES

64. See U.S. Government Accountability Office, *Cybersecurity: DHS and Selected Agencies Need to Address Shortcomings in Implementation of Network Monitoring Program*, GAO-20-598 (August 18, 2020); see also United States National Security Strategy, 23 (2017); see also The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, 18 (2009) (which, in 2009, noted: "government and private-sector personnel, time, and resources are spread across a host of bodies engaged in sometimes duplicative or inconsistent efforts. Partnerships must evolve to clearly define the nature of the relationship [and] the roles and responsibilities of various groups and their participants").
65. LtCol Kurt Sanger and CDR Peter Pascucci, "Revisiting a Framework on Military Takedowns Against Cybercriminals," Lawfare (July 2, 2021) (https://www.lawfareblog.com/revisiting-framework-military-takedowns-against-cybercriminals).
66. PPD-41, supra note 11; see The White House, "FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government," (April 15, 2021) (The United States has formally named the Russian Foreign Intelligence Service (SVR) "as the perpetrator of the broad-scope cyber espionage campaign that exploited the SolarWinds Orion platform and other information technology infrastructures. . . . The scope of this compromise is a national security and public safety concern.").
67. 14 U.S.C. §101.
68. Pub. L. 107-296.
69. 6 U.S.C. §468(a)(1).
70. 33 U.S.C. §1223.
71. 14 U.S.C. §91.
72. 46 U.S.C. §3306.
73. 14 U.S.C. §141.
74. 14 U.S.C. §89.
75. Ibid.
76. 50 U.S.C. §191.
77. 14 U.S.C. §101.
78. 14 U.S.C. §103.
79. United States Coast Guard New Release, "U.S. Coast Guard ships depart Puerto Rico on mission to strengthen Trans-Atlantic ties" (April 2, 2021), https://content.govdelivery.com/accounts/USDHSCG/bulletins/2cb0645 (accessed October 20, 2021).
80. Ibid.
81. Pub.L. 80-253 (amended December 28, 2001).
82. EO 12333.
83. See, for example, Department of Defense Instruction 5240.04, *Counterintelligence Investigations* (Feb. 2, 2009 (*Incorporating Change 1, Effective October 15, 2013*) (Within the Department of Defense, only Military Department Counterintelligence Organizations (Army Military Intelligence, Naval Criminal Investigative Service, and Department of the Air Force Office of Special Investigations) are authorized to conduct counterintelligence investigations. No other DoD counterintelligence elements, including the Defense Intelligence Agency, the Combatant Commands, or other military organizations have this authority. However, because the Coast Guard derives its counterintelligence authorities directly from the President in EO 12333, the Commandant may define the personnel, methods, and means by which it conducts counterintelligence investigations when not operating under the Department of Defense.).
84. U.S. Guard Cyber Command, "Commander's Strategic Direction 2021," (August 2021), https://www.uscg.mil/Portals/0/Images/cyber/2021-Cyber-Strategic-Outlook.pdf (accessed September 21, 2021).
85. 46 U.S.C. §70116.
86. Sean Lyngaas, "Hackers breached computer network at key US port but did not disrupt operations," CNN.com (September 23, 2021), https://www.cnn.com/2021/09/23/politics/suspected-foreign-hack-houston/index.html (accessed October 1, 2021).
87. U.S. Guard Cyber Command, "Commander's Strategic Direction 2021," August 2021, https://www.uscg.mil/Portals/0/Images/cyber/2021-Cyber-Strategic-Outlook.pdf (accessed September 21, 2021), 7.

NOTES

88. Kimberly Underwood, "Coast Guard Embarks on Cyber Offense," *SIGNAL* (October 1, 2021), https://www.afcea.org/content/coast-guard-embarks-cyber-offense (accessed October 5, 2021).
89. 10 U.S.C. §1003.
90. Ibid.
91. 32 U.S.C. §104.
92. Defense Manpower and Data Center, "Selected Reserve Personnel by Reserve Component and Rank/Grade (Updated Monthly): September 2021," DoD Personnel, Workforce Reports & Publications, https://dwp.dmdc.osd.mil/dwp/app/dod-data-reports/workforce-reports (accessed November 5, 2021) (as of September 2021, the combined strength of the Army National Guard and Air National Guard was 446,008 personnel.).
93. See, for example, Md. Public Safety Code Ann. §13 (2020).
94. See 10 U.S.C. §12301(a) (Full mobilization); 10 U.S.C. §12302(a) (Partial mobilization); see also 10 U.S.C. §12304 (Active Duty other than War or National Emergency).
95. See 10 U.S.C. §12406 (Federal activation to repel an invasion, suppress a rebellion, or execute laws of the United States); (10 U.S.C. §251 (Federal activation of the militia of one state to quell insurrection in another); see also 10 U.S.C. §252 (Federal activation to enforce federal law in the event of an insurrection).
96. 32 U.S.C. §502(f).
97. Pub. L. 104-321.
98. Chief National Guard Bureau Instruction 3000.04, *National Guard Bureau Domestic Operations*, January 24, 2018 ("National Guard Civil Support -- Support provided by the National Guard while in a State Active Duty status or Title 32 status to civil authorities for domestic emergencies, designated law enforcement, and other activities.").
99. See, e.g., Md. Public Safety Code Ann. §13-402 (2020).
100. See 18 U.S.C. 1385; but see 10 U.S.C. §12406.
101. Cyberspace Solarium Commission ("Examples of states relying on National Guard units to deal with cybersecurity incidents include Colorado, Louisiana, and Texas, where the governors declared state of emergencies to activate their National Guard."), 65.
102. Pub. L. 116-283 § 1729.
103. Ibid.
104. Ibid.
105. 14 U.S.C. §101.
106. See 14 U.S.C. §89.
107. Fed. Rules of Crim. Pro. 41(6)(b)(6); see April Falcon Doss, "We're From the Government, We're Here to Help: The FBI and the Microsoft Exchange Hack," JustSecurity.org (April 16, 2021), https://www.justsecurity.org/75782/were-from-the-government-were-here-to-help-the-fbi-and-the-microsoft-exchange-hack/ (accessed April 16, 2021). (The FBI used this authority to remove malware from networks affected by the Microsoft Exchange Server vulnerability exploited by the Hafnium – malicious cyber actors associated with the Chinese government.).
108. U.S. Gov't Accountability Off., GAO-21-288, *HIGH-RISK SERIES: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges* (March 2021), https://www.gao.gov/assets/gao-21-288.pdf ("To address this challenge, federal agencies need to take the following four actions: (1) develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace, (2) mitigate global supply chain risks, (3) address cybersecurity workforce management challenges, and (4) ensure the security of emerging technologies.").
109. Ibid.

Everything Flows: Russian Information Warfare Forms and Tactics

in Ukraine and the US Between 2014 and 2020

Samantha Mullaney

ABSTRACT

This case study builds on previous analyses of Russian information warfare and covers the forms and tactics in simultaneous campaigns in Ukraine and the US between 2014 and 2020, using Daniel P. Bagge's DOPES methodology to discern and analyze patterns within events data from the two campaigns. Use of DOPES illustrates that Russian information warfare possesses discernible forms and tactics across varying contextual situations and is highly flexible. The forms and tactics align with Russian information warfare (IW) doctrine and the goals of reflexive control. The case study concludes with a discussion of strategic and policy level recommendations to counter the effects of Russian IW.

INTRODUCTION

Russian IW includes the doctrine Russia uses to achieve specific aims, whether strategic, operational, or tactical, and Russia's methods; it encompasses both principles and procedures.[1] One of the main challenges for western scholars and practitioners in identifying Russia's IW abilities and effectiveness is finding evidence or data of outcomes. Some scholars conclude that the effects are minuscule.[2] However, looking at Russian IW by searching for evidence of outcomes paints a deceptive picture and can lead scholars to draw skewed conclusions.

This research builds on previous research and analysis of Russian strategic use of IW, especially regarding new-type warfare means and the forms and methods of fighting, as suggested by Timothy Thomas.[3] It also seeks to identify Russia's use of multiple elements

Samantha Mullaney, a graduate of Augusta University's Masters in Intelligence and Security Studies Program in Augusta, Georgia, focuses her research on information warfare forms, tactics, and implications. Her capstone included completing an information warfare internship at the Georgia Cyber Center, where she researched Russian information warfare forms and tactics in Ukraine and the US. Samantha has a BA in History from Fairfield University, an MA in Elementary Education from Boston University, and spent nearly a decade teaching in Djibouti, Yemen, Jordan, and the UAE. She speaks intermediate Arabic and basic German. samantha.mullaney@protonmail.com

of IW in simultaneous campaigns.[4] Finally, as Costello explains, the US must identify, understand, and evaluate Russia's tools in the Initial Phase of War (IPW) and IW campaigns.[5] Many scholars have chronicled Russia's IW in Ukraine and the US between 2014 and 2020 as separate studies, but few have attempted to categorize the known events in a manner that would identify common forms or tactics.

This paper's six sections cover first the doctrinal evolution of Russian IW and its use of reflexive control as the primary theoretical paradigm underpinning IW. Second, Bagge's methodology of events categorization is explained. Third, the paper lays out the events' categorization results by form, tactic, target and vulnerability. Fourth, the results are discussed. Fifth, the paper addresses how Bagge's methodology should be used in future research. Last, the paper identifies policy areas applicable to the results and how the US can combat the forms and tactics of Russian IW.

BACKGROUND

Information is a foundational weapon in the pursuit of geostrategic goals. Russia's primary goals include destabilizing the geopolitical balance and reasserting its sphere of influence through information superiority.[6] To do this, Russia views warfare more broadly than the US and sees a state's population as a means to attain its goals.[7] Moreover, as will become apparent through the discussion of reflexive control, Russia views knowing its adversary as the enabling mechanism for successful IW.

Russian IW Doctrine and Reflexive Control

IW is central to achieving Russia's strategic goals. The framing concept Russia uses to implement and achieve IW is reflexive control (RC), a theory that has evolved over a century. The concept of RC can be subdivided into two sections.[8] The first is the reflexive system, and the latter is the reflexive process.

The reflexive system includes the target and any other participant in the system, including the observer and target, and each of their mental constructs. Each person in the system has a mental construct of the system and how each other person views the system. When adversaries meet, Lefebvre posits that the outcome will be "determined by the way the adversaries represent each other's mental world."[9] Essentially, he who best understands the adversary's mental world can interpret decisions most correctly, thereby giving them the advantage. This is the reflexive process.

An often-overlooked element of reflexive control is that it is a means to accomplish other outcomes and is an end goal in and of itself. For example, an actor uses reflexive control to gather information about an adversary that can be used in other ways, but control over the decision-making process is also the goal.

New Russian use of reflexive control can debatably be identified as the creation of an operator of awareness. This is when the actor does not have a specific goal but where the influence projected onto the adversary narrows the possible decisions, enabling the actor to reasonably predict decisions.[10] Current RC utilizes psychological effects on decision-makers, communicates false or partially false information, coerces the enemy to envision defeat, and uses the enemy's resources against it.[11] In addition, the use of cyberspace has allowed the theory to implement methods of access to the masses.[12]

For example, a Russian Ministry of Defense document defines IW as conflict in the information space that seeks to force “a state to make decisions in the interests of their opponents” by undermining political, information, social, or economic systems, as well as implementing “mass psychological campaigns against the population of a State in order to destabilize society and the government.”[13] Other published doctrine similarly espouses utilizing psychological or ideological information to “undermine trust in the government...[and] lead to the destabilization of the situation.”[14]

For simplicity, in this case study reflexive control is defined as the ability to influence the adversary to make the decisions you want him to make by influencing, transforming, and ultimately undermining the decision-making system.[15] In essence, reflexive control is effective marketing on steroids and directed for statecraft instead of commerce and control rather than management. Most importantly, the practice of reflexive control creates small actions that seem trivial to the target but have massive and complex intentions.[16]

Modern Russian IW Doctrine

Modern Russian IW is distinguished from western definitions of the concept by multiple factors. First, there is no differentiation between peacetime and war or civilian and military spheres. This is a point of issue for democracies. Next, unlike recent doctrine in the US, Russia does not view IW through cyber-colored glasses.[17] Cyber elements are a tool used in Russian IW, and therefore there is no distinction between cyber and information spheres.[18] The only distinction made in the Russian concept of IW is between code-based and content-based methods, or what some authors have termed information-psychological and information-technology methods.[19] Also, Russian IW is long-term. IW seeks to decay "the moral values, psychological state or even the decision maker's character" to alter the perception of information.[20]

Last, IW is not meant to be kinetic in the traditional, western conception of kinetic warfare. Russian General Valery Gerasimov, perhaps the easiest figurehead for Westerners to associate with Russian IW, explains that nonmilitary means could have higher success rates than kinetic means in achieving objectives, and psychological measures have become the norm.[21] The fact that some US scholars have attempted to view IW success through the lens of whether it impacts kinetic action is essentially a product of mirror-imaging and inhibits an accurate understanding of the purpose and methodology of Russian IW.

All forms of information become a legitimate target for Russia, regardless of the state of war. While individual Russian attempts at IW may seem ineffective, Giles explains that "credibility is not always a metric of success for Russian information warfare campaigns."[22] The goal is to eliminate objective truth, inhibit the ability to report on a situation, destabilize the society, weaken morals and confidence, and destroy empirical knowledge.[23] Destabilization can lead to pressure on government officials and citizens to accept a solution that they would not have under their own volition, closing the loop of the reflexive control process.[24]

Indirect actions taken under the umbrella of IW intend to influence the enemy across a broad range of sectors by distributing disinformation to destroy the enemy from within.[25] Included in the means of achieving this is the protest potential of a population and other measures that have the possibility of demoralizing the public.[26] The long-term nature of effective IW campaigns creates persistent narratives that end up causing members of the target society to question themselves.[27] Moreover, the IW methodology can achieve a wide range of strategic objectives through the use of reflexive control.[28] For Russia, IW is the starting point of the new type of warfare; it determines whether and which future actions should be taken.[29]

METHODOLOGY

This research uses Daniel P. Bagge's DOPES method to categorize events and correlate them with known patterns, which in turn relies on S.A. Komov's intellectual elements of IW.[30] It is important to note that Russia's IW is flexible depending upon the environment. The following categories are often used simultaneously, offensively, and in a long-term manner against an adversary to discredit, defame and divide the state through polemics.[31]

Events were collected through open-source information from government indictments and reports, think-tank publications, declassified military reports and publications, independent organizations' research and analysis, investigative journalism, and news reporting. The events were input to an Excel sheet and then categorized by form, tactic, target audience, vulnerability, and source citation. Following categorization of the events data, processes of IW were compared by stage of war.

The Ukraine events data is divided into three stages, a broad consolidation of Gerasimov's six stages of warfare: pre-Crimean invasion, post-Crimean invasion but pre-Eastern Ukraine invasion, and post-Eastern Ukraine invasion. These were three clear-cut transitions within the war and corresponded to the use of paramilitary forces. The US events data were divided into two phases, as three separate phases were unable to be identified and paramilitary forces were not used. The two stages are pre-and post-2016 election. The Russian IW campaign is ongoing in the US, as is clear from the findings below.

RESULTS

Ukraine

Table 1

Form Pre-Crimean Invasion	Form Post-Crimea, Pre-Eastern Ukraine	Form Post-Eastern Ukraine Invasion
Pressure	Pressure	Pressure
Distraction	Suggestion	Distraction
Division	Distraction	Deception

Table 1 shows that pressure is the constant form of IW Russians deployed in Ukraine, throughout all stages of war. Distraction made up nearly half of the forms implemented during the IPW, or pre-Crimean invasion, with division also highly utilized. The forms changed once Russia invaded Crimea, with suggestion being used in 65 percent of the events. Division increased, but far less than distraction and suggestion. Post-invasion of Eastern Ukraine, distraction regained its usefulness, and deception became more common. Figure 1 illustrates the growth of deception, distraction and pressure throughout the campaign while Table 2 highlights the percentage change of form over time.

Table 2

Form	Pre-Crimean Invasion Percentage	Post-Crimea, Pre-Eastern Ukraine Percentage	Post-Eastern Ukraine Percentage
Deception	25%	45%	61%
Deterrence	21%	42%	19%
Distraction	46%	52%	64%
Division	42%	45%	27%
Overload	4%	30%	25%
Pacification	21%	43%	20%
Paralysis	38%	41%	18%
Pressure	67%	71%	77%
Provocation	38%	25%	8%
Exhaustion	13%	47%	35%
Suggestion	38%	65%	54%

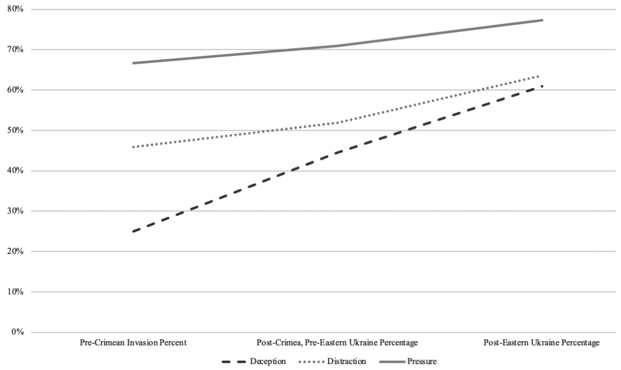


Figure 1. Forms in Information Warfare that Increase as War Progresses

Table 3

Tactic Pre-Crimean Invasion	Tactic Post-Crimea, Pre-Eastern Ukraine	Tactic Post-Eastern Ukraine Invasion
Political Action	Consolidation of control	Disinformation
Code-based	Code-based	Amplification
Disinformation	Cover	Code-based
Economic Manipulation	Electronic Warfare	Cross-legitimization

Table 3 shows that code-based tactics were used throughout the war, while people of influence were used more heavily at the beginning (13 percent) and middle phases (14 percent) rather than the end phase (10 percent). That said, disinformation through co-opted media and civil society outlets comprised the most common tactic in the final stage. Four out of the six tactics used in the IPW are not highly utilized in the middle phase, including political action, disinformation, and economic manipulation. Amplification and cross-legitimization became important toward the war's end. Figure 2 illustrates changes in use of tactics.

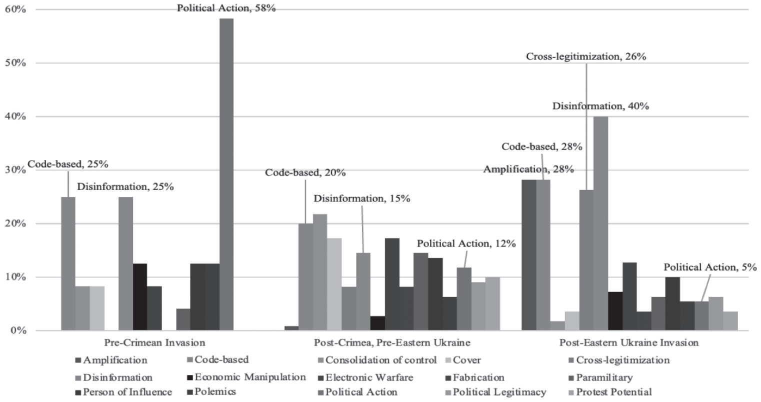


Figure 2. Tactic Used Over Time

Table 4

Target Pre-Invasion Crimea	Target Post-Crimea, Pre-Invasion of Eastern Ukraine	Target Post-Invasion of Eastern Ukraine
Russian domestic audience	Russian domestic audience	Russian domestic audience
Ukraine general population	Ukrainian government	Ukrainian general population
Ukrainian government	Ukrainian general population	Ukrainian government
NATO	NATO	NATO

Table 4 confirms that the Russian domestic audience remained the most important target throughout the war. Between the invasion of Crimea and the invasion of Eastern Ukraine, particular emphasis was placed on targeting the Ukrainian government (see Figure 3). NATO was a top target, but still significantly less targeted than the Russian or Ukrainian population.

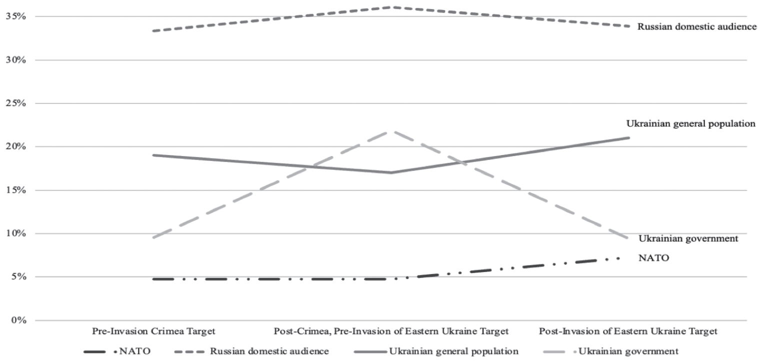


Figure 3. Target by Phase of War

Vulnerability Pre-Crimean Invasion	Vulnerability Post-Crimea, Pre-Eastern Ukraine	Vulnerability Post-Eastern Ukraine Invasion
Government Legitimacy	Government Legitimacy	Russia's Narratives to Citizens
Economic Dependence	Russia's Narratives to Citizens	Government Legitimacy
Reputation of US	Command and Control	Russian Legitimacy for Intervention

Table 5

Russia's IW largely targeted Ukrainian government legitimacy throughout all phases of the war, with post-Eastern Ukraine seeing a rise in Russia's emphasis on its domestic narratives, as noted in Table 5. Ukraine's economic dependence was exploited in the IPW, as was the US's reputation. As Russia consolidated control throughout the war, it targeted vulnerabilities within its society and sought to legitimize the war.

United States

Table 6

Form Pre-Election	Form Post-Election
Pressure	Pressure
Suggestion	Suggestion
Division	Division

Table 7

Form	Pre-Election Percentage	Post-Election Percentage	Change
Pressure	23%	20%	-3%
Suggestion	16%	19%	3%
Division	13%	17%	5%
Deception	11%	12%	1%
Overload	9%	9%	0%
Exhaustion	9%	10%	1%
Distraction	8%	1%	-7%
Paralysis	6%	5%	-1%
Deterrence	2%	0%	-2%
Provocation	2%	7%	5%
Pacification	1%	0%	-1%

The ongoing nature of Russia's IW campaign on the US created just two phases of warfare. Table 6 lays out the lack of change in IW form, and Table 7 shows some nuance between phases. Pressure made up 23 percent of the form for all events pre-2016 election, with suggestion at 16 percent and division at 13 percent, as shown in Table 7. These percentages changed slightly, post-election, with pressure at 20 percent, suggestion at 19 percent, and division at 17 percent. The largest change between forms by stage of the IW campaign was evidenced in the increased use of provocation post-2016 election, which increased from two to seven percent. Division saw a similar increase. Distraction fell from eight percent to one percent post-2016 election.

Tactics before and after the 2016 election differed, as Table 8 and Figure 4 confirm. While the primary tactic used was code-based, use of polemics and amplification grew the most, by five and seven percent, respectively. Conversely, leaks were less utilized post-2016 election, shrinking by nine percent. Table 9 compiles the change in tactic between the phases of the IW campaign.

Table 8

Tactic Pre-Election	Tactic Post Election
Code-based	Code-based
Political Legitimacy	Polemics
Leak	Amplification
Political Action	Political Legitimacy

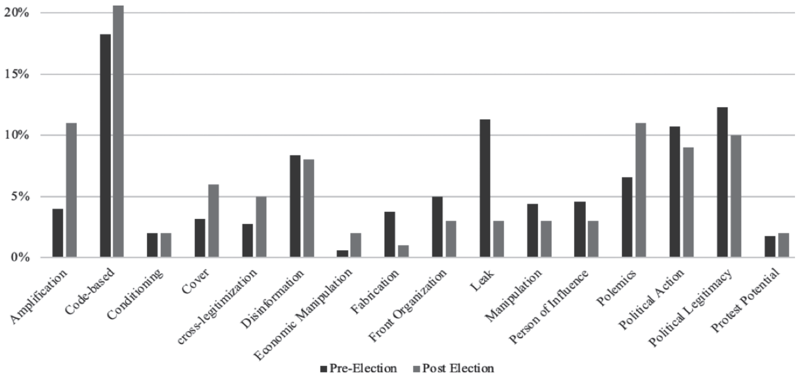


Figure4. Tactic Used Over Time

Table 9

Tactic	Change
Amplification	7%
Polemics	4%
Cover	3%
Code-based	3%
Cross-legitimization	2%
Economic Manipulation	1%
Manipulation	-1%
Person of Influence	-2%
Political Action	-2%
Front Organization	-2%
Political Legitimacy	-2%
Fabrication	-3%
Leak	-8%

Table 10

Target Pre-Election	Target Post-Election
US Public	US Public
US Policy Elites	Civil Society
Media	Media
Russian Domestic Audience	US Policy Elites

Table 11

Vulnerability Pre-Election	Vulnerability Post-Election
US Elites	Civil Society
Media	Media
Civil Society	US Reputation
US Reputation	US Elites

Table 12

Vulnerability	Pre-Election Percentage	Post-Election Percentage
US Elites	29%	13%
Media	18%	22%
Civil Society	18%	26%
US Reputation	17%	19%

The consistent IW target was the US public, holding 34 percent and 19 percent of the share of events before and after the election, respectively, as illustrated in Table 10. Although US policy elites were heavily targeted pre-2016 election with 24 percent of all events directed at them, this decreased to 11 percent post-election as the campaign moved toward targeting the media and civil society, which grew five and ten percent, respectively.

Russian IW saw vulnerabilities within US elites, the media, the US's reputation, and civil society throughout the IW campaign. Table 11 shows that the vulnerabilities did not change, but there was a different hierarchy of priorities in each stage. US elites were seen as less vulnerable following the election and were replaced by the media. Civil society was the most vulnerable part of American society post-2016 election, with 26 percent of all events directed toward it.

DISCUSSION

Use of Bagge's DOPES Methodology

This case study clearly shows that Bagge's DOPES analysis usefully delineates Russian IW forms and tactics. Indeed, DOPES analysis is perhaps the first of its kind to characterize Russian IW forms and tactics, and future scholars will find it useful for known Russian information interference, in categorizing events by form and tactic to discern patterns and emphases of Russian IW campaigns. The benefits of DOPES is clear. First, the forms and tactics Russia employs reveal a picture of how Russia views the reflexive system, and can be used in an offensive counterintelligence manner. Second, knowing the forms and tactics enables resources to be adequately distributed. Finally, the analyst is better informed to recommend measures to inhibit or mitigate Russian IW attempts.

DOPES delineates the evolving nature of Russia's forms of IW throughout the Ukrainian conflict, and reveals the flexibility of the Russian IW doctrine. Russia was interested in preventing Ukraine from joining NATO and the EU, sought control over Ukrainian policy, and needed Ukraine for domestic ideological purposes.[32] As each stage of warfare unfolded, Russia could assess whether and how those goals could be met by the context on the ground and was flexible in the tactics and forms used to achieve the goals.[33]

While categorizing helps practitioners, the data itself will enable a fine-tuned understanding of Russian IW. The events data for this case study were compiled over a short period and are not exhaustive. Future research should apply DOPES to larger events data sets that have multiple researchers cross-categorizing events. Finally, DOPES should be strengthened by incorporating other analytical processes such as Hammond-Errey's information influence and interference framework, thereby adding considerable depth to conclusions from events data.[34]

Ukraine

The effectiveness of Russia's IW campaign in Ukraine revolves around its understanding of Ukraine's reflexive system. Pressure, which DOPES defines as disseminating information that delegitimizes or destabilizes the government, is the main form of IW in Ukraine throughout all stages of warfare. The Ukrainian government has a reputation for corruption, incompetence, and general lack of ability and is one of the weakest links in the decision-making network within Ukraine. By heightening these exploitable elements within Ukraine through political action, disinformation through the media, and economic manipulation to decrease support for the government, Russia effectively pressured the Ukrainian government and outside elements into delayed reaction. Ukraine's will to resist diminished over time because Russia effectively targeted communication infrastructure and people of influence within the media and politics.[35]

Post-invasion of Crimea, Russia turned to suggestion and distraction to validate its military incursion to its domestic audience. Code-based tactics, cover, and electronic warfare were the most common tactics during this stage and enabled a broad implementation of suggestion and distraction and also inhibited an international response.

Russian forces consolidated control of military installations, the media, the internet, and cellular networks through electronic warfare tactics. Consolidation of control in the information sphere enabled Russia to utilize the tactic of cover entities across the media spectrum and within local organizations to distract observers from its activities. Specifically, television is still the primary source of information dissemination in Ukraine and Crimea, and 74 percent of the population derives information mainly from television. One leading Russian television station in Ukraine is associated with the Institute of CIS Countries' director who is a proponent of Novorossiya.[36] Essentially, Russia used consolidation of control over the media to implement both suggestion and distraction concerning the invasion of Crimea while also legitimizing its actions.

Post-Eastern Ukraine, the form of IW changed, and deception was implemented on a massive scale to rewrite the origins of the conflict, alter beliefs about facts on the ground, and manipulate the allocation of resources in a manner that fostered positive decision-making outcomes for Russia, mainly in the form of a lack of Western intervention and the inability of the Ukrainian government to mount an effective response. Indicative of this is the report that in 2019 one in three Ukrainians was confused as to who started the war in Crimea.[37] Also, external governance has become an accepted narrative in eastern regions, illustrating the effectiveness of focusing on suggestion pre-invasion of Eastern Ukraine.[38]

At this point, the conflict became frozen, one of many outcomes favorable to Russia. High levels of disinformation, primarily enabled by the consolidation of control over the media, telecommunications system, and strategically placed elites parroting Russian narratives, achieved deception and pressure in the final stage. Amplification and cross-legitimization were used between media sources to normalize disinformation and achieve deception.

Russia's use of paramilitary forces in Ukraine was vital, but was hardly the most surprising aspect of warfare. More surprising was Russia's ability to "coordinate military and non-military means, including the information warfare aspects."[39] It did this by dividing the population early on, distracting international entities that could interfere, and placing high economic, diplomatic, and social pressure on Ukraine. Russia then vilified the leadership as fascist, claimed that government actions were unconstitutional, posited itself as the defender of a created victim group, and suggested that the West backed the protesters.[40] Finally, all that was left was to continue distraction through heightening disinformation levels, effectively paralyzing the decision-making capabilities of Ukrainians and Western diplomats, and corrupting the reflexive system.

Russia also used code-based tactics throughout the periods of war examined here. Russian IW doctrine consistently uses information-technology approaches throughout an IW campaign, and the events data show effective implementation of the doctrine. Since code-based tactics support any form of IW, it is understandable to see it as one of the most used tactics in Ukraine. Code-based tactics enabled other tactics to delegitimize the Ukrainian government, amplify disinformation, spread ideas, and consolidate control.

DOPES highlights a western misunderstanding that the most effective period of IW is the beginning of the war.[41] IW was vital through all stages of warfare, including throughout the kinetic stage. Western analysts assuming that Russia intends IW to be carried out linearly in a war setting underestimate Russia's IW strategy.

Russia's flexible IW doctrine enabled it to achieve international paralysis and increased federalism, and therefore Russian influence, in the region. The outcome raises doubts about whether specific plans are necessary when using reflexive control and IW or just broad directions.[42] Furthermore, Russia's deep understanding of the cultural and reflexive system, and all the previous long-term leg work associated with co-opting it, proved vital for the demoralization of the target. The exact progression of forms and tactics will be implemented differently in future Russian IW campaigns. However, scholars and practitioners should acknowledge that Russia understood the target society and exploited its vulnerabilities and that the Russian implementation of IW aligns with its stated doctrine.

The United States

Whereas Ukraine lies within Russia's traditional sphere of influence and holds a unique position within Russia's national heritage, the US is the dominant democratic state espousing the liberalism that most threatens Russia, and the IW campaigns in these two states were quite different. As Sokolsky and Stronski explain, the key aims against the US were to delegitimize institutions, disintegrate the coalition of Western states through division, and destroy the supranational organizations that undergird democratic values.[43] Flake notes that Russia pushes a narrative of a "corrupt and failing" US democratic system, building on pre-existing ideas in specific segments of the US population.[44] Russia targets these groups in order to amplify, disseminate, and normalize its narrative.

DOPES shows that pressure is the most commonly used form in the US campaign. Pre-election, Russia used suggestion and division to attack the moral legitimacy and value system that drove decision-makers within the US reflexive system. Leaks, political action campaigns, and attacks on the political legitimacy of policy elites were common tactics. Undergirding these tactics was the specific targeting of the US media enterprises, a primary source of legitimacy within US civil society. The tactics align with known Russian IW doctrine, which attempts to destabilize countries through psychological attacks and undermine political, economic, and social systems.[45]

Kuleshov, Zhutdiev, and Fedorov explain that Russia's goal is to use psychological influence to encourage important resources to be "handed over voluntarily, since this is seen not as the result of aggression, but as a progressive movement toward democracy and freedom."[46] The tactics Russia used pre- and post-election illustrate this use of reflexive control. For example, the pre-election emphasis on leaks and attacks on political legitimacy enabled Russia to foster and amplify divisions post-election. Polemics further destabilized and disintegrated trust in media sources, with a recent Gallup poll noting that only 21 percent of Americans have "a great deal" or "quite a lot" of trust in newspapers.[47] In essence, Russia focused its IW campaign on driving a push for perceived progress toward a better democracy while at the same time hollowing out and co-opting the very elements of a healthy democratic system.

The pre-2016 election focus was on political elites. Post-election, Russia began targeting general civil society, hoping to funnel public discontent and division from the elites to general citizens. Easy US targets for Russia during the IW campaign included racism and immigration, both subjects with large numbers of activists to co-opt into increasing the state's instability. Russia can exaggerate the extent of racism in the US because of real discrimination that exists.[48] Again, this aligns with an understanding of the reflexive system of the US, where political elites rely on mass perception, which civil society perpetuates.

Some scholars have highlighted the trend of Russia embedding itself within social media networks, learning how to interact successfully, and then manipulating the narrative and the actual network.[49] Persistent, long-term use of #blacklivesmatter by Russian agents within online African American networks illustrates this manipulation and co-option.[50] Scholars have also noted the Russian emphasis "to divide America by further polarizing an already polarized political climate."[51]

DOPES facilitates analysis of both of these trends, and the events data illustrates how the tactics employed can change while the form stays the same because the IW's target has changed. The change reflects a Russian understanding of the origins of US government legitimacy and Russia's technical ability to creatively and quickly build on trends evidenced in the target society to achieve successful outcomes from IW campaigns.

Comparison

The overarching aim of IPW is information superiority in the reflexive system, and Russian IW campaigns have implemented this doctrine across a wide range of cases, of which this study focused on two. The data illustrates Russia is clearly capable of running simultaneous IW campaigns that span the globe. In addition, one of the best-used methods for achieving information superiority includes the co-option of the mass media, military command-and-control processes, elite decision-makers, and the public in democratic states.[52]

Moreover, the DOPES forms and tactics align with the goal of RC.[53] Critics of Russia's work in Eastern Ukraine say there was no clear doctrine, but DOPES illustrates a flexible doctrine with clear and consistent categories of forms and tactics regardless of the target. This flexible and broad doctrine benefits Russian decision-makers who may fail to achieve tactical victories because it enables a wide range of follow-on options to achieve the broader mission.[54]

Russia aims to induce paralysis in both Ukraine and the US, identify and co-opt groups with anti-systemic leanings, and create alternative realities that they can later reinforce through Russian-backed entities.[55] The progression from division to suggestion and distraction in Ukraine illustrates this process. The evolution of tactics from political action and leaks to polemics and amplification in the US is a similar illustration. Vorobyov and Kiselev explain that this process often presents as buying up mass media, creating a perception of protecting democracy, infiltrating local government elections, and using nonprofit organizations.[56] These tactics are used in both Ukraine and the US campaigns, as the events data illustrate.

Russia knows it cannot destroy the US, but the US can destroy itself. The Leninist concept of disintegration provides the historical conceptualization for Russia to implement a campaign where “every manifestation of discontent” is utilized.[57] Disinformation becomes a potent weapon of societal disruption.[58] Russia achieves this by undercutting the government’s legitimacy, deeming individuals and institutions hypocritical or morally repugnant, and co-opting language.[59]

In a 2017 US Senate hearing, it was noted that Russian IW is not so much about manipulating groups into trusting Russia but instead encouraging groups to legitimize their ideas and delegitimize all others, which is the Marxist idea of repressive tolerance.[60] Through the modern implementation of RC, groups come to view one another as adversaries who have no common ground, leading to group conflict.[61]

The flexibility of Russia’s IW encourages use of different forms and tactics in different states. Russia will not likely replicate the Crimea model or even the US model. Instead, its IW will reappear with different combinations of tactics and forms which can be altered and redirected within the campaign based on new developments within the specific reflexive system.

RECOMMENDATIONS

The US must address its shortcomings from multiple directions if it desires to regain the strategic advantage or even successfully defend itself against Russian IW forms and tactics. Military involvement is a necessary but incomplete step; hyper-focus on a military solution will create an inadequate response to IW.

Recommendation 1: Bolster human networks, which are imperative for both offense and defense.

Human-centered strategies should identify and disrupt the human networks engaged in propagating IW, create networks to launch our IW campaigns, and facilitate durable and robust counterintelligence. From the counterintelligence perspective it means identifying connections between those within a decision-making loop and outside entities, such as Kremlin-linked think tanks and oligarchs, who are pressured in IW campaigns through illicit finance and investment.[62] The US must identify and disrupt these flows.

Recommendation 2: Regain institutional knowledge of Russian IW.

The US Intelligence community should target the Russian institutions that provide a bedrock for developing Russian IW doctrine and RC. For example, one widely understood element of effective RC is encouraging unpredictability. DOPES analysis can help counter this.[63] Clearly identifying the elements of Russian IW will lead to possible avenues of mitigation.

Recommendation 3: Consolidate and coordinate IW in the US.

The US must professionalize IW human capital and then decentralize and disperse the implementation of strategic goals through these individuals. Furthermore, consideration of recreating the Active Measures Working Group (AMWG) to identify Russian IOs may be beneficial.[64] The organization could "identify and expose" Russian disinformation and there could be a classified and public version of the group.[65]

Recommendation 4: Bolster Counterpropaganda.

Counterpropaganda should highlight Russia's illiberalism toward particular groups, outing the corruption of Russian elites and oligarchs, amplifying dissident stories within Russia, and the potential use of the Orthodox community, which today is strongly aligned with the Russian state. Each of these forms was used successfully by Russian counterpropagandists in Ukraine during World War II, as laid out by Kudinova.[66]

Recommendation 5: Acknowledge a necessary culture shift at home.

The priority as to combating tactics, especially disinformation and polemics, should be objectivity more than balance.[67] Objectivity and resilience are perhaps the two most important methods to combat Russian IW, although both of these would require a change in current American cultural norms. A society under attack needs to endure the present chaos with patience and fortitude until the facts can be found.[68] Society also must be resolved first to understand the facts before rushing to conclusions. Unfortunately, current means of mass communication in the US engender neither resilience nor objectivity. Indeed, they heighten impatience.

Recommendation 6: Set standards for online privacy and data protection.

IW abuses the lack of individual privacy afforded by the current regulatory measures in the digital space.[69] The data collected on an individual, which the US government cannot use, is sold and used by adversaries to launch IW campaigns to persuade or modify an individual's behavior.[70] Regulating who can collect personally identifiable data, its stored duration, how it is to be stored, and how it can be disseminated are all key avenues of regulation by the federal government.[71]

CONCLUSION

The goal of Russian IW is not to create a war; it is to prepare the ground in case of war and assist war once in process. Information warfare need not convince anyone; it simply needs to generate noise and destroy the idea of objective truth.[72] Essentially, it comes down to convincing those you can and confusing those you cannot. Russia's narratives are appealing because they tell a linear story that is flexible and straightforward, two elements that draw in "unwitting naïve idealists."[73]

Ultimately, Russia's use of IW is flexible, and it uses whichever tactics are most appropriate for the timing and context.[74] However, when combined, the effect can become fatal for a society.[75] Ukraine and the US bear witness to this process. Each tool used by the Russians is meant as one aspect of a cumulative, long-lasting campaign to create, direct, and support a particular framework beneficial to Russia's geopolitical goals. Bagge's DOPES methodology is a valuable tool to identify the forms and tactics of Russian IW as they occur in real-time while also providing evidence of Russia's ability to adhere to and implement its IW doctrine in multiple ways simultaneously. The US requires an ever nimble and robust response to mitigate Russian IW.

DISCLAIMER

The views and opinions expressed in this article are those of the author alone and do not reflect the official policy or position of the U.S. Department of Defense (DoD), U.S. Cyber Command, or any agency of the U.S. Government. Any appearance of DoD visual information or reference to its entities herein does not imply or constitute DoD endorsement of this authored work, means of delivery, publication, transmission, or broadcast.

NOTES

1. Daniel Bagge, *Unmasking Maskirovka: Russia's Cyber Influence Operations* (New York, New York: Defense Press, 2019), 27.
2. Sandor Fabian, "The Russian Hybrid Warfare Strategy-Neither Russian Nor Strategy," *Defense & Security Analysis* 35 no. 3, (2019): 308-325.
3. Timothy Thomas. Thinking Like *a Russian Officer: Basic Factors and Contemporary Thinking on the Nature of War* (US Army Training and Doctrine Command, 2016), 38.
4. Timothy Thomas, "Russian Military Thought: Concepts and Elements," *MITRE Corporation* (US European Command, 2019): 12-3.
5. Katherine Costello, "Russia's Use of Media and Information Operations in Turkey: Implications for the United States," (RAND Corporation, 2018), 3, http://www.jstor.com/stable/resrep19906.
6. Bagge, *Unmasking Maskirovka*, 72, 85.
7. Media Ajir and Bethany Vailliant, "Russian Information Warfare: Implications for Deterrence Theory," *Strategic Studies Quarterly* Fall (2018): 70-89; Conor Cunningham, "A Russian Federation Information Warfare Primer." *The Henry M. Jackson School of International Studies* (November 12, 2020), 2, https://jsis.washington.edu/news/a-russian-federation-information-warfare-primer/.
8. Vladimir A. Lefebvre, *Conflicting Structures*, trans. Victorina D. Lefebvre (Los Angeles: Leaf & Oaks Publishers, 2015).
9. Lefebvre, *Conflicting Structures*, 12.
10. Lefebvre, *Conflicting Structures*, 55.
11. Sergey G. Chekinov and S. A. Bogdanov, "Strategic Deterrence and Russia's National Security Today," *Voennaya Mysl' (Military Thought)*, 3 (2012): 11-20; Stanislav Ermak and Aleksandr Raskin, "Are All Methods Good in Battle? On Some Aspects of Reflexive Control of the Enemy," *Armeyskiy Sbornik (Army Journal)* 7 (2002): 44; V. N. Karankevich, "How to Learn to Deceive the Enemy," *Voennaya Mysl' (Military Thought)* 15 (2006): 135-152.
12. Bagge, *Unmasking Maskirovka,* 53.
13. Ministerstvo Oborony Rossiyskoy Federatsii (Ministry of Defense of the Russian Federation), *Conceptual Views on the Activities of the Armed Forces of the Russian Federation in Information Space* (2011), www.ens.mil.ru.
14. Makhmut Gareev, *If War Comes Tomorrow? The Contours of Future Armed Conflict*, trans. Yakov Vladimirovich Fomenko (Abingdon: Routledge 1998), 53.
15. Bagge, *Unmasking Maskirovka*; C. Kamphuis, "Reflexive Control: The Relevance of a 50-year-old Russian Theory Regarding Perception Control," *Militaire Spectator* 187, no. 6 (2018): 329; Kevin N. McCauley, *Russian Influence Campaigns Against the West: From the Cold War to Putin (*North Charleston, South Carolina: CreateSpace Independent Publishing Platform, 2016); Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (New York: Farrar, Straus and Giroux, 2020); Timothy Thomas, "Russia's Reflexive Control Theory and the Military," *Journal of Slavic Military Studies* 17, no. 2 (2004): 237-256.
16. Keir Giles, *The Next Phase of Russian Information Warfare (*NATO Strategic Communications Centre of Excellence, 2016): 3; Keir Giles, *Handbook of Russian Information Warfare,* Research Division (NATO Defense College, 2016), 23.
17. Giles, *Handbook of Russian*, 9.
18. Ulrik Franke, *War by Non-Military Means: Understanding Russian Information Warfare*, Russia Studies Programme, March (Swedish Defense Research Agency, 2015), 20; Giles, *The Next Phase* (2016): 4.
19. Bagge, *Unmasking Maskirovka*, 46; Giles, *Handbook of Russian*, 9.
20. Bagge, *Unmasking Maskirovka,* 63.
21. Valery Gerasimov, "The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations," *Voyenno-Promyshlennyy Kuryer* (2013).
22. Giles, *The Next Phase.*
23. Giles, *The Next Phase.*
24. Jolanta Darczewska, *The Anatomy of Russian Information Warfare: The Crimean Operation, A Case Study* (OSW Centre for Eastern Studies, 2014), 6.
25. Thomas, *Thinking Like a Russian*, 15.
26. Sergey G. Chekinov and S. A. Bogdanov, "The Strategy of the Indirect Approach: Its Impact on Modern Warfare," *Voennaya Mysl' (Military Thought)* (2011): 4; Chekinov and Bogdanov, "Initial Periods of War," 27; Gerasimov, "The Value of Science."

NOTES

27. Giles, T*he Next Phase* (2016).
28. Cunningham, "A Russian Federation," 5.
29. Thomas, *Thinking Like a Russian,* 30.
30. S. A. Komov, "About Methods and Forms of Conducting Information Warfare," *Military Thought* (English edition), 4 (July-August 1997), 18-22.
31. Costello "Russia's Use of;" Darczewska, *The Anatomy of,* 26; Rid, *Active Measures*, 133, 147.
32. Maria Snegovaya, "Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare," Institute for the Study of War (2015), 15.
33. Snegovaya, "Putin's Information Warfare," 15.
34. M. Hammond-Errey, "Understanding and Assessing Information Influence and Foreign Interference," *Journal of Information Warfare* 18, no. 1 (2019): 1-22.
35. Franke, *War by Non-Military*, 45.
36. Oleksandra Tsekhanovska and Liubov Tsybulska, *Evolution of Russian Narratives About Ukraine and Their Export to Ukrainian Media Space* (Ukraine Crisis Media Center, 2021), 4, 6, https://uacrisis.org/en/russian-narratives-about-ukraine7.
37. Detector Media, *Sources of Information, Media Literacy, and Russian Propaganda: The Results of the All-Ukrainian Public Opinion Poll*, March 2019, 10.

38 Detector Media, "On the Other Side of the Screen: An Analysis of Media Consumption and Disinformation in the Ukraine's Information Environment," May 18, 2021, https://detector.media/infospace/article/188115/2021-05-18-on-the-other-side-of-the-screen-an-analysis-of-media-consumption-and-disinformation-in-the-ukraines-information-environment/

39. Franke, *War by Non-Military*, 44.
40. McCauley, *Russian Influence Campaigns,* 354.
41. Snegovaya, "Putin's Information Warfare," 17.
42. Kristiina Muur, et al., "Russian Information Operations Against the Ukrainian State and Defense Forces: April-December 2014 in Online News," *Journal on Baltic Security* 2, no. 1 (2016): 63.
43. R. Sokolsky and P. Stronski, *The Return of Global Russia: An Analytical Framework*, Carnegie Endowment for International Peace, December 14, 2017, https://carnegieendowment.org/2017/12/14/return-of-global-russia-analytical-framework-pub-75003.
44. Lincoln Flake, "Russia and Information Warfare: A Whole-of-Society Approach," *Lithuanian Annual Strategic Review* 18 (2020): 168.
45. Gareev, *If War Comes*, 53; Ministry of Defense of the Russian Federation, *Conceptual Views* on.
46. E. Kuleshov, B. B. Zhutdiev, and D. A. Fedorov, "Information-Psychological Confrontation Under Contemporary Conditions: Theory and Practice," *Vestnik Academia Voennykh Nauk* (*The Journal of* t*he Academy of Military Science*) 1 (2014): 108.
47. Megan Brenan, "Americans' Confidence in Major U.S. Institutions Dips," *Gallup*, July 14, 2021, https://news.gallup.com/poll/352316/americans-confidence-major-institutions-dips.aspx.
48. Oleg Kalugin, *Spymaster* (New York: Basic Books, 2009), 54.
49. David M. Beskow and Kathleen M. Carley, "Characterization and Comparison of Russian and Chinese Disinformation Campaigns," in *Disinformation, Misinformation, and Fake News in Social Media,* (2020), 63-81.
50. Beskow and Carley "Characterization and Comparison;" Patrick Savage, *Social Media Information Operations: How Russia Has Used Social Media to Influence US Politics* (American Security Project, 2017).
51. Beskow and Carley "Characterization and Comparison."
52. Sergey G. Chekinov and S. A. Bogdanov, "Initial Periods of Wars and Their Impact on a Country's Preparations for a Future War," *Voennaya Mysl' (Military Thought)* 4 (2012): 27.
53. Bagge, *Unmasking Maskirovka*; Kamphuis, "Reflexive Control," 329; McCauley, *Russian Influence Campaigns; Rid, Active Measures*; Thomas, "Russia's Reflexive Control."
54. Muur, et al., "Russian Information Operations, 69.
55. Todd C. Helmus, et al., *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe* (RAND Corporation, 2018), 9.
56. I. Vorobyov and V. Kiselev, "Hybrid Operations as a New Form of Armed Conflict," *Voyennaya Mysl* 5 (2015): 41-49.

NOTES

57. Vladimir Lenin, *What Is to Be Done*? (New York: International Publishers, 1929), 84.
58. McCauley, *Russian Influence Campaigns,* 22.
59. United States Senate, "Russian Influence and Unconventional Warfare Operations in the 'Gray Zone': Lessons From Ukraine," hearing before the Subcommittee on Emerging Threats and Capabilities of the Committee on Armed Services, March 29, 2017 in Washington D.C., 5, http://www.fdsys.gov.
60. Ibid.
61. Marek N. Posard et al., *From Consensus to Conflict: Understanding Foreign Measures Targeting* U.S. Elections, RR-A704-1 (RAND Corporation, 2020), https://doi.org/10.7249/RRA704-1.
62. Heather A. Conley et al., *The Kremlin Playbook 2: The Enablers,* Center for Strategic and International Studies, March (2019), https://www.csis.org/features/kremlin-playbook-2.
63. Giles, *Handbook of Russian,* 53.
64. Steve Abrams, "Beyond Propaganda: Soviet Active Measures in Putin's Russia," *Connections: The Quarterly Journal* 15, no. 1 (2016): 10.
65. Abrams, "Beyond Propaganda," 10, 11.
66. L.V. Kudinova, "The Role of Soviet Counter-Propaganda in Countering the Voluntary Departure of the Population from the Occupied Ukrainian Territories to Work in Germany," *Gileya* 110 (2016): 81-85.
67. Keir Giles, *Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power,* Russia and Eurasia Programme, March (Chatham House: The Royal Institute of International Affairs, 2016).
68. Snegovaya, "Putin's Information Warfare," 18.
69. Jessica Dawson, "Microtargeting as Information Warfare," *The Cyber Defense Review Winter*, 6, no. 1 (2021): 65.
70. Dawson, "Microtargeting as Information, 69, 71.
71. Jessica Dawson. Presentation at SECR 6982: Information Warfare class, Augusta University, Augusta, GA, November 2, 2021.
72. Steven Wilson, "What Are Russia's Goals with Disinformation on Social Media? Professor Steven Wilson Explains," *BrandeisNow* October 22, 2020.
73. McCauley, Russian Influence Campaigns, 66; Ben Nimmo, *Anatomy of an Info-War: How Russia's Propaganda Machine Works and How to Counter It*, Strategy Council (Central European Policy Institute, 2015).
74. Kateryna Zarembo and Sergiy Solodkyy, "The Evolution of Russian Hybrid Warfare: Ukraine," *CEPA January* 29, 2021.
75. Roy Godson et al., *Soviet Active Measures, People-To-People Contacts, and the Helsinki Process* (New York: Ramapo Press, 1986).

A Military of Influencers: The U.S. Army Social Media, and Winning Narrative Conflicts

Lieutenant Colonel Robert J. Ross, Ph.D.
Josh Rutland

ABSTRACT

In the interconnected era of the Internet, the military must confront the new face of an old threat: narrative conflict. Where states once maintained nearly absolute domestic control of the narratives surrounding their military engagements, social media have created a wide array of perspectives, arguments, and disinformation campaigns that constantly affect both the civilian and military populations. These campaigns encourage the questioning of state objectives and threaten the identity of the individual and the collective ontological identity of the society, making it more difficult for states to maintain momentum and support for their military endeavors. Without that support, military campaigns can collapse, regardless of the skill or preparedness of warfighters. This research explores three topics relevant to the U.S. Army in hopes of helping it better equip itself to succeed in narrative conflicts: the strategic impacts of commander's decisions on the battlefield, the need to control signals emissions, and the consequences of bulk internet data sales. It then concludes by providing brief policy suggestions for mitigating these issues.

INTRODUCTION

When the Gutenberg printing press emerged in the late 15th century, it rocked the foundations of societal order in Europe by establishing the first networked era.[1] The ensuing mass production of pamphlets made them accessible to the common person.[2] As the masses of common Europeans began to study religious texts for themselves, new perspectives emerged to challenge the church's

Lieutenant Colonel Robert J. Ross is the Strategic Initiatives Group Chief for the Commanding General of U.S. Army Cyber Command, Fort Gordon, GA. Lieutenant Colonel Ross advises the ARCYBER Commanding General on cybersecurity, information-age conflict, and information warfare strategy. He is a former assistant professor in the Electrical Engineering and Computer Science Department at the U.S. Military Academy at West Point, NY. He is a former Chief Research Scientist for the Army Cyber Institute, a position in which he served as the Information Warfare Team Lead. He has a B.S. degree in Computer Science from Rowan University, an M.S. in Computer Science from Monmouth University, and a Ph.D. in Information Science from the Naval Postgraduate School. Lieutenant Colonel Ross is a cyberwarfare officer and former artilleryman with two combat deployments to Iraq. His research interests are organizational science, strategic foresight, information warfare, 21st century conflict, and financial technology.

authority.[3] Ultimately, the increasingly rapid dissemination of information through advancing technology caused the questioning, undermining, and weakening of the authority of the Roman Catholic Church, which had dominated religious narratives in Europe for more than 1,000 years.

Technology has continued to grow in modern times, with mobile phones and the Internet creating a network of instantaneous communications much, much larger in scope than that of Gutenberg's printing press. The growing technology has amplified impacts on society, with conventional authorities facing unprecedented challenges to their leadership. The time has passed for state control over the information flow across and within its borders using traditional media methods, and official narratives that shaped public opinion in support of the state. Political and ideological dissonance quickly and ubiquitously pours across the borderless Internet from which the global audience drinks.[4] Blog posts, cell phone footage, podcasts, drone recordings, and myriad other content forms are deemed valid regardless of merit or origin.[5] Collectively, they form the new narratives consumed and further propagated by the masses on social media. The result is, once again, a questioning of conventional authority and the degradation of that authority's power at an unprecedented rate. The walls of Westphalia have fallen again.

These developments have troubling implications for contemporary warfighting scenarios, which require a motivated military and citizenry for victory. While traditional military conflict continues, as in the Russian invasion of Ukraine, and remains a critical component of warfare, the importance of narrative conflict has never been greater. The Internet, mobile phones, and social media offer an opportunity for states to infiltrate the minds of their adversaries' citizenry through

Josh Rutland is a graduate of Augusta University's Master in Intelligence and Security Studies program. He currently works as a researcher in the Augusta University Department of Emergency Medicine and will soon be employed by ARCYBER as an Information Technology Specialist. His research focuses on information warfare, cybersecurity, terrorism, and biosecurity. His work has appeared in such journals as *Politics and the Life Sciences, Politics & Policy, Behavioral Sciences of Terrorism and Political Aggression, Journal of Cyber Policy,* and *PLOS Global Public Health*.

widespread, tailored propaganda efforts. These efforts may be designed to facilitate a variety of outcomes, including diminished support for a war. Demoralization on such a wide scale threatens to "rob an army of its spirit and a commander of his courage," which Sun Tzu described as the key to victory, destroying an adversary's will to fight without so much as a single battle.[6] The Islamic State of Iraq and Syria's (ISIS) victory over the Iraqi Army at Mosul provides a potent example of the power of narrative: The 10,000 troops present in Mosul had mostly abandoned their posts out of fear spawned by ISIS terror campaigns that streamed across the Internet long before ISIS forces arrived in the city.[7] The result was an easy victory for ISIS forces. Though the Iraqi force was larger and better armed, its fear of ISIS ultimately ensured its defeat.[8] Even the US has fallen prey to the effects of narrative defeat during the wars in Vietnam, Iraq, and Afghanistan. Wars can be won or lost based on their surrounding narratives despite overwhelming tactical victory in every engagement using traditional military force.

This article argues that winning modern narrative conflicts will demand doctrinal change within the Army and other services in some key areas relevant to information operations, public affairs, psychological operations, and cyber space operations. The study focuses on three important issue areas: the strategic impacts of soldiers' decision-making, vulnerabilities related to signature management, and the threats posed by bulk data collection and sales conducted by third party social media platforms. To demonstrate this point, the article proceeds in two sections. First, we briefly analyze the three focal issue areas using existing literature that highlights their importance and details the security issues. Then, we provide relevant policy suggestions, based on modifications of former and existing Army doctrine generated from researching this topic.

THE STRATEGIC CORPORAL

U.S. Marine General Charles Krulak conceptualized the strategic actions at the lowest tactical level in his 1999 essay titled “The Strategic Corporal.” Krulak argued that “success or failure will rest, increasingly, with the rifleman and with his ability to make the *right* decision at the *right* time at the point of contact” with both the enemy and the local population.[9] In addition to the pressures of high stress environments where lives are at stake; the soldier in the field also bears the burden of overcoming two major obstacles: a general hostility and weariness on the part of the local population and the mutually perceived cultural divisions between one’s own “ingroup” and the “outgroup” that inhibit communication and personal bonding.[10] While this places additional demand on warfighters, their ability to understand and adopt relevant customs and behaviors of the indigenous populations with which they interact will shape their own personal relationships within that society and the general disposition of that society toward other warfighters with whom they interact in the future.[11]

As such, the ability of Army warfighters also to function and be perceived as “cultural mediators” and community members when interacting with a foreign populace is a critical tool that must be maintained like any other piece of equipment in a soldier’s toolkit.[12] This has led to calls for redesigned professional military education processes that highlight the importance of language training, cultural education, and “educational and experiential cross-fertilization between the military and other government agencies” or humanitarian organizations relevant to future operational fields.[13] Major Linda Liddy of the Australian Army also argues that the modern soldier will need to be academically savvy in topics such as “military law and leadership, military history, and current affairs and ethics” in order to prepare fully for their role as warfighters and influencers expected to carry out complex operations with military and humanitarian ambitions.[14]

The omnipresence of cell phones with cameras and Internet connectivity further ensures that tactical-level actions, positive or negative, will ripple across the societies with which they interact and extend beyond their immediate communities.[15] Strategic adversaries could coopt footage depicting cultural insensitivity, whether accidental or deliberate, to fuel terrorist recruitment[16] or turn large populations and Internet communities against the U.S. Army. This could diminish its security, morale, and chances of operational success.[17] Warfighters must do everything in their power to set themselves apart in the minds of those with whom they interact in operational theaters to establish mutual respect, cooperation, and beneficence.[18] A warfighter has a personal presence in the minds of those with whom they interact. This means that the warfighter ceases to be simply an American or a soldier to become a friend or community member, which can be critical in environments such as the Middle East where cultural and familial bonds mean far more than shared regional or territorial residency. In short, impressions and reputations are critical; they can make or break an operation tactically and narratively.[19] Warfighters will need to be able to shape their reputations in a positive way to ensure operational success.

SIGNATURE MANAGEMENT VULNERABILITIES

Signature management vulnerabilities are those associated with the impacts on battlefield events or troop deployments of signals emitted and received from electronic devices.[20] While myriad strategic vulnerabilities exists with respect to signature management and narrative conflict, two significant threats stem from physical infrastructure and "digital exhaust,"[21] which is described by Harper Reed as "a constant trail of activities, behaviors, preferences, signatures, and connections" left behind by every digital device that is tied to both that device and its user.[22] Both have the potential to contribute to adversaries' interception of sensitive information regarding Army units, ultimately resulting in "the design and development of adversary systems, tactics, training, and force preparations capable of countering Army unit capabilities, activities, and intentions."[23] As such, new considerations must be accounted for to limit public knowledge of Army units and their deployments successfully.

Control of physical infrastructure means control over and access to any signals that pass through it.[24] Army units thus cannot be sure their communications are secured when operating in a foreign theater where critical infrastructure is built, owned, and operated by potentially adversarial forces.[25] As the world transitions to 5G technology, this becomes an even greater risk, as 5G infrastructure is being built primarily by China across parts of Asia, Africa, and Europe.[26] This gives China "access to the private data of billions of people" which may include "individuals' medical histories, spending habits, political views, personal details expressed on social media, physical location, financial situation" and much other data the state could adapt to "gain a commercial or technical advantage in data-driven markets, target key individuals for recruitment by intelligence operations, or compromise political figures."[27] Civilians are not the only potential target of this type of data collection. Anyone using the network is vulnerable.[28] As such, it is imperative that the Army anticipate this battlefield vulnerability and develop alternatives to using foreign infrastructure, such as establishing its own permanent infrastructure in contested regions of influence.[29]

While physical infrastructure poses a significant vulnerability, digital exhaust may represent the most significant threat associated with signature management. Digital exhaust refers to the impact on the virtual realm resulting from military movements and engagements.[30] Adversaries could use this information to determine troop movements before they are made public, putting warfighters in harm's way, risking operational failure, and presenting adversaries with an opportunity to humiliate or propagandize against their opponent. The Bellingcat Study, the Second Nagorno-Karabakh War, and recent events in Ukraine all represent examples of how dangerous digital exhaust can be in the wrong hands.

During the Bellingcat Study, a handful of amateur Internet sleuths crowdsourced information largely comprised of the Russian military's digital exhaust to provide decisive evidence that Russian forces had shot down Malaysian Airlines Flight MH17 in July 2014.[31] The Bellingcat group, led by Eliot Higgins, used online videos and photographs to identify the specific Buk anti-aircraft missile that had shot down MH17.[32] It then collected a number of videos and photographs of the Buk that enabled it to plot successfully a timeline and geographic trail of its movements from Russia into Ukraine which proved Russia's culpability in MH17's destruction.[33] The discovery forced Russia into a losing battle with the Bellingcat group to control the narrative surrounding the MH17 incident that ultimately resulted in the Russian government's embarrassment.[34] The Bellingcat group harnessed the power of social media to expose a global power and its army.[35] Anyone with a vested interest, state-or civilian-sponsored, could employ Bellingcat's methods against any army, should that army fail to account for its troops' digital exhaust.

The Second Nagorno-Karabakh War between Armenia and Azerbaijan represents a more direct example of digital exhaust exploitation by one state against another.[36] Using Turkish Bayraktar TB2 drones and Israeli HAROP Loitering Munitions (LM) , Azerbaijani forces devastated the Russian-supported Armenian ground forces through the nearly exclusive use of unmanned strikes.[37] The cameras inside these drones captured live footage of the bombing and the destruction from the strikes, which was then broadcast to both sides by the Azerbaijanis for propaganda purposes.[38] The result was an invigorated war effort by Azerbaijan and a gravely deteriorating Armenian will to fight through the constant reliving of events and fear of unexpected future drone strikes.[39] The kinetic effects of drone strikes are lost lives and destroyed equipment, already damaging to the morale of a targeted belligerent. However, the ability of the drones to capture live full-motion video (FMV) and immediately broadcast this footage to online social media forums create powerful synergies between the kinetic and cognitive effects of unmanned aerial systems. Effects from these unmanned aerial systems cause both physical and psychological deterioration of their intended prey. Azerbaijan used FMV footage to amplify wisely what could be classified as the highly survivable kinetic effects of these weapons. Eventually, the Armenian war effort was crippled after a series of defeats displayed TB2 drones "literally flying circles near three S-300 sites while waiting to strike their targets before doing damage assessment and flying away," forcing the Armenian Army to capitulate rapidly.[40]

The Russian-backed Armenian Army was powerless to counter the effects of these Turkish and Israeli unmanned aerial systems (UAS). Ukraine, with which Russia has been in direct conflict since 2014, noticed this.[41] In September 2021, Ukraine acquired 24 TB2 drones from Turkey to bolster its own efforts against Russia after observing their effectiveness in the Second Nagorno-Karabakh War.[42] The following month, the Ukrainians deployed the TB2s against Russian-backed separatists in Crimea for the first time, damaging a 122mm D-30 howitzer in the Donbass region that had previously injured one Ukrainian soldier and killed another.[43] The Ukrainians followed the Azerbaijan example by using the onboard camera systems to collect and distribute footage of the air strike online.[44] The Ukrainian Army employed this capability with continuously devastating effect after the Russian invasion in February 2022. While this is the most recent example of lessons from the Second Nagorno-Karabakh War's proliferation, it likely represents an early look at how future wars may be fought.[45] This deadly combination of conventional weaponry and narrative shaping tools represents a dangerous threat for states that fail to develop methods for controlling digital exhaust such as drone footage of engagements, especially battlefield losses.

BULK DATA COLLECTION AND SALES

Bulk data collection refers to the mass collection of personal data gathered by social media companies and other website managers.[46] As users browse websites and services that require them to accept "informed consent" agreements coupled with the proliferation of Internet of things (IoT) devices when creating or linking personal accounts, the providers and creators of these services collect bulk data from their browsing patterns.[47] Two types of research typically employ these data: academic and marketing.[48] Marketing research practices in particular represent the greatest threat from bulk data collection, as this type of research usually involves the construction of personalized profiles of each individual user to monitor and record that person's likes, dislikes, interests, purchases, media preferences, and a variety of other traits.[49] While almost all web browsing generates bulk data, social media websites represent the prime collection ground for these data as they offer a look into not only a person's preferences, but also who they associate with, social movements with which they identify , and their personal beliefs.

This process, defined as "microtargeting" by MAJ Jessica Dawson,[50] represents a gold mine from a marketing perspective, as companies can use these data to construct carefully tailored advertisement intended to lure consumers into viewing and purchasing their products. However, from a security standpoint, microtargeting represents a potential narrative nightmare, as it offers anyone with access to this detailed profile information a roadmap for how best to propagandize messages in a way that will convince its target audience to adopt a desired perspective.[51] The Cambridge Analytica case demonstrates the potential for influencing operations based on the "digital exhaust" of users in the form of bulk data intentionally used to microtarget for the purpose of influencing "likely voter" decisions.[52] Both civilians and military personnel are vulnerable to microtargeting practices regardless of their social media use because, "even if an individual does not have a Facebook account, Facebook has a shadow account for them, collected from friends' phones, contacts lists, and emails as well as data Facebook itself purchases."[53] Usually, the only significant barrier to accessing these data is a licensing fee, meaning foreign adversaries can easily acquire them for nefarious purposes.

The same adversaries may also be able to amplify their microtargeted messages to a large audience of military personnel and civilians using "a relatively novel and increasingly dangerous means of persuasion within social media," which Lt Col Jarred Prier calls "commanding the trend."[54] This method involves using bot-driven, falsified swarms of activity or "views" to manipulate the algorithms that social media sites use to "analyze words, phrases, or hashtags to create a list of topics sorted in order of popularity."[55] This activity swarm increases a page's visibility and its likelihood of being clicked and shared by convincing social media algorithms that a topic is growing in popularity, prompting the algorithm to promote it on trending pages.[56] Algorithms do not verify the authenticity of stories before promoting them, nor do they verify the credibility of the users who share them. While some companies have begun modifying their algorithms and attempting to find countermeasures to bot swarms, the reality remains that by the time a topic has reached the trending page it has already spread beyond containment.[57] Narratives promoted in this manner that are harmful to Army interests could prove dangerous and impossible to control.

POLICY SUGGESTIONS

As Joint Chiefs of Staff Chairman General Mark Milley has argued, strategic competitors' increasing capability to "fight the US through multiple layers of stand-off in all domains" means that a "doctrinal evolution" of the American way of war is necessary.[58] The lessons demonstrated in conflicts in Ukraine, Iraq, and Armenia suggest that narrative victory is growing in importance and a continual trend in the future.[59] The doctrinal adjustments necessary for the U.S. Army to fortify itself properly for this changing dynamic of warfare will likely be complex and take time to implement, but they will be essential to victory in future conflicts. The Army is probably the greatest modern conventional warfighting force, but it will need to bolster its ability to shape narratives surrounding conflicts in which it becomes involved to ensure that its conventional victories translate into strategic success.

The modern soldier must become conscious of his or her role as General Krulak's "strategic corporal," straddling the line between warfighter and diplomat.[60] In addition to combat capabilities, a soldier must be well-trained for decision making, problem solving, and positive cultural interaction.[61] Soldiers must be prepared for the eyes of the world on social media to scrutinize any and every action they take. The fate of Army morale and its reputation in the global court of public opinion hinges on the individual warfighter's ability to project a positive image of the Army to further the nation's strategic objectives. It is worth emphasizing that this does not represent a call for any lowering in priority of traditional combat skills and training; it is rather a call to elevate the importance of cultural and linguistic training as well as social media literacy.[62] Basing warfighter evaluations on both combat ability and social skills represents one way of honing these skills among Army personnel.

Signature management vulnerabilities present significant risks to operational security (OPSEC). Improving signals management strategies has been identified as a crucial step in advancing the U.S. Marine Corps' (USMC) contemporary warfighting capabilities for future conflicts.[63] The Army should afford signature management the same importance. Addressing these risks demands a prompt solution to the problems of physical infrastructure and the digital exhaust of personnel. The primary threat in the physical domain comes from China's 5G-infrastructure proliferation through its Belt and Road Initiative.[64] Using NATO as a "forum for collaboration" and expansion of US owned and operated 5G infrastructure is an optimal potential solution.[65] While this initiative will likely require significant investment in 5G-technology development and construction, the US could employ these technologies and their distribution as a diplomatic tool for strengthening relationships with existing allies or building new relationships with potential strategic partners. The Army and NATO operations in allied regions would also enjoy the benefits of US owned 5G systems: safe, trusted, and secure communications technology that would fully support the OPSEC of US joint and coalition forces.

Digital exhaust control may be more difficult to accomplish. The Army's ban on the use of personal communication devices on the battlefield is a constructive step, as it helps prevent the possibility of telecommunications interception, movement tracking using mobile device signals, and exposure to enemy disinformation that might demoralize or misinform soldiers.[66] Taking steps to mask deployment information such as supply purchases that may leave physical or digital paper trails should also be a priority. Purchasing supplies through a third-party or "middle-man," buying supplies in smaller quantities rather than in bulk and sending supplies to deployment zones with warfighters rather than shipping them directly there separately all represent potential solutions. To address online propaganda campaigns such as those seen in the second Nagorno-Karabakh War and Ukraine, the Army might consider using trend hijacking techniques such as bot swarming, as detailed by Prier, to bury adversaries' social media campaigns.[67] The Army needs to develop tactics, techniques, and procedures (TTPs) that mirror the informational effects demonstrated by the TB2 Bayraktar's successes in both the second Nagorno-Karabakh and Ukraine conflicts. TTPs that enhance the synergies between powerful kinetic and psychological effects stemming from these platforms. Furthermore, worth considering is the recruitment of existing social media influencers to help promote the Army's narratives, encouraging warfighters who demonstrate social media proficiency to become a new breed of battlefield correspondent, or the establishment of a U.S. Information Agency similar to the one created by President Eisenhower in 1953 to address US influence strategy during the Cold War. Israel's efforts to recruit young, tech-savvy, female social media operatives from existing Israeli Defense Force (IDF) units represents a notable success in this area.[68]

The Army's approach to bulk data sales and collection must respect the limitations put in place by the Fourth Amendment to the U.S. Constitution. For this reason, direct collection of data on American citizens for the purpose of microtargeted narrative construction is not a possibility. Rather, as MAJ Dawson[69] suggests, it may be useful for the Army to establish limits on data collection through cooperation with social media companies. The prevention of data collection from accounts owned by service members and their families represents a good starting point.[70] The encouragement of more stringent limits on obtaining these data from social media companies and the permitted uses of the data also represents a potential point of collaboration between the Army and social media corporations.

CONCLUSION

As the U.S. Army prepares for future conflicts, it becomes increasingly critical to consider the demonstrations of narrative power from the past and those unfolding in the present day. Winning future conflicts will mean winning narrative conflicts. To do that, the Army needs to adopt appropriate doctrinal changes related to information operations, public affairs, and cyber space operations. Tactical actions will shape strategic success, which emphasizes the need to train and equip warfighters as ambassadors of the Army's intentions and good will. Words, tweets, TikToks, Instagram posts, drone recordings, and any other microtarget-enabling media deemed "view-worthy" are the weapons of narrative conflicts. The Army must learn to leverage these weapons and deny them to strategic adversaries. This means limiting digital exhaust, cooperating with social media companies to undermine adversaries' ability to target US warfighters and citizens, and establishing a comprehensive public relations arm of the Army to promote its narratives on the ideological battleground. As conflict evolves, so too must the warfighter. It is time to forge an Army of influencers.

DISCLAIMER

The views and opinions expressed in this paper are those of the author alone and do not reflect the official policy or position of the U.S. Department of Defense (DoD), U.S. Cyber Command, or any agency of the U.S. Government. Any appearance of DoD visual information or reference to its entities herein does not imply or constitute DoD endorsement of this authored work, means of delivery, publication, transmission, or broadcast.

NOTES

1. Niall Ferguson, *The Square and the Tower: Networks and Power, from the Freemasons to Facebook*, Penguin Books (2019).
2. Ibid.
3. Ibid.
4. David Patrikarakos, *War in 140 Characters: How Social Media is Reshaping Conflict in the Twenty-First Century*, Hachette UK, (2017).
5. Ibid.
6. Sun Tzu, *The Art of War,* translated by Sammeul Griffith, Duncan Baird (2005, original work published 5th century BC), 108.
7. Peter warren Singer and Emerson T. Brooking, *LikeWar: The Weaponization of Social Media*, Eamon Dolan Books (2018).
8. Ibid.
9. General Charles C. Krulak, T*he Strategic Corporal: Leadership in the Three Block War*, Center for Army Lessons Learned Fort Leavenworth KS Virtual Research Library (1999), 5.
10. Stephen Bochner, "The Social Psychology of Cross-Cultural Relations," in *Culture in Contact: Studies in Cross-Cultural Interaction*, edited by Stephen Bochner, Volume 1, Oxford: Pergamon (1982), 14.
11. Bochner, "The Social Psychology of Cross-Cultural Relations," 13; Krulak, *The Strategic Corporal.*
12. Bochner, "The Social Psychology of Cross-Cultural Relations," 15.
13. Kevin D. Stringer, "Educating the Strategic Corporal: A Paradigm Shift," *Joint, Interagency, Intergovernmental, and Multinational Newsletter* (2011), 65; Major Linda Liddy, "The Strategic Corporal: Some Requirements in Training and Education," *Australian Army Journal* 2, no. 2 (2004), 139-148.
14. Liddy, "The Strategic Corporal: Some Requirements in Training and Education," 142.
15. Patrikarakos, *War in 140 Characters.*
16. Charlie Winter, *Media Jihad: Islamic State's Doctrine for Information Warfare*, London, UK, International Centre for the Study of Radicalisation and Political Violence (2017).
17. Patrikarakos, *War in 140 Characters.*
18. Bochner, "The Social Psychology of Cross-Cultural Relations," 13; LTC Robert J. Ross, Creating White Space: Interaction and the Adaptation of Team Social Identity in Complex Environments, Naval Postgraduate School Monterey, Monterey CA (2019), 19.
19. Krulak, The Strategic Corporal.
20. Brett van Niekerk and M. S. Maharaj, "Mobile Devices and the Military: Useful Tool or Significant Threat?," *Journal of Information Warfare* 11, no. 2 (2012), 1-11.
21. Josh Rutland "A Military of Influencers: The U.S. Army, Social Media, and Winning Narrative Conflicts" [unpublished master's thesis], Augusta University.
22. Brian David Johnson, Alida Draudt, Jason C. Brown, LTC Robert J. Ross, Ph. D., "Information Warfare and the Future of Conflict," produced by Cyndi Coon, The 2019 Threatcasting Workshop, Arizona State University (2019), 68.
23. U.S. Army, *U.S. Army Techniques Publication 3-13.3: Army Operations Security for Division and Below*, Headquarters, Department of the Army (2019), 1-1.
24. Luiz A. Dasilva, Jeffrey H. Reed, Sachin Shetty, Jerry Park, Duminda Wijeskera, and Haining Wang, "Securing 5G: NATO's Role in Collaborative Risk Assessment and Mitigation," *Cyber Threats and NATO 2030: Horizon Scanning and Analysis* (2020), 74-87.
25. Carolyn Bartholomew, "China and 5G," *Issues in Science and Technology* 36, no. 3 (2020), 50-57.
26. Ibid.
27. Ibid., 52-52.
28. Dasilva et al., "Securing 5G".
29. Ibid., 85.
30. Johnson et al., "Information Warfare and the Future of Conflict"; Rutland, "A Military of Influencers."
31. Matt Sienkewicz, "Open BUK: Digital labor, media investigation and the downing of MH17," *Critical Studies in Media Communication* 32, no. 3 (2015), 208-223; Patrikarakos, *War in 140 Characters.*

NOTES

32. Patrikarakos, War in 140 Characters, 181.
33. Ibid.
34. Ibid. Eliot Higgins, We Are Bellingcat: Global Crime, Online Sleuths, And The Bold Future Of News, Bloomsbury Publishing (2021).
35. Higgins, We Are Bellingcat: Global Crime, Online Sleuths, And The Bold Future Of News.
36. John Antal, "The First War Won Primarily with Unmanned Systems: Ten Lessons from the Second Nagorno-Karabakh War" (2021), https://www.socom.mil/.
37. Ibid.
38. Ibid.
39. Ibid.; Stijin Mitzer and Joost Oliemans, "Aftermath: Lessons of The Nagorno-Karabakh War Are Paraded Through the Streets of Baku," Oryx (2021), https://www.oryxspioenkop.com/; Rutland, "A Military of Influencers."
40. Mitzer and Oliemans, "Aftermath: Lessons of The Nagorno-Karabakh War Are Paraded Through the Streets of Baku," para. 22.
41. Burak Ege Bekdil, "Ukraine is set to buy 24 Turkish drones. So why hasn't Russia pushed back?" *Defense News* (September 29, 2021), https://www.defensenews.com/unmanned/2021/09/29/ukraine-is-set-to-buy-24-turkish-drones-so-why-hasnt-russia-pushed-back/.
42. Ibid.
43. Joseph Trevithick, "Ukraine Strikes Russian-Backed Forces Using Turkish-Made TB2 Drones For The First Time," *The Drive* (October 27, 2021), https://www.thedrive.com/the-war-zone/42894/ukraine-strikes-russian-backed-forces-using-turkish-made-tb2-drones-for-the-first-time.
44. Antal, "The First War Won Primarily with Unmanned Systems;" Trevithick, "Ukraine Strikes Russian-Backed Forces Using Turkish-Made TB2 Drones For The First Time."
45. Stephen Witt, "The Turkish Drone That Changed The Nature Of Warfare," *The New Yorker* (May 9, 2022), https://www.newyorker.com/magazine/2022/05/16/the-turkish-drone-that-changed-the-nature-of-warfare.
46. Rutland, "A Military of Influencers."
47. Trang Tran, "Personalized ads on Facebook: An effective marketing tool for online marketers," *Journal of Retailing and Consumer Services* 39 (2017), 230-242.
48. Ralph Schroeder, "Big Data and the brave new world of social media research," *Big Data & Society* 1, no. 2 (2014), 2.
49. Tran, "Personalized ads on Facebook."
50. Major Jessica Dawson, "Microtargeting as Information Warfare," *The Cyber Defense Review* 6, no. 1 (2021), 63-80.
51. Ibid.
52. Jim Isaak and Mina J. Hanna, "User data privacy: Facebook, Cambridge Analytica, and Privacy Protection," *Computer* 51, no. 8 (2018), 56-59; Dawson, "Microtargeting as Information Warfare."
53. Dawson, "Microtargeting as Information Warfare," 72.
54. Lt Col Jarred Prier, "Commanding the Trend: Social Media as Information Warfare," *Strategic Studies Quarterly* 11, no. 4 (2017), 51.
55. Ibid., 52.
56. Ibid.
57. Rutland "A Military of Influencers."
58. "The U.S. Army in multi-domain operations 2028," Fort Monroe, VA: Army Training and Doctrine Command (2018), 3.
59. Irina Khaldrova and Mervi Pantti, "Fake News: The Narrative Battle Over the Ukrainian Conflict," *Journalism Practice* 10, no. 7 (2016), 891-901; Singer and Brooking, *LikeWar;* Antal, "The First War Won Primarily with Unmanned Systems".
60. Krulak, *The Strategic Corporal.*
61. Ibid.
62. Stringer, "Educating the Strategic Corporal".
63. Capt. Luke Klena, "Technical Signature management for Small Units," *Marine Corps Gazette,* May 2021 (2021).

NOTES

[64] Dasilva et al., “Securing 5G.”
[65] Ibid., 85.
[66] Singer and Brooking, *LikeWar;* Van Niekirk and Maharaj, “Mobile Devices and the Military.”
[67] Prier, "Commanding the Trend.”
[68] Patrikarakos, *War in 140 Characters.*
[69] Dawson, “Microtargeting as Information Warfare.”
[70] Ibid.

Deterrence Thru Transparent Offensive Cyber Persistence

Lieutenant Colonel Ryan Tate
Colonel Chad Bates

ABSTRACT

State-enabled cyber campaigns are achieving cumulative, strategic effects on the United States. A lack of transparency limits offensive cyber capabilities from affecting the cost-benefit decisions of malicious cyber actors. However, recent operations suggest the United States can positively attribute malicious cyber activities, impose significant consequences with offensive cyber force, and translate those actions into deterrence of specific malicious activities using public communication. Persistent, public disclosure is necessary for offensive cyberspace operations to deter malicious cyber activities, nested with US strategic guidance, and achievable based on recent cyberspace operations. Transparent Offensive Cyber Persistence combines persistence with post factum, public disclosure of the justification, targets, and impacts of offensive cyber force, exchanging information for deterrence credibility. This work evaluates its suitability, acceptability, feasibility, and risks. Transparent Offensive Cyber Persistence exploits the relative advantages of offense in cyberspace to impose costs directly on malicious cyber actors, compel targets to defend everywhere, dissuade other actors, set a legitimate narrative of consequences for unacceptable malicious cyber activities, and shape international norms.

The United States (US) is under constant attack from increasingly capable state-enabled malicious cyber actors. The Cybersecurity and Infrastructure Security Agency (CISA) reported cyber incidents cost the US economy $242 billion in 2018.[1] McAfee and the Center for Strategic and International

LTC Ryan Tate is assigned to Joint Force Headquarters – Cyber (Army) (JFHQ-C) with duty at US Central Command. He holds a Master's degree in Computer Science from Duke University and in Strategic Studies from the US Army War College. He commissioned at the United States Military Academy in 2003 and transferred to Cyber Operations in 2016. His tactical assignments include the 3rd Battalion, 7th Infantry Regiment and 4th Brigade Combat Team, 3rd Infantry Division, where he deployed in support of Operation Iraqi Freedom (OIF), and the 326th Combat Engineer Battalion and 101st Sustainment Brigade, 101st Airborne Division, where he deployed for OIF. He served as assistant professor of Computer Science at West Point, NY and training chief for the US Army Cyber School. Finally, he served as a cyber combat mission team lead and JFHQ-C J35/planning lead at US Army Cyber Command.

Studies (CSIS) assess most attacks originate from Russia, China, North Korea, and Iran who have symbiotic relationships with malicious cyber actors.[2] Cybersecurity alone is unable to deter these actors: the US must significantly raise their perceived costs. US National Cyber Strategy deters via "the imposition of costs through cyber and non-cyber means."[3] U.S. Cyber Command (USCYBERCOM) has substantial offensive cyberspace capabilities, but the nature of cyberspace has limited their deterrent value.

The US must re-evaluate how offensive cyber force complements deterrence strategy. Cyber deterrence studies from Congress, the Department of State (DOS), and Department of Defense (DoD) produced foundational recommendations grounded in theory and practice.[4] Yet, challenges such as attribution and the risk of compromise impede implementation. USCYBERCOM adopted the strategic concept of *cyber persistence* to continuously contest adversaries in cyberspace. General Paul Nakasone, Commander of USCYBERCOM and Director of the National Security Agency (NSA), said that strategic effects "come from the use – not the mere possession – of cyber capabilities."[5] USCYBERCOM's persistence concept and recent offensive cyberspace operations illuminate new options for offensive cyber capabilities in deterrence. Scholars debate whether cyber deterrence is feasible and argue USCYBERCOM persistence is inherently defensive, but deterrence is central to US strategy and malicious cyber actors persist in their own offensive campaigns against the US. How can offensive cyber persistent engagement complement US cyber deterrence strategy?

Persistent, public disclosure is necessary for offensive cyberspace operations to deter malicious cyber activities, nested with US strategic guidance, and achievable based on recent cyberspace operations. The concept of *transparent offensive cyber persistence* combines cyber persistent engagement with calculated, post factum disclosure of operations information to

COL Chad Bates currently serves as faculty at the US Army War College in the Center for Strategic Leadership. COL Bates previously served as the Special Assistant to the Commanding General, US Army Cyber Command (ARCYBER), focusing on the readiness and training of ARCYBER's work force and served as the Deputy G-35/7 within the headquarters. He is currently a Cyber officer, but in 1995 he began his military career as a field artillery officer and in 2005 transferred to become a simulation operations officer (FA57) focusing on the field of modeling & simulation (M&S) and data science. He earned his PhD from George Mason University specializing in Earth systems and Geospatial Information Science, with a focus on spatial analysis and work process improvements. He earned a BS from the United States Military Academy, double Master's degrees from Webster University, and an additional Master's degree from the Naval War College.

influence the cost-benefit decisions of malicious cyber actors. This will shape international behavior by deterring the scope and aggressiveness of malicious cyber activities and encouraging like-minded allies to act in kind. Transparent offensive cyber persistence is based on deterrence theory, intragovernmental recommendations for cyber deterrence, scholarship, and observations from US and European law enforcement responses to malicious cyber activities, including US elections security interference, DarkSide, Trickbot, and Emotet. This work describes the strategic problem of malicious cyber activities, a framework for cyber deterrence with offensive cyberspace capabilities, US strategic guidance, and the concept of transparent offensive cyber persistence and then analyzes this concept and its implications.

THE STRATEGIC PROBLEM OF MALICIOUS CYBER ACTIVITIES

State and non-state actors employ cyber activities to subvert US power and asymmetrically erode US competitive advantages. Emily Goldman argues that the US is facing a crisis, losing ground in cyberspace as the volume, diversity, and sophistication of threats increases and shifts from exploitation to disruptive and destructive attacks.[6] State-enabled malicious cyber activities include espionage of intellectual property, sanctioned cybercrime to fund illicit activities and degrade strategic competitors, covert influence campaigns, and disruptive attacks on critical infrastructure. General Nakasone describes the stakes:

> Today peer and near-peer competitors operate continuously against us in cyberspace. These activities are not isolated hacks or incidents, but strategic campaigns. Cyberspace provides our adversaries with new ways to mount continuous, nonviolent operations that produce cumulative, strategic impacts by eroding U.S. military, economic, and political power without reaching a threshold that triggers an armed response.[7]

Operating costs and risks for malicious cyber activity are low while pay-offs are substantial. British consulting firm Deloitte estimated monthly cyber-criminal enterprise operating costs for a campaign with multiple tools falls between $544 and $3,796.[8] Conversely, the Federal Bureau of Investigation (FBI) calculated $4.1 billion in thefts from the American public in 2020, averaging over $5,000 each incident.[9] Commercialization trends make more tools more available at lower costs. But malicious cyberspace activity benefits from more than cost-efficiency. Chris Demchak explains the design of cyberspace provides malicious cyber actors five advantages: choice of *scale*, ability to act from any *proximity,* access to tools with desired *precision,* surprise and reuse inherent in the *deception of tools*, and the ability to avoid retaliation from *opaqueness in origins*.[10] FBI Director Christopher Wray said "we've got to change the cost-benefit calculus of criminals and nation-states who believe they can compromise US networks, steal US financial and intellectual property, and hold our critical infrastructure at risk, all without incurring any risk themselves."[11] The US can raise costs using offensive cyberspace operations.

CYBER DETERRENCE FRAMEWORK

Deterrence theory implies the threat of consequences will discourage actors from conducting malicious cyber activities against the US. Joint doctrine explains deterrence will "prevent adversary action through the presentation of a credible threat of counteraction."[12] Offensive cyber forces – USCYBERCOM – may deter malicious cyber actors by creating the expectation that retaliatory costs will exceed the benefits of malicious cyber activities. Intragovernmental recommendations for such a strategy have emerged over the past several years.

Congressional, DOS, and DoD advisory groups published recommendations for offensive cyber deterrence. The 2020 US Cyberspace Solarium Commission concluded cyber deterrence requires clear communication of consequences, costs that outweigh perceived benefits, credibility of capability and resolve, escalation management, the ability to attribute, and a policy for when to "voluntarily self-attribute cyber operations ... for the purposes of signaling capability and intent to various audiences."[13] DOS stressed malicious cyber actors must be certain they will face consequences and the need for a range of swift, transparent consequences for significant cyber incidents combined with tailored public and private communications, improved attribution, direct targeting of cyber actors, interagency planning to manage escalation, and coordinated reprisal with international partners.[14] DoD's 2017 Task Force on cyber deterrence proposed tailored, scalable deterrence campaigns of countervailing costs targeting what malicious cyber actors value using multiple instruments of power, explicit or implicit (by precedent) communication of the capability and will to respond, investments in attribution, and risk management of unintended effects, escalation, tool compromise, and other policy objectives.[15] This Task Force predicted deterrence posture will lead to cyber norms and declaratory policies important for international legitimacy, a better alternative to cyber arms races. Government recommendations encapsulate many of the underlying theories and challenges debated among scholars.

Scholars debate the feasibility of deterrence in cyberspace below the use-of-force threshold and articulate consistent themes on what cyber deterrence must address. Nye says cyber deterrence depends on perception, must address attribution, uncertainty, and escalation risks, and should consider costs in terms of entanglement and norms.[16] Goodman contends real-world examples demonstrate cyber deterrence is viable but concedes challenges include attribution, contestability (resulting from anonymity), scalability, a lack of reassurance, escalation, and clear signaling.[17] Conversely, Fischerkeller and Harknett argue the uniqueness of cyberspace makes deterrence infeasible below the use-of-force threshold, observing that continuous interactions encourage stable, agreed competition.[18] Taddeo reasons deterrence is limited by the dynamic, ambiguous nature of cyberspace conflict regarding attribution, credible signaling, escalation, uncertainty of effects, and proportionality.[19] Goldman says deterrence theory no longer explains continuous cyber engagement because there is a paradigm shift underway demanding development of persistence concepts.[20] Attribution, credibility, clear communication, scalability, environmental uncertainty, misperceptions, escalation risk, risks of compromise, unintended effects, and the question of norms are themes pervading scholarship debate on cyber deterrence. This intersection of government and scholars' recommendations provides a useful framework.

Effective deterrence requires capability, credibility, and communication. Capability is the power to project targeted, proportionate, and scalable cyberspace effects that impose significant costs. Credibility means malicious cyber actors believe there is capability and the resolve to use it. Communication is the mechanism to clearly signal intent to impose consequences for specific malicious cyber activities (below the use-of-force threshold) to target audiences.

Critical enabling capabilities are attribution, intelligence, and operations capacity.[21] Attribution is the ability to trace malicious cyber activities to a malicious cyber actor in sufficient degree to enable targeted reprisal, despite obfuscation and anonymity in cyberspace. Intelligence support enables cyberspace attribution, assessments of effects and reactions, and identification of malicious cyber actor interests and perceptions. Operations capacity implies the ability to plan, employ capabilities, and communicate to influence malicious cyber actor decisions, while mitigating risk and building international support and legitimacy.

The primary challenges, or risks, of cyber deterrence are compromise, unintended effects, and escalation. Compromise is the unintended disclosure of sensitive cyberspace capabilities and vulnerabilities or intelligence sources and methods. The inherent uncertainty and volatility of cyberspace makes operations susceptible to unpredictable effects and both ambiguity and manipulation of perception. Escalation includes unintended adversary responses that intensify conflict. Transparent offensive cyber persistence addresses each component of this model to raise expected costs for malicious cyber actors while nesting within US strategy.

A STRATEGIC APPROACH

President Biden's Interim National Security Strategic Guidance identified a national priority to "deter and prevent adversaries from directly threatening the United States and our allies."[22] His guidance describes malicious cyber actors held accountable through proportionate costs and, with allies and partners, shaped global norms in cyberspace.[23] The 2018 National Cyber Strategy explains that the "United States will formalize and make routine how we work with like-minded partners to attribute and deter malicious cyber activities with integrated strategies that impose swift, costly, and transparent consequences when malicious actors harm the United States or our partners."[24] In summary, a strategic objective for offensive cyber deterrence is: a transparent system of US allies and partners that imposes proportionate consequences on malicious cyber actors to reinforce and shape global norms in cyberspace.

In practice, the US has imposed swift, costly, and transparent consequences outside of cyberspace for certain malicious cyber activities. The Department of Justice (DOJ) recently announced an indictment of four Chinese nationals for malicious cyber activities targeting the US and its allies.[25] In April 2021, the Department of Treasury (USDT) retaliated for the SolarWinds attack with broad financial prohibitions on specific companies and individuals in the Russian defense and technology sector.[26] Similarly, reprisals against Russian cyber-enabled interference in the 2018 and 2020 US elections included criminal indictments disclosing significant intelligence on Project Lakhta and economic designations against the Internet Research Agency that revealed 15 names and specific activities.[27] US economic and legal reprisals divulged surprising details on the individuals, companies, and specific activities of malicious cyber actors.[28] This suggests that without compromising sensitive intelligence, the US can declassify and release sufficient information to attribute malicious cyber actors and describe their activities publicly. Yet, there are few public details of USCYBERCOM's offensive actions to impose costs on malicious cyber actors.[29]

USCYBERCOM does not discuss offensive cyberspace operations details. According to General Nakasone, cyber persistence empowers USCYBERCOM "to compete with and contest adversaries globally, continuously, and at scale, engaging more effectively in the strategic competition that is already under way."[30] General Nakasone's 2019 statement to the Senate Armed Services Committee explained USCYBERCOM imposed costs and "changed [Russia's] risk calculus for future operations."[31] In 2020, the Director of National Intelligence declassified intelligence assessing Russia "did not make persistent efforts to access election infrastructure, such as those made by Russian intelligence during the last US presidential election."[32] A defense article reported USCYBERCOM conducted over 2,000 operations defending the 2020 elections.[33] This indicates US cyberspace operations deterred specific malicious cyber activities targeting the elections, but the contribution of offensive cyber capabilities remains classified.

In contrast to announcements from DOJ and USDT, there was insufficient detail to understand the impacts and targets of offensive cyberspace operations defending US elections. One reason to limit transparency in cyberspace operations is to minimize the chance of revealing intelligence or capability. But limited transparency also restricts information malicious cyber actors need to recognize the threat that US cyberspace capabilities pose to their interests. Despite the secrecy, the scale, and stated successes of USCYBERCOM operations provide two important observations. The first is that USCYBERCOM can design and deliver effects with offensive cyber capabilities without risking, or with acceptable risk of, the exposure of sensitive tools or methods. The second is that USCYBERCOM's concept of persistent engagement has the power to generate multiple options to impose costs on malicious cyber actors in cyberspace. Given such a capability, how important is transparency?

Transparency enables the communication required for deterrence credibility. Transparency via public disclosure attributes specific malicious cyber activities and describes their consequences, communicating a clear threat for unacceptable behavior. This message demonstrates the US ability to impose significant costs on malicious cyber actors and the resolve to respond to certain types of malicious cyber activities. This basic concept is built on the framework of deterrence theory, government recommendations, and scholarship precepts. Not only is offensive cyberspace operations transparency achievable but, when executed persistently, it builds legitimacy and shapes global norms consistent with US strategic guidance.

TRANSPARENT OFFENSIVE CYBER PERSISTENCE

Transparent offensive cyber persistence is a method to complement US cyber deterrence strategy with offensive cyberspace operations. Its two driving mechanisms are: (1) disclosure (i.e., transparency): post factum, public announcements stating which activities elicited reprisal, the specific targets with their justification, and the effects of the operation; and (2) persistence: an offensive cyberspace operation targeting malicious cyber actors' interests (e.g., cyberspace assets) to impose costs appropriate for proportionate reprisal.

Disclosure exchanges information for the credibility of capability and will. Publicly providing declassified information creates transparency that demonstrates the imposition of steep consequences for certain malicious activities. Transparency supports legitimacy by connecting the evidence of proportionate, targeted strikes to the culpability of specific actors or assets and their activities which elicited the response. Disclosure is essential to build deterrence credibility in a domain of impunity, to demonstrate legitimate reprisal for unacceptable activities, and to shape international norms.

Cyber persistence is USCYBERCOM's concept of continuous engagement to shape malicious cyber actor behavior. Persistence creates credibility in the US resolve to respond to cyber actors directly in cyberspace through consistent action. However, persistence alone has marginal influence on malicious cyber actor decision-making because of the limited observability inherent in cyberspace. Disclosing cyberspace effects unambiguously communicates capability with intent and generates deterrence from persistent engagement.

Persistence with transparency will clearly communicate the high costs the US will impose in response to specific malicious cyber activities and shape international behavior. Consistently focusing on specific malicious cyber activities that threaten national interests, such as attacks on critical infrastructure or the integrity of elections, communicates which activities are most unacceptable.[34] This approach affords the ability to minimize compromise, escalation, and misperception and for consideration of information trade-offs in advance of an operation.

ANALYSIS: SUITABILITY, ACCEPTABILITY, FEASIBILITY, AND RISK

This section illustrates how the capability, credibility, and communication of transparent offensive cyber persistence shapes a transparent system of US allies and partners that imposes proportionate consequences on malicious cyber actors to reinforce and shape global norms in cyberspace. It examines the risks of compromise, unintended effects, and escalation, including a brief discussion of implementation risk. It also reviews repercussions for ethics, interagency and international partnerships, and USCYBERCOM's attribution, intelligence, and planning abilities.

Suitability

Cyberspace capabilities are capable of imposing costs that reverse the cost-benefit balance of malicious cyber activities. CISA reported median per-incident cyber damages range from $56,000 to $1.9 million including immediate expenses, lost revenues, and disruptions to business function.[35] The expectation of reprisal at this scale would provide a powerful disincentive for certain malicious cyber activities.[36] General Nakasone lauded USCYBERCOM's ability to effectively degrade malicious cyber actors and achieve decisive results.[37] Cyber-attacks disrupt operations, impose direct damages, compel expensive recovery and replacement measures, and damage reputations (e.g., forcing cover-ups). But what matters for deterrence is the expectation of facing those consequences.

Demonstrations of offensive cyber capability must overcome their inherent uncertainty, anonymity, and obfuscation to signal capability and resolve. Evan Montgomery's research on emerging military technologies with limited observability suggests capability employment is the most unambiguous way to signal a threat.[38] Recent law enforcement operations demonstrate transparency can extract deterrence credibility from offensive cyber capabilities. FBI and Europol cyberspace actions accompanied with public announcements generated a deterrent effect and enabled the voluntary coordination of cybersecurity partners to collectively raise costs for Trickbot, Emotet, and Darkside.[39]

A sophisticated operation in late 2020 reportedly disrupted Trickbot, a massive malware platform enabling "top-tier cybercriminals" to harvest financial data since 2016.[40] Malwarebytes reported a 68% percent reduction in Trickbot activity since the operation.[41] Researchers assessed only short-term disruption and concluded meaningful deterrence would require "novel solutions" targeting the malicious cyber actors' own assets to include releasing information about the actors and aggressive targeting of Trickbot infrastructure.[42] This implies strong deterrence requires costs exceeding temporary deactivation – what USCYBERCOM can deliver. USCYBERCOM reprisal is necessary to deter resilient actors who have benefitted from years of state sponsorship and success. Europol approached this threshold in early 2021.

In January 2021, Europol announced actions across eight countries that severely disrupted the cyber infrastructure of Emotet, a notorious access vector for state-enabled actors.[43] As a disrupter, Emotet may have affected 19% of global networks since 2014 and recently enabled successful critical ransomware attacks against hospitals and the mid-2020 targeting of US state and local governments.[44] Security firm Checkpoint assessed that Europol's operation caused an 80% reduction in infections and 40% decrease in control communications.[45] Researchers reported that as a result Emotet became "pickier about who they target" after unprecedented adjustments.[46] Europol's operation demonstrates significant costs can have a deterrent effect on the scope and scale of malicious cyber activities.

In May 2021, Russian cybercriminal group DarkSide conducted a successful ransomware attack against Colonial Pipeline, operator of the largest US oil pipeline. One month later, DOJ announced an FBI cyber operation recaptured $2.3 million directly from DarkSide's cryptocurrency accounts, declaring, "We will continue to target the entire ransomware ecosystem to disrupt and deter these attacks."[47] Reportedly, DarkSide suffered infrastructure disruption and announced it would stop its ransomware-as-a-service program and avoid public targets, as affiliates began to shun its services.[48] Trickbot, Emotet, and DarkSide reprisals illustrate how to transparently strike back in cyberspace, imposing costs and influencing actors' decisions.

Despite Trickbot, Emotet, and DarkSide resilience, law enforcement actions reduced the scope and scale of post-recovery activities. FBI and Europol announcements informed affiliated actors they can and will be subjected to cyberspace force. When the FBI announced it targeted DarkSide, there was rapid behavior change and distancing from DarkSide affiliates to avoid further costs.[49] In each case, public disclosure demonstrated resolve to impose consequences with offensive cyber capabilities, the costs those actions imposed, and the specific activities that precipitate them. Stronger deterrence requires costs that exceed temporary disablement. USCYBERCOM can impose those costs, and transparency is essential to clearly signal this intent.

Actions send a clear message of intention, and public disclosure is required to overcome perception challenges. Consistent disclosure of offensive cyberspace effects demonstrates the capability to attribute and impose costs combined with the resolve to respond to specific malicious cyber activities. Publishing the costs imposed in reprisal informs both actors responsible for targeted assets and parties likely to verify the incident.[50] Publicity creates reputational costs and reduces the chance for successful downplay, denial, and deception by forcing the adversary to contend with a competing narrative.[51] Establishing the initial account of events with first-hand knowledge from an operation provides the opportunity to link consequences to specific malicious cyber activity and document their scope and scale as legitimate reprisal. Persistent, public disclosure of USCYBERCOM offensive cyberspace reprisal would significantly increase the credibility of threats to actors who conduct cyber activities threatening national interests. It also sets conditions for behavioral norms in the international community.

Transparent offensive cyber persistence shapes global norms on responses to malicious cyber activities. Norms are common expectations about acceptable behavior. The World Bank reports voluntary government alliances develop global norms by bringing issues into public discourse when there is strong leadership, accountability, and legitimacy.[52] The use of relevant and credible evidence is crucial in building public and political support.[53] Public disclosure provides a transparent accounting of consequences and specific malicious activities, enabling global discourse on unacceptable behaviors and legitimate reprisal. Transparency builds trust with the US population and with allies. In his remarks to the European Union in 2019, Under Secretary of State Christopher Ford explained:

> ...normative understandings can help anchor the policy choices of responsible states in responding to bad behavior in cyberspace — which is what normative regimes do by way of compliance enforcement. This issue of consequences is an emerging area of cooperation between likeminded states, one that is called for in our National Cyber Strategy.[54]

Disclosure leads by example and demonstrates the acceptable use of offensive capabilities for deterrence, encouraging like-minded partners to contribute in-kind. A voluntary alliance of like-minded states imposing cyberspace consequences on malicious cyber actors will greatly improve deterrence.

The transparency of Trickbot and Emotet operations led to formulations of voluntary alliances to impose consequences. Microsoft coordinated global telecommunications providers and others to further disrupt Trickbot, securing court orders for direct disruption.[55] The FBI also continued reprisal, announcing additional indictments and releasing additional Trickbot information in June 2021.[56] Europol's Emotet reprisal also exemplified a security community coordinating to impose costs through cyberspace operations, law enforcement, and public announcements in eight countries. In his study on deterrence and norms in cyberspace, Tim Stevens argues norms-based "deterrence communities" increase the chance of deterrence and encourage the exercise of power, emphasizing that global normative frameworks not backed with credible force fail to deter non-state actors.[57] Publicly holding malicious cyber actors accountable facilitates cooperation from like-minded partners and an international system that curbs unacceptable behavior, cumulatively raising costs for malicious cyber actors. The United States can impose significant consequences with offensive cyber capabilities and translate those actions into deterrence with public disclosure to shape global norms.

Acceptability

It is possible to disclose the impact of an offensive cyber operation and release intelligence regarding targets without compromising tools, methods, and vulnerabilities or intelligence sources and methods. Conventional thinking is that disclosure compromises sensitive capabilities. However, FBI, Europol, and USDT announcements demonstrate disclosure can release details on costs imposed and specific targets while protecting methods and sources. Further, the volume of operations that USCYBERCOM conducted in its defense of the US elections indicate the command's ability to deliver noticeable effects without compromising capabilities. The plausibility of such information is extant in the accesses exposed during the observable effects of cyber-attack.[58] Therefore, post factum disclosure may reveal little more than the intelligence and access compromised already with reprisal. The aforesaid operations indicate it is possible to declassify enough intelligence for public attribution that legitimizes reprisal. The transparency of consistent public disclosure enables additional risk mitigation.

Transparency and persistence mitigate the risks of unintended effects. Cyberspace uncertainty causes unintended effects from misperceptions to unreliable timelines in executing operations. Even conventional military power is difficult to assess in advance of a conflict.[59] Persistence reduces this uncertainty through repetitive execution which builds experience in the execution and assessment of technical risks. Public disclosure communicates directly to target and international audiences the intended effects, targets of an operation, outcomes, and which activities provoked reprisal. Consistent disclosure demonstrates the intent to deliver targeted responses for certain malicious activities. Persistent demonstration reduces uncertainties regarding intentions externally and capabilities internally. Transparency limits misperception.

Consistent public disclosure provides a clear strategic message that reduces the risk of escalation. Timely disclosure connects cyberspace effects to malicious activity reprisal as (or before) adversary decision-makers learn of the strike. While disclosure attributes actions to the US, which aids attribution for malicious cyber actors, it also informs the international community. There is risk public exposure will incur accusations of misattribution or retaliation for reputational costs, in which case limited or private messaging may be more appropriate. Fischerkeller and Harknett note fears of escalation are unwarranted because malicious cyber activities already challenge national security and cyberspace competitive interaction stabilizes rather than escalates.[60] US actions during the Cold War suggest that creative uses of the military send strong signals not inherently escalatory.[61] Disclosing information provides the opportunity to ensure observers have sufficient data to assess US actions, including evidence of the justification, targets, and actions that reduce opportunities for misrepresentation.

Nothing in transparent offensive cyber persistence compromises the law of armed conflict or partnership practices at USCYBERCOM, which will continue to adhere to the principles of necessity, proportionality, and distinction. While there is debate about the military intervening in cybercriminal activity, there is precedence for intervention against non-state actors when national interests are threatened, such as counter piracy. Further, it is possible to conduct a cyberspace attack on malicious cyber actors' logical assets while minimizing collateral damage to legitimate but unwitting host services. For example, FBI and Europol operations remediated bot access, freeing unsuspecting users' devices from malicious control without harming their hosts. Close coordination with law enforcement will continue to be fundamental in ensuring compliance with international law regarding third parties. Finally, USCYBERCOM operates closely with interagency partners to vet targets and facilitate the review of intelligence equities before releasing any information, minimizing unintended effects. Transparency also encourages international partners to assess the actions of USCYBERCOM and shape their adoption as international norms.

Feasibility

USCYBERCOM operations provide sufficient capability to project targeted, proportionate, and scalable cyberspace effects of significant cost. Its offensive teams degrade, disrupt, destroy, or manipulate adversary information, information systems, and networks.[62] Michael Warner provides a describes the progression of USCYBERCOM's offensive capabilities, which disrupted Islamic State social media in 2016, as reaching a "new level" in scale and scope during the defense of US elections in 2018.[63] Actions defending the US elections in 2018 and 2020 demonstrate the ability to attribute malicious cyber activities and execute at scale.[64] General Nakasone affirmed USCYBERCOM's ability to impose tailored costs on malicious cyber actors.[65] USCYBERCOM operates a Cyber Mission Force of 6,200 servicemembers including offensive forces organized in Cyber National Mission Teams and Cyber Combat Mission Teams.[66] It has multiple operational headquarters providing planning and coordination capabilities.[67] General Nakasone reported the combined strength of USCYBERCOM and subordinate commands reached 238,000 personnel with other supporting elements across DoD.[68] Disclosure to extract deterrence from existing USCYBERCOM activities may require a modest increase in personnel to support this additional function. However, USCYBERCOM also draws from the resources of the US intelligence community to support messaging, effects, and attribution.[69] In summary, USCYBERCOM has the planning, intelligence, and teams capable of generating a range of effects suitable for imposing proportionate consequences and the resources to attribute malicious cyber activities.

Risk

Previous subsections discussed the primary risks of compromise, unintended effects, and escalation but implementation risk requires elaboration. Implementation risk includes under-delivering attribution or disclosure intelligence and under-producing cyber effects options required for reprisal. Early planning for public disclosure in most offensive cyberspace operations will maximize future options to enhance deterrence. A campaign of targeted reprisal actions will afford the best opportunity to exceed the cost-benefit thresholds of resilient malicious cyber actors. Some diversion of resources may be required to develop options for public disclosure. Not every opportunity will fit, but even periodic demonstration will provide important input to adversary decision-making. Interagency coordination to discover intelligence equities and political-military risk (e.g., conflict with other policy objectives) will remain an important factor in decisions to execute operations and declassify intelligence. Ultimately, greater risk lies in allowing malicious cyber actors to continue without imposing any significant costs their campaigns of malicious cyber activities that undermine US power.

IMPLICATIONS

Law enforcement and economic actions are powerful but fail to impose high enough costs to deter resolute cyber actors, particularly those outside jurisdictional reach. The FBI and Europol demonstrated consequences for major cybercriminals with public announcements detailing tangible costs and specific intelligence on the actors. They leveraged successful multi-national, public-private deterrence communities targeting cyber criminals without compromising sensitive intelligence or capabilities. Yet, cybercriminals have made fortunes and benefited from state support, building resiliency to legal and economic measures. Malicious cyber activities targeting critical infrastructure and other interests of national security demand higher consequences. When authorized, military power projection in and through cyberspace must severely degrade and destroy malicious cyber actors' assets. Such actions will send a strong message that malicious cyber activities threatening national and allied interests are not worthwhile. USCYBERCOM efforts may complement whole-of-government action, target the most significant malicious cyber actors, and significantly deepen costs for activities threatening critical infrastructure, elections, or other national interests.

Transparent offensive cyber persistence creates opportunities to achieve information advantage. Information advantage involves securing the initiative over other actors' behavior, situational understanding, and decision-making.[70] Using offensive cyber forces to impose consequences in a transparent manner exploits the relative advantages of offense in cyberspace, compelling targets to defend everywhere while discouraging other malicious cyber actors. Disclosure seizes the initiative, setting the narrative of legitimate reprisal coincidently with reprisal discovery. It provides a public account of US actions with evidence that malicious cyber actors must refute. Publicity reduces actors' abilities to construct alternate stories and downplay consequences. The costs of reprisal can be significant, as discussed above, and instigate substantial second order effects from the ensuing investigation and remediation.[71] Offensive cyber capabilities are the means to impose costs on actors less susceptible to diplomatic, law enforcement, or economic actions. Additionally, consistency in public disclosure provides the ability to privately message adversaries when it is crucial to demonstrate restraint or retain the option to escalate reputational costs. Furthermore, transparency encourages like-minded allies to also reinforce acceptable behavior in cyberspace. This will create a deterrence community with the resolve and capability to raise costs for malicious cyber actors.

CONCLUSION

Malicious cyber activities erode the competitive advantages of the US. Malicious cyber actors operate with impunity despite economic, legal, and diplomatic reprisals, leveraging symbiotic relationships with Russia, China, North Korea, and Iran. Historian and theorist Sir B.H. Liddell Hart said, "It is folly to imagine that the aggressive types, whether individuals or nations, can be bought off... but they can be curbed. Their very belief in force makes them more susceptible to the deterrent effect of a formidable opposing force."[72] The US can influence the cost-benefit decisions of such actors. It can lead like-minded states to new international norms that make cyberspace a costly domain to conduct certain malicious activities, such as infrastructure or elections attacks. Transparent offensive cyber persistence provides this deterrent framework, combining transparency and persistence.

Persistent, public disclosure is necessary for offensive cyberspace operations to deter malicious cyber activities, nested with US strategic guidance, and attainable based on recent cyberspace operations. Recent operations suggest the United States can positively attribute malicious cyber activities, impose significant consequences with offensive cyber capabilities, and translate those actions into deterrence with calculated public communication. Whole-of-government cyberspace operations demonstrate consistent action with disclosure is likely to deter the scope and aggressiveness of malicious cyber activities. Those operations and USCYBERCOM's limited public record also suggest the significant, additional costs of military power projection in cyberspace would greatly influence malicious cyber actor decision-making. Transparent offensive cyber persistence exchanges disclosure for credible cyber deterrence, supports US strategic ends suited to offensive cyber capabilities, mitigates the risks of compromise and escalation, and demands few additional resources. The primary mechanisms of persistence and disclosure implement key intragovernmental and scholarship recommendations for cyber deterrence while addressing the unique challenges of cyberspace. Consistent and transparent consequences will send a clear threat to malicious cyber actors, return the advantages of offense in cyberspace to US strategy, and facilitate new norms in cyberspace.

The concept of deterrence will remain as valid as the utility of influencing adversary decisions. The cumulative effect of malicious cyber activities already threatens national security.

Some argue persistent strategic competition in cyberspace tends toward stability below the use-of-force threshold, but it is unknown if malicious cyber actors are actively attempting to cross that threshold. The US must demonstrate offensive cyber capabilities not only to influence the cost-benefit analysis of malicious cyber actors. It must also advance discourse among allies, promote international norms, upgrade perceptions of US power, and force strategic dilemmas on malicious cyber actor enablers who seek cost-effective strategies to attack the United States.

DISCLAIMER

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

NOTES

1. Cybersecurity and Infrastructure Security Agency (CISA), *Cost of a Cyber Incident: Systematic Review and Cross-Validation* (Arlington, Virginia: CISA, October 26, 2020), 11, https://www.cisa.gov/sites/default/files/publications/CISA-OCE_Cost_of_Cyber_Incidents_Study-FINAL_508.pdf , CISA reported $242B was the median estimate in a range from $1B to over $7T.
2. Zhanna M. Smith and Eugenia Lostri, *The Hidden Costs of Cybercrime* (San Jose, California: McAfee, December 2020) 3, 27-32, https://www.csis.org/analysis/hidden-costs-cybercrime .
3. Donald J. Trump, *National Cyber Strategy of the United States of America* (Washington, DC: The White House, September 2018), 3.
4. Specifically, the 2020 US Cyberspace Solarium Commission, 2017 Defense Science Board Task Force on Cyber Deterrence, and the 2018 US Department of State Recommendations to the President.
5. Paul M. Nakasone, “A Cyber Force for Persistent Operations,” *Joint Force Quarterly 92, no. 1,* (2019): 12.
6. Jacquelyn Scheider, Emily Goldman, Michael Warner, Paul Nakasone, et al., *Ten Years In: Implementing Strategic Approaches to Cyberspace* (Newport Papers, 2020), 35-36; Dr. Emily Goldman served as a strategist working for the Department of State and USCYBERCOM.
7. Paul M. Nakasone, “A Cyber Force for Persistent Operations,” *Joint Force Quarterly 92, no. 1,* (2019): 10-11.
8. Deloitte Development LLC, *Black-market Ecosystem: Estimating the Cost of Pwnership,* (Deloitte, December 2018), 21, https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-black-market-ecosystem.pdf.
9. Federal Bureau of Investigation (FBI), *Internet Crime Report 2020* (Washington, DC: FBI, 2020), 3, https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf .
10. Scheider et al.*, Ten Years* ..., 49; Dr. Chris Demchak is the RDML Grace M. Hopper Professor of Cyber Security and Director, Center for Cyber Conflict Studies at the US Naval War College.
11. Federal Bureau of Investigation (FBI), “FBI Strategy Addresses Evolving Cyber Threat,” last modified September 16, 2020, https://www.fbi.gov/news/stories/wray-announces-fbi-cyber-strategy-at-cisa-summit-091620.
12. Joint Chiefs of Staff, *Doctrine of the Armed Forces of the United States, JP 1* (Washington DC: Joint Chiefs of Staff, 2017), I-15.
13. Sen. Angus King and Rep. Mike Gallagher, The United States Cyberspace Solarium Commission (final report, Washington, DC: US Congress, March 2020), 26-34, https://www.solarium.gov/; The 2019 National Defense Authorization act chartered the CSC to address the challenge of increasing cyberspace attacks on the United States.
14. Department of State, *Recommendations to the President on Deterring Adversaries and Better Protecting the American People from Cyber Threats* (Washington, DC: Department of State, May 2018), https://www.state.gov/wp-content/uploads/2019/04/Recommendations-to-the-President-on-Deterring-Adversaries-and-Better-Protecting-the-American-People-From-Cyber-Threats.pdf .
15. Department of Defense, *Final Report of the Defense Science Board (DSB) Task Force on Cyber Deterrence* (Washington, DC: Department of Defense Science Board, February 2017), 1-7, https://dsb.cto.mil/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf.
16. Joseph Nye, Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (2016): 44-71; Dr. Joseph Nye, Jr. is University Distinguished Service Professor at Harvard University.
17. Will Goodman, "Cyber Deterrence: Tougher in Theory than in Practice?" *Strategic Studies Quarterly* 4, no. 3 (2010): 102-135; Will Goodman advised Senator Patrick Leahy and the Assistant Secretary of Defense for Homeland Defense and Global Security.
18. Michael Fischerkeller and Richard Harknett, "Deterrence is Not a Credible Strategy for Cyberspace," Orbis 61, no. 3 (2017): 381-393; The authors’ concept of continuous interaction shaped USCYBERCOM’s concept of persistent engagement. Dr. Fischerkeller is a researcher in the Institute for Defense Analyses and Dr. Harknett is Professor and Dept. Head of Political Science at the University of Cincinnati.
19. Mariarosaria Taddeo, "The Limits of Deterrence Theory in Cyberspace," *Philosophy & Technology 31*, no. 3 (2018): 339-355; Mariarosaria Taddeo is Associate Professor and Senior Research Fellow, Oxford Internet Institute, University of Oxford.
20. Scheider et al., *Ten Years...*, 38-40.
21. Avoiding attribution and, in that, retribution is key for malicious cyber actors to preserve favorable cost-benefit tradeoffs for cyber activities.

NOTES

22. Joseph R. Biden, Jr., *Interim National Security Strategic Guidance* (Washington, DC: The White House, March 2021), 9.
23. Biden, *Interim National Security Strategic Guidance*, 18.
24. Trump, *National Cyber Strategy*, I, 21.
25. Department of Justice, "Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research" (Washington DC: Department of Justice, July 19, 2021), https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion.
26. Department of Treasury, "Treasury Sanctions Russia with Sweeping New Sanctions Authority" (press release, Washington, DC: Department of Treasury, April 15, 2021), https://home.treasury.gov/news/press-releases/jy0127.
27. Department of Justice Office of Public Affairs, "Russian National Charged with Interfering in U.S. Political System," last updated October 19, 2018, https://www.justice.gov/opa/pr/russian-national-charged-interfering-us-political-system; and "Treasury Targets Russian Operatives over Election Interference, World Anti-Doping Agency Hacking, and Other Malign Activities," last updated December 19, 2018, https://home.treasury.gov/news/press-releases/sm577.
28. Department of Treasury, "Sanctions Related to Significant Malicious Cyber-Enabled Activities," accessed September 4, 2021, https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information/sanctions-related-to-significant-malicious-cyber-enabled-activities and Department of Justice, "search results for cyber indictment," accessed September 4, 2021, https://search.justice.gov/search?utf8=%E2%9C%93&affiliate=justice&sort_by=&query=cyber+indictment.
29. USCYBERCOM defensive actions provide substantial detail; See USCYBERCOM Public Affairs, "US Cyber Command, DHS-CISA release Russian malware samples tied to SolarWinds compromise," last updated April 15, 2021, https://www.cybercom.mil/Media/News/Article/2574011/us-cyber-command-dhs-cisa-release-russian-malware-samples-tied-to-solarwinds-co/.
30. Nakasone, "A Cyber Force for Persistent Operations," 12.
31. Hearing before the Senate Committee on Armed Services, 116th Congress, February 14, 2019 (statement of General Paul Nakasone, Commander of US Cyber Command).
32. *Foreign Threats to the 2020 US Federal Elections*, National Intelligence Council (declassified report, Washington, DC: Director of National Intelligence, March 20, 2021), 3, https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2021/item/2192-intelligence-community-assessment-on-foreign-threats-to-the-2020-u-s-federal-elections .
33. David Verdun, "Cybercom's Partnership With NSA Helped Secure U.S. Elections, General Says," Department of Defense, last updated March 25, 2021, https://www.defense.gov/Explore/News/Article/Article/2550364/cybercoms-partnership-with-nsa-helped-secure-us-elections-general-says/.
34. Cyberspace reprisals are unlikely to deter all malicious activities, such as cyberspace espionage. USCYBERCOM strikes may optimally supplement law enforcement responses to maximize costs when malicious cyber activities threaten national interests.
35. Cybersecurity and Infrastructure Security Agency (CISA), *Cost of a Cyber Incident: Systematic Review and Cross-Validation* (Arlington, Virginia: CISA, October 26, 2020), 9-16, https://www.cisa.gov/sites/default/files/publications/CISA-OCE_Cost_of_Cyber_Incidents_Study-FINAL_508.pdf; CISA also mentions that full costs are likely underrepresented in some datasets.
36. Deloitte, *Black-market Ecosystem*, 21, reported monthly cyber-criminal operating costs between $544 and $3,796.
37. Nakasone, "A Cyber Force for Persistent Operations," 11.
38. Evan Braden Montgomery, "Signals of Strength: Capability Demonstrations and Perceptions of Military Power," *Journal of Strategic Studies* 43, no. 2 (2020): 317-324; Montgomery also suggests demonstrating low observability, emerging capabilities is required to upgrade estimates of US power. Evan Montgomery is a Senior Fellow and Director of Research and Studies at the Center for Strategic and Budgetary Assessments in Washington, D.C.
39. Europol is the European Union Agency for Law Enforcement Cooperation; For additional information, see https://europa.eu/european-union/about-eu/agencies/europol_en.
40. Krebs on Security, "Attacks Aimed at Disrupting the Trickbot Botnet," last modified October 2, 2020, https://krebsonsecurity.com/2020/10/attacks-aimed-at-disrupting-the-trickbot-botnet/; The unattributed operation neutralized bots and directly degraded control servers.

NOTES

41. Adam Kujawa et al., *State of Malware 2021,* Report (Santa Clara, CA: Malwarebytes Inc., 2021), 18, https://www.malwarebytes.com/resources/files/2021/02/mwb_stateofmalwarereport2021.pdf.
42. Intel471, “Recent Trickbot Disruption Operation Likely to Have Only Short-Term Impact,” last modified October 13, 2020, https://intel471.com/blog/trickbot-disruption-microsoft-short-term-impact/ .
43. Europol, “World’s Most Dangerous Malware Emotet Disrupted Through Global Action,” Press Release, last modified January 27, 2021, https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action .
44. Check Point, Ltd., “Collaborative Global Effort Disrupts Emotet, World’s Most Dangerous Malware,” last modified 28 January, 2021, https://blog.checkpoint.com/2021/01/28/collaborative-global-effort-disrupts-emotet-worlds-most-dangerous-malware/; state and local government targeting is from CISA, “Emotet Malware,” National Cyber Awareness System Alert AA20-280A, last modified October 24, 2020, https://us-cert.cisa.gov/ncas/alerts/aa20-280a.
45. Check Point, Ltd., “Collaborative Global Effort.”
46. Kujawa et al., *State of Malware* 2021, 18.
47. Department of Justice Office of Public Affairs, “Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside,” last updated June 7, 2021, https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside; Colonial Pipeline paid 75 bitcoins to Darkside as ransom to restore critical data.
48. Intel471, “The Moral Underground? Ransomware Operators Retreat After Colonial Pipeline Hack,” last updated May 14, 2021, https://intel471.com/blog/darkside-ransomware-shut-down-revil-avaddon-cybercrime.
49. There are more examples publicly available; for example, FBI cyber and non-cyber actions targeting Game Over Zeus in 2014 caused it to “never return to its previous scale” as described in https://www.secureworks.com/research/evolution-of-the-gold-evergreen-threat-group; for more recent operations, see https://www.justice.gov/opa/pr/department-justice-launches-global-action-against-netwalker-ransomware.
50. Parties likely to verify a reprisal include third party cybersecurity researchers and malicious cyber actors’ affiliates and sponsors.
51. Nye, "Deterrence and Dissuasion in Cyberspace," 48, 60.
52. Johanna Martinsson, “Global Norms: Creation, Diffusion, and Limits” (World Bank: Washington, DC, 2011), 4, 8, https://openknowledge.worldbank.org/handle/10986/26891.
53. Martinsson, Global Norms, 22.
54. Christopher Ford, “Rules, Norms, and Community: Arms Control Discourses in a Changing World,” (remarks of Dr. Ford, Under Secretary of State for Arms Control and International Security, to the European Union in Brussels, December 13, 2019) https://2017-2021.state.gov/rules-norms-and-community-arms-control-discourses-in-a-changing-world/index.html.
55. Symantec, “Trickbot: U.S. Court Order Hits Botnet’s Infrastructure,” last modified October 12, 2020, https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/trickbot-botnet-ransomware-disruption.
56. US Department of Justice, “Latvian National Charged for Alleged Role in Transnational Cybercrime Organization,” last modified June 4, 2021, https://www.justice.gov/opa/pr/latvian-national-charged-alleged-role-transnational-cybercrime-organization.
57. Tim Stevens, "A cyberwar of ideas? Deterrence and norms in cyberspace." Contemporary Security Policy 33, no. 1 (2012): 148-170, 156-157; Dr. Tim Stevens is Senior Lecturer in Global Security at King’s College London.
58. Reprisal target system administrators would likely identify exposed accesses as a plausible source of information but may also downplay or deny the extent of any network penetration.
59. Evan Braden Montgomery, “Signals of Strength,” 316.
60. Michael Fischerkeller and Richard Harknett, "Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation," *The Cyber Defense Review* (2019): 267-287.
61. Tami Davis Biddle, “Coercion Theory: A Basic Introduction for Practitioners,” accessed June 14, 2021, https://tnsr.org/2020/02/coercion-theory-a-basic-introductionfor-practitioners/.
62. Joint Chiefs of Staff, *Cyberspace Operations, JP 3-12* (Washington, DC: Joint Chiefs of Staff, 2018), II-7.

NOTES

63. Michael Warner, "US Cyber Command's First Decade," *A Hoover Institution Essay, Aegis Series Paper*, no. 2008 (2020): 14-18.
64. Hearing before the Senate Committee on Armed Services, 117th Congress, March 25, 2021 (statement of General Paul Nakasone, Commander of US Cyber Command).
65. Hearing before the House Committee on Armed Services Subcommittee on Intelligence and Emerging Threats and Capabilities, 116th Congress, March 4, 2020 (statement of General Paul Nakasone, Commander of US Cyber Command).
66. "Cyber Mission Force Achieves Full Operational Capability," USCYBERCOM Public Affairs, last modified May 17, 2018, https://www.cybercom.mil/Media/News/News-Display/Article/1524492/cyber-mission-force-achieves-full-operational-capability/.
67. USCYBERCOM Public Affairs, "A Command First: CNMF trains, certifies task force in full-spectrum operations," last updated June 7, 2021, https://www.cybercom.mil/Media/News/Article/2647621/a-command-first-cnmf-trains-certifies-task-force-in-full-spectrum-operations/.
68. Posture Statement of General Paul M. Nakasone, Commander, United States Cyber Command before the 117th Congress Senate Armed Services Committee, March 25, 2021 (testimony of General Paul Nakasone, Commander of US Cyber Command).
69. Warner, "US Cyber Command's First Decade," 9; and Department of State, "Joint Statement on Advancing State Behavior in Cyberspace" (joint statement, Washington, DC: Department of State, September 23, 2019), https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/.
70. Information advantage is an emerging doctrinal concept. This definition is based on an Army strategic leader's presentation to the US Army War College on November 9, 2021.
71. Based on consensus reached during the author's operational planning with senior leaders in USCYBERCOM and partner forces from January – April 2021.
72. Basil H. Liddell Hart, Part IV, "Fundamentals of Strategy and Grand Strategy," in Strategy, 2nd ed. (New York: Penguin, 1991), 359.

Ethical Assessment of Russian Election Interference

Using the Framework of Just Information Warfare

Second Lieutenant Joseph Zuccarelli
Second Lieutenant Nico Manzonelli

ABSTRACT

The consistent development of information and communication technologies poses new ethical challenges for military leaders and policymakers in the fifth domain of warfare–cyberspace. This article engages a relatively new ethical framework known as Just Information Warfare (JIW) to assess one of the highest profile instances of information warfare in recent years–Russian interference in the 2016 US presidential election. First, we define information warfare and describe how concepts from two well-known ethical theories–Just War Theory and Information Ethics–merge to create JIW. Next, we analyze Russian military officers' 2016 election interference efforts and the corresponding US response through a JIW lens. Finally, we offer three key takeaways from our analysis that warrant further thought.

INTRODUCTION

US military doctrine revolved around four fundamental domains of warfare, land, air, sea, and space, until 2010 when cyberspace, a fifth domain, was officially added.[1] The Department of Defense (DoD) defines cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunication networks, computer systems, and embedded processors and controllers."[2] Over the past decade, the expansion of cyberspace has forced military leaders to consider the ability to control, disrupt, or manipulate an adversary's informational infrastructure as important as traditional measures of military strength. Information and communication technologies

Joseph Zuccarelli, a Draper Laboratory Scholar pursuing his MS in Data Science at Harvard University, recently graduated from the United States Military Academy with a Mathematical Sciences major and a Cyber Security minor. While pursuing his undergraduate degree, Joseph worked as a Senior Writing Fellow in the West Point Writing Program and focused his undergraduate studies on researching applied mathematics and technical communication. His internship experience includes work with the Florida Panthers sports analytics team studying National Hockey League data. Joseph is a U.S. Army Second Lieutenant and will serve in the Cyber branch following completion of his studies at Harvard. joseph_zuccarelli@g.harvard.edu

increasingly prove to be useful technologies for waging war and are revolutionizing military affairs. In addition to military leaders, ethicists and policymakers also are now compelled to consider how to apply or adapt traditional ethical theories to this fifth domain.

INFORMATION WARFARE

Information Warfare (IW), properly defined, entails the use of information and communication technologies to breach an adversary's informational infrastructure in order either to disrupt it, or to obtain relevant data concerning the adversary's resources, military strategies, etc.[3] IW differs from traditional warfare in basic respects. Traditional warfare is necessarily violent and involves the sacrifice of human lives and kinetic damage to both military and civilian infrastructures. In contrast, IW enables entities to damage and degrade adversaries without physical force or violence. While traditional warfare is generally limited to human beings and physical objects, IW introduces two new dimensions: artificial and non-physical entities. Although the lack of violence and the overall non-destructive nature of IW seems to make it desirable from an ethical and political perspective, IW's disruptive nature can severely damage contemporary societies' information infrastructure and lead to dangerous outcomes. Consider the following examples from the past decade.

In June 2015, the US Office of Personnel Management (OPM) suffered one of the largest breaches of government data in US history after a data breach compromised an estimated 21.5 million records. Among the compromised records were highly sensitive Standard Form 86s (SF 86 – Questionnaire for National Security Positions), which are used to document background investigations of prospective US government employees and include personally identifiable information like Social Security numbers, names, birthdates, places of birth, and addresses. While the motive behind the breach remains unclear, the overwhelming consensus

Nico Manzonelli, a MIT Lincoln Laboratory Military Fellow working in the Cyber Security and Information Sciences Division, is pursuing his MS in Data Science at Harvard University. A recent graduate from the United States Military Academy with a BS in Systems Engineering, Nico served as a Senior Writing Fellow in the West Point Writing Program and competed on Army's varsity wrestling team. In his undergraduate studies, he focused his research on data visualization, analytics, and natural language processing. His internship experience includes working with the National Basketball Association's Technology and Products Division. Nico is a U.S. Army Second Lieutenant and will serve in the Cyber branch following completion of his studies at Harvard. nicomanzonelli@g.harvard.edu

is that Chinese government-sponsored hackers presumably carried out the attack to compile a database of US government employees.[4]

In February 2022, Russia launched a full-scale ground invasion of Ukraine. Although this ongoing conflict entails the typical physical violence associated with traditional warfare, Russian-led IW operations aim to influence public opinion and damage Ukraine's information infrastructure via cyberattacks. Prior to invasion, Russia conducted a long-running misinformation campaign using state-sponsored media outlets and Kremlin-backed online personas to cast Ukrainians as the perpetrators of genocide against Russian speakers in eastern Ukraine. The twofold purpose of said misinformation campaign was to justify the invasion of Ukraine and to paint NATO-affiliated countries as aggressors in the conflict.[5] In addition to their misinformation campaign, Russia coupled cyber and kinetic military operations for their initial invasion and continue to coordinate cyberattacks to steal information and degrade Ukrainian capabilities.[6]

JUST WAR THEORY

Ethical analyses of war typically follow three main paradigms: Just War Theory (JWT), Pacifism, or Realism. JWT is an ethical framework studied by military leaders, ethicists, theologians, and policymakers that focuses on providing justifications for how and why wars are fought. Rather than use the framework to justify "good" military actions, JWT often serves as a structured method for assessing the morality of actions in war. Traditional JWT is divided into two sets of principles: *jus ad bellum* ("right to go to war")—the morality of initiating war, and *jus in bello* ("right conduct in war"), which focuses on the morality of conduct within a war,[7] as more fully described in the next two paragraphs.

Jus ad bellum typically consists of the following six principles: just cause, legitimate authority, right intention, reasonable prospects of success, proportionality, and last resort.[8] Just cause requires that the reason for going to war must be justified (e.g., self-defense). Legitimate authority indicates that only duly constituted public authorities are allowed to wage war. Right intention refers to the fact that the entity waging war must actually intend to achieve the established just cause, rather than use it as a pretext for achieving a wrongful end. Reasonable prospects of success requires that the entity waging war must have some reasonable probability of success. Proportionality indicates that the expected benefits of waging war must exceed its expected evils or harms. The sixth and final principle, last resort, requires that there is no less-harmful avenue to achieve the established just cause other than war.[9]

Jus in bello includes three basic principles: discrimination, proportionality, and necessity.[10] Discrimination requires that those involved in the conduct of war must always properly distinguish between military objectives and civilians, and limit attacks to military objectives. Proportionality requires combatants to ensure that collateral harm to civilians is not excessive in relation to the military advantage achieved by any act of war. Finally, necessity requires combatants to always use the least harmful means feasible in order to achieve any otherwise just military objective.[11]

As the nature of warfare has evolved to include IW, applying JWT principles to modern conflicts has become increasingly difficult. This issue mainly arises because JWT typically focuses on the use of force in physically violent warfare, and not the cyber domain, where IW engages abstract entities. The unconventional nonviolent property of IW complicates core JWT concepts such as harm, target, and attack. This challenge is widely discussed in existing literature.[12] The following two sections detail how philosophers address the shortcomings of JWT by introducing two additional ethical frameworks.

INFORMATION ETHICS

Information Ethics (IE) is an ethical approach that enables the analysis of moral issues from an informational perspective. IE follows from the consideration that internet and communication technologies have radically changed the context in which moral issues arise, requiring us to rethink the foundations upon which our traditional ethical positions are based.[13] Under IE, the moral value of an entity is determined by its contribution to the enrichment of the information environment. This environment, also referred to as the infosphere, includes all existing things, physical or non-physical, and the relations occurring among them.[14] If the infosphere seems all-encompassing, that's because it is. While biocentric ethics are based on the moral value of life and the negative value of suffering, IE is concerned with the moral value of existence.[15] In practice, this implies that the information environment includes a person, a person's computer, and the data on said computer and thus all have moral standing. The blooming or enrichment of the infosphere is considered the ultimate good, while its corruption or destruction is considered the ultimate evil. Any form of corruption or destruction of an entity in the information environment is referred to as entropy.[16]

Using the key terms defined in the previous paragraph, IE outlines four principles for evaluating individuals' contributions to the information environment.[17] These four principles are defined as follows:

1. Entropy should not be caused in the infosphere (null law);
2. Entropy should be prevented in the infosphere;
3. Entropy should be removed from the infosphere;
4. The flourishing of informational entities and of the whole infosphere should be promoted by preserving, cultivating, and enriching their properties.

These principles are fairly straightforward, which, when merged with those outlined by JWT, bring us to the final ethical theory discussed in this article–Just Information Warfare (JIW).

JUST INFORMATION WARFARE

As an ethical framework, JIW merges concepts from JWT with IE to establish necessary and sufficient criteria for waging IW.[18] JIW hinges on the following three principles defined below:

1. IW should be waged solely against entities that endanger or disrupt the well-being of the infosphere;
2. IW should be waged to preserve the well-being of the infosphere;
3. IW should not be waged solely to promote the well-being of the infosphere.

Adhering to the first principle renders the decision to resort to IW morally just. Under this principle, any entity that endangers or disrupts the well-being of the infosphere forfeits its basic rights to flourish or even exist within the infosphere and renders itself a morally just target under JIW. This principle empowers actors in the information environment to discriminate justly between proper and improper IW targets.[19]

The second principle gives other actors in the information environment a moral obligation to prevent any malicious actor from causing more entropy within the infosphere. In other words, IW waged to reestablish the status quo or mend a damaged infosphere is morally just under JIW. Under this principle, nation-state actors conducting IW should only be used as an active measure to reduce or prevent instances of entropy within the infosphere.[20]

The third and final principle indicates that IW waged to improve the prosperity of the information environment is never just. Under the theory of IE, IW is understood as a form of disruption. Therefore, by definition, IW is never desirable and should not be used a vehicle to foster the infosphere's prosperity. Instead, IW is only to be considered a necessary evil used to combat the uncontrolled increase of entropy within the infosphere.[21]

It is important to underscore that any actor waging IW must adhere to the principle of proportionality, which may differ from but logically tracts the concept of proportionality in the context of JWT. In both JWT and JIW, proportionality implies that the means of conducting warfare must not cause more harm than the military actions addressed or corrected through an instance of warfare.[22] However, while measuring relative use of force and collateral damage is more straightforward in traditional conflict, defining comparative entropy in the information environment is nuanced and beyond the scope of our analysis.

CASE STUDY: RUSSIAN 2016 ELECTION INTERFERENCE

Background

In 2016, the Republican ticket of Donald Trump and Mike Pence defeated the Democratic ticket of Hillary Clinton and Tim Kaine in what many consider one of the greatest upsets in US election history. Beyond this point, the 2016 US presidential election was also a significant instance of Russian election interference. Since 2016, details of Russian interference efforts have come out in drips and drabs, with information revealed in memoranda released by intelligence agencies, court documents filed by Special Counsel Robert Mueller, testimony from Trump associates, and investigative news reports.[23] In 2020, the Senate Intelligence Committee released its final report, a nearly 1000-page document that details Russia's aggressive IW tactics used to influence the outcome of the election.[24] The US Intelligence Community (IC) ultimately concluded that the Russian interference centered around three goals: damage the Clinton campaign, boost the Trump campaign, and sow distrust in American democracy overall. To accomplish their goals, Russian IW efforts focused on three basic tactics: probing state voter databases, hacking the Democratic campaign and its committees, and spreading false propaganda on social media.[25]

The IC concluded Russian hackers did not alter actual votes during the 2016 election, but evidence suggested pre-election attacks on voter registration systems in at least 21 states. Reports indicate that the hackers stole information on approximately 500,000 voters from an unnamed state's database, to include names, addresses, birthdates, driver's license numbers, and partial Social Security numbers. It remains unclear what the Russians did with this compromised information.[26]

Beyond their attacks on US voter registration systems, Russian hackers also successfully accessed several restricted Democratic campaign systems by sending phishing emails to various Clinton campaign staffers and volunteers. Camouflaged as Google security notifications, phishing allowed the hackers to access several notable campaign members' accounts, including chairman John Podesta, and steal tens of thousands of emails. The emails were then released during the run-up to election day to create repeated negative news cycles for the Clinton campaign. The hackers also used very similar tactics to attack the Democratic Congressional Campaign Committee and the Democratic National Committee.[27]

While the first two tactics described above are considered as traditional cyber-attacks, Russians also utilized digital influence operations to interfere with the election. As one of the more subtle IW approaches, Russian hackers developed troll factories (i.e., entities employing personas who post comments on social media reinforcing misinformation) and bots (i.e., programs that send out messages automatically in response to the appearance of a keyword) that incite division among the electorate. Prior to the election, Russia employed troll factories and bots to post controversial content divisively covering topics such as the Black Lives Matter movement, immigration, and gun control. There is also evidence of Russian groups buying and frequently posting political ads derisive of the Clinton campaign.[28]

In response to the findings on Russian election interference, the US government has taken steps to protect against foreign IW tactics and imposed punitive measures upon Russia. Immediately following the 2016 election, then Director of National Intelligence Dan Coats led the expansion and permanent establishment of "election-security task forces" at the FBI, DHS, NSA, and U.S. Cyber Command (USCYBERCOM).[29] In 2018, a federal grand jury indicted 12 Russian military intelligence officers for interfering with the 2016 election (see Figure 1).[30]

WANTED BY THE FBI

CONSPIRACY TO COMMIT AN OFFENSE AGAINST THE UNITED STATES; FALSE REGISTRATION OF A DOMAIN NAME; AGGRAVATED IDENTITY THEFT; CONSPIRACY TO COMMIT MONEY LAUNDERING

RUSSIAN INTERFERENCE IN 2016 U.S. ELECTIONS

Boris Alekseyevich Antonov

Dmitriy Sergeyevich Badin

Anatoliy Sergeyevich Kovalev

Nikolay Yuryevich Kozachek

Aleksey Viktorovich Lukashev

Artem Andreyevich Malyshev

Sergey Aleksandrovich Morgachev

Aleksandr Vladimirovich Osadchuk

Aleksey Aleksandrovich Potemkin

Ivan Sergeyevich Yermakov

Pavel Vyacheslavovich Yershov

Figure 1: Russian Officers Wanted by the FBI[31]

In 2019, the US issued economic sanctions against Russians involved with the Internet Research Agency, an organization that manipulates social media for misinformation purposes, as a warning against foreign interference in US elections.[32]

ANALYSIS

Russian Actions

When analyzing Russian election interference efforts from a JIW perspective, this clearly was an instance of unjust IW due to violations of principles I and II. Again, principle I limits just acts of IW to only those directed at entities that endanger or disrupt the well-being of the infosphere. There is no documented record of US-sponsored IW against Russia; the US has never acted tantamount to forfeit its rights within the infosphere, thereby targeting the 2016 election was morally unjust under JIW. Furthermore, principle II dictates that actors in the information environment only wage IW in order to preserve the infosphere's well-being. Having stolen sensitive US voter information, Russian hackers introduced an enormous amount of entropy to the infosphere. Additionally, by leaking campaign members' private emails and spreading major misinformation campaigns via bots or troll factories, Russian actions clearly disrupted the information environment. Such entropy-increasing actions seriously undermined the well-being of the infosphere and created chaos so as to further Russia's political agenda, which further qualifies Russian election interference as an unjust instance of IW.

US Actions

By analyzing the US response to the Russian election interference under the same framework, we conclude that US actions comported with JIW. Russia clearly forfeited its basic (i.e., principle I) rights in the infosphere, thereby exposing itself as a just target of IW. Indeed,the US, as a significant actor within the information environment, was morally obligated to counter Russia's efforts and prevent state-sponsored hackers from further perpetrating entropy in the form of IW. US leaders fulfilled this obligation by taking a defensive approach to IW. Consistent with principle II, the US response sought to reduce Russian IW-caused chaos within the infosphere, specifically with major steps to improve election-security and leveraging legal measures or economic sanctions to more effectively deter Russian IW. The most recent US presidential election perhaps serves as evidence that these efforts are working, as there were no major findings of successful IW attacks.

CONCLUSIONS

Ultimately, our work suggests three main takeaways. First, traditional ethical theories or frameworks do not often apply directly to the cyberspace realm. Second, election interference is becoming an IW vulnerability that democratic countries must safeguard against. Third, JIW provides a relatively new and useful ethical tool for analyzing instances of IW.

Analyzing IW through the lens of JWT confirms that cyberspace poses unique challenges in applying traditional ethical frameworks. As previously indicated, IW seldom involves physical violence, which renders gaging the proportionality of IW attacks and subsequent counterattacks more challenging. IW can include but does not require attack by uniformed soldiers, and countries often unofficially sponsor underground hacking groups, blurring the line between combatants and non-combatants. Attribution poses yet another hurdle in cyberspace warfare; hackers are extremely effective in terms of disguising themselves, making it hard even to identify potential targets of counter-IW.

Given the growing complexity of cyber-attacks, election interference is now an extremely relevant form of IW that countries must protect against. Elections form the basis of democratic legitimacy; therefore, it is essential that the citizens of democratic nations feel fully confident in their results. Countries such as the US are taking extra steps to defend against election interference, specifically by establishing election-security task forces. There also is a need to ensure that international law is kept current with the increasingly sophisticated technology that facilitates foreign election interference.

Indeed, JIW can serve as a useful tool for gaging the ethics of waging IW. Through using JIW to analyze the election interference and corresponding responses, we reveal that many ethical solutions exist in this space. For instance, the US could have undertaken other just actions in response to Russian election interference. The JIW framework is one helpful tool for government leaders and policymakers, who must continue to consider moral justifications for IW when enforcing international law.

DISCLAIMER

Views expressed here are those of the authors and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, or the Department of Defense.

NOTES

1. Charles H. Hall, "Operational Art in the Fifth Domain," Naval War College, Newport RI, Joint Military Operations Department (2011), https://apps.dtic.mil/sti/pdfs/ADA546255.pdf.
2. William E. Gortney, *Department of Defense Dictionary of Military and Associated Terms* (Washington D.C.: Joint Chiefs of Staff, 2010), https://apps.dtic.mil/sti/pdfs/AD1024397.pdf.
3. Edward L. Waltz, *Information Warfare Principles and Operations* (Norwood, Massachusetts: Artech House, Inc., 1998).
4. Stephanie Gootman, "OPM Hack: The Most Dangerous Threat to the Federal Government Today," *Journal of Applied Security Research,* vol. 11, no. 4 (2016), 517-525, https://www.tandfonline.com/doi/full/10.1080/19361610.2016.1211876.
5. Maria Snegovaya, "Putin's Information Warfare in Ukraine," *Soviet Origins of Russia's Hybrid Warfare, Russia Report*, No. 1 (2015), 133-135, https://www.jstor.org/stable/pdf/resrep07921.1.pdf; Jessica Brandt and Adrianna Pita, "How Is Russia Conducting Cyber and Information Warfare in Ukraine?" Brookings (March 3, 2022), https://www.brookings.edu/podcast-episode/how-is-russia-conducting-cyber-and-information-warfare-in-ukraine/.
6. "Defending Ukraine: Early Lessons from the Cyber War," *Microsoft* (2020), 6-7, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK.
7. Michael Walzer, *Just and Unjust Wars: A Moral Argument with Historical Illustrations* (New York: Basic Books, 2015).
8. Seth Lazar, "War," *The Stanford Encyclopedia of Philosophy*, Edward N. Zalta, ed. (2020), https://plato.stanford.edu/entries/war/#toc.
9. Ibid.
10. Ibid.
11. Ibid.
12. Randall R. Dipert, "The Ethics of Cyberwarfare," *Journal of Military Ethics,* vol. 9, no. 4 (2010), 384-410, https://www.tandfonline.com/doi/abs/10.1080/15027570.2010.536404.
13. Luciano Floridi, "Information Ethics, Its Nature and Scope," *SIGCAS Computers and Society*, vol. 36, no. 3 (2006), 21-36, https://dl.acm.org/doi/abs/10.1145/1195716.1195719.
14. Ibid.
15. Ibid.
16. Luciano Floridi, *The Ethics of Information* (Oxford, United Kingdom: Oxford University Press, 2013).
17. Luciano Floridi, "Information Ethics: On the Philosophical Foundation of Computer Ethics," *Ethics and Information Technology*, vol. 1, no. 1 (1999), 33-52, https://link.springer.com/article/10.1023/A:1010018611096.
18. Mariarosaria Taddeo, "Just Information Warfare," *Topoi*, vol. 35, no. 1 (2016), 213-224, https://link.springer.com/article/10.1007/s11245-014-9245-8.
19. Ibid.
20. Ibid.
21. Ibid.
22. Ibid.
23. Office of the Director of National Intelligence, "Background to 'Assessing Russian Activities and Intentions in Recent US Elections': The Analytic Process and Cyber Incident Attribution" (2017), https://www.dni.gov/files/documents/ICA201701 .pdf; Matthew Cole et al., "Top-Secret NSA Report Details Russian Hacking Effort Days Before 2016 Election," *The Intercept* (June 5, 2017), https://theintercept.com /2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/; Kate Fisher, "Russian Interference in the 2016 United States Presidential Election," *Plan II Honors Thesis*—The University of Texas at Austin (2019), https:// repositories.lib.utexas.edu/handle/2152/75445.
24. "S. Rept. 116-290 - Russian Active Measures Campaigns and Interference in the 2016 US Election, Volumes I-V," Library of Congress (2022), https://www.congress.gov/116/crpt/srpt290/CRPT-116srpt290.pdf.
25. Abigail Abrams, "Here's What We Know So Far About Russia's 2016 Meddling," *Time* (April 18, 2019), https://time.com/5565991/russia-influence-2016-election.

NOTES

26. Ibid.
27. Ibid.
28. Ibid.
29. Adam Goldman, “F.B.I. Warns of Russian Interference in 2020 Race and Boosts Counterintelligence Operations,” *The New York Times* (April 26, 2019),

https://www.nytimes.com/2019/04/26/us/politics/fbi-russian-election-interference.html.

30. “Russian Interference in 2016 US Elections,” *FBI: Most Wanted* (2022), https://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections.
31. Ibid.
32. Lara Jakes, “With Sanctions on Russia, US Warns Against Foreign Election Meddling,” *The New York Times* (September 30, 2019), https://www.nytimes.com/2019/09/30/us/politics/us-russia-sanctions-election-meddling.html.

The Cyber Defense Review

◆ Research Note ◆

Regulating Cyber Warfare Through the United Nations

Cadet Andrew Luzzatto

ABSTRACT

Cyber warfare is an emerging type of conflict threatening international establishments such as international humanitarian law and the norms guiding interactions between states. Currently, with no means to slow down their use, the rate at which cyber weapons are being produced and launched between states is growing. One organization that can change that is the United Nations. The United Nations possesses several facilities that make it a powerful tool to address the ever-expanding problem of international cyber security. While other options for imposing regulations exist, state governments should favor the United Nations as the premier platform to address this issue.

INTRODUCTION

Throughout the 21st century, a consensus of academics and policymakers agree that the continuing power and significance of modern cyber weapons threatens state norms and international law. Recent cyber-attacks have demonstrated blatant violations of international humanitarian law and the Universal Declaration Of Human Rights, as well as less concrete intrusions of national sovereignty. This stems partly from a lack of regulations addressing the issue. As of now, there is no internationally recognized definition for cyber weapons, no specific treaties that regulate them, and no means to prevent their use and rapid proliferation. Though there has been much discussion regarding different treaties and regulations that could be implemented to address cyber warfare, the question of how to implement these policies remain mostly unanswered. In other words, there is no present consensus on the means or the venue to discuss this problem. As the United Nations is a multilateral body with experience dealing with

Mr. Andrew J. Luzzatto is a fourth-year cadet at Norwich University majoring in Computer Security and Information Assurance. His coursework extends into cyberlaw, international relations, and ethics in computing and technology. For the past six years, he has participated in both high school and collegiate Model United Nation's programs. He is also member of the National Science Foundation CyberCorps Scholarship for Service Program, which pays for two years of undergraduate education in exchange for two years of service in the public cybersecurity sector.

unconventional weapons, it is the ideal organization to address this issue, as it possesses both the means and mandate to regulate cyber warfare.

ISSUES WITH CYBER WARFARE

Lack of a Standard Definition

Similar to terms like "terrorism" and "hybrid warfare," it is difficult to define what exactly "cyber warfare" and its related terms ("cyber-attack," "cyber-espionage," etc.) are. In fact, the definition of the word "cyberspace" itself is still a matter of debate, with different countries and international organizations prescribing different meanings in different situations.[1] While several proposals have been made by states and academics alike, no single definition seems to be comprehensive enough to fully encompass the issue and to address the concerns of most governments.[2]

An example of such an attempt to set these definitions as they related to international law is the Tallinn Manual on International Law Applicable to Cyber Warfare. Written in 2013 by a group of twenty international experts on the subject, the Tallinn Manual seeks to informally resolve the confusion regarding the regulation of cyber warfare.[3] The manual itself is made of a set of 95 rules that states should follow when conducting cyber operations.[4] Though this document effectively addresses several points of ambiguity surrounding international cyber warfare (including its related definitions), it functions only as an academic work.[5] This stipulation makes the document potentially useful for the creation of new international definitions and laws, but not suitable as a legally binding interpretation of international law.

Without a standard international definition, states can modify the meaning of the term "cyber warfare" according to their interests. For example, consider the Russian Federation's definition of an alternate term, "information warfare," which is defined in part as a "conflict between two or more States in the information space with the goal of...carrying out mass psychological campaigns against the population of a State in order to destabilize society and the government."[6] This definition specifically addresses destabilization, which allows Russia to label social media posts, news stories, and blogs that oppose the interests of the Russian government as information warfare. The Shanghai Cooperation Group (of which Russia is a member) maintains a similar definition.[7] Critics of this definition of information warfare are concerned that it validates state censorship.[8] In an effort to sidestep this problem, states steer away from terms like "information warfare" and "information security" during international discussions on cyber regulations.[9]

Difficulty Applying International Norms and Laws

The way that cyber warfare relates to the established laws and norms that drive international relations is still unsettled. States and scholars do not yet know how the ideas of damage, sovereignty, and privacy apply to cyberspace. The relationship between cyber warfare and the principle of the use of force is chief among these concerns. According to the UN Charter, Chapter I, Article 2, Paragraph 4 and Chapter VII, Article 51, state actors can only use force as a form of self-defense against an armed attack.[10] Without proper international regulations that address the status of cyber weapons, states who consider cyber-attacks equivalent to armed attacks can justify their use of retaliatory strikes in the name of self-defense. While this has not yet occurred or been formally codified, the US has stated that it reserves the right to respond to enemy cyber-attacks "as we would to any other threat to our country."[11] Similarly, the North Atlantic Treaty Organization (NATO) has declared that it may, under currently undefined circumstances, consider a cyber-attack against any member state as an armed attack that would trigger the organization's Article V "collective defense measure."[12] Considering that these two entities have developed their own definitions for cyber warfare, and that these definitions differ from those of their competitors', namely the Shanghai Cooperation Group, there is a possibility that an unresolvable legal debate could erupt from a cyber-attack.

The attribution and identification of attacks are also major issues in cyberspace. Because cyber weapons are designed to exploit vulnerabilities unknown to the target, administrators often do not know they are being attacked until it is too late. The secret nature of cyber-attacks also makes it challenging, but not impossible, to identify the perpetrators of an attack.[13] It is even more difficult to address whether the culprit is working with a state government.[14] Even after a specific group or individual has been identified as the source of an attack, state governments can (and often do) deny any affiliation. Such was the case with the WannaCry ransomware virus. When the US attributed the virus to a member of the North Korean government, the North Korean Foreign Ministry promptly replied that the issue "has nothing to do with us."[15] States are easily able to deny and avoid affiliation with groups conducting cyber-attacks. This has disrupted the idea of deterrence, as retaliation against a state government could be interpreted as a first use of force and not as an act of self-defense.

Ethical Concerns

Several state actors, to include Israel, Iran, and Russia, have started utilizing civilians, private businesses, and critical health, water, and electrical infrastructure as targets in cyber warfare campaigns. Such a situation occurred in an exchange of cyber-attacks between Israel and Iran in the spring of 2020, when both states targeted elements of civilian infrastructures, including Israeli water treatment plants and privately owned business systems at Iran's Shahid Rajaee Port.[16] A similar incident occurred in December of 2015, when Russian hackers (who were possibly linked with the Russian government) launched a cyber-attack against several Ukrainian power plants, causing over 200,000 people to lose power.[17] State and non-state actor use of cyber espionage against civilian targets has also become immensely popular, though that practice is beyond the scope of this article.

International humanitarian law dictates that a distinction between combatants and civilians must be maintained in all forms of conflict.[18] In certain situations, this can be extremely difficult, as private infrastructure is usually intertwined and sometimes indistinguishable from military targets. Military organizations use the same computers, programs, networks, privately owned infrastructure, and cloud service providers as other internet users. In short, the dual-use nature of cyber infrastructure can leave civilian targets in the way of dangerous cyber-attacks.

OTHER OPTIONS FOR CONFRONTING THE ISSUE

Bilateral Agreements

Bilateral discussions and treaties play a crucial role in preventing and regulating all forms of warfare, including cyber. Whenever a cyber-attack occurs, the first channels used to discuss the issue are those established between the target and the perceived perpetrator. Within these venues, states can discuss possible resolutions to issues in cyberspace before escalating to other means. Additionally, discussions about cyber warfare within these forums allow states to gain a clearer understanding about each other's policies and objectives.[19]

The problem with bilateral agreements is that they, by their very nature, only settle disputes between two states. They fail to address the impact cyberspace has had on the world as a whole.[20] Additionally, bilateral treaties tend to be more fragile than larger, multilateral treaties.[21] This may be because of a lack of additional states and entities providing accountability for state actions. As accountability is one of the key concerns for cyber warfare, bilateral agreements alone cannot fully regulate the practice of conflict in cyberspace.

Regional Bodies

Regional bodies can help states collectively identify and classify cyber security threats. In these larger, multilateral organizations, discussions are centered around the larger, persistent security concerns faced by the group.[22] Groups like NATO and the European Convention on

Cyber Crime are a few examples of organizations effectively defining terms and regulating actions in cyberspace.[23]

There is skepticism within the international community as to how effective a regional body can be at accommodating and incorporating the policies of other countries into their framework. While regional bodies are effective at forming a consensus among like-minded parties, they fail to resolve conflicting ideas between separate groups, including differing ideas on definitions for cyber warfare. Such a concern was voiced by Brazil, China, and India regarding the European Convention on Cyber Crime. Though the convention has played a critical role in helping to define and regulate specific cybercrimes, these states still fear that the treaty is "inherently inapplicable to non-European countries."[24] Despite a lack of evidence to substantiate these concerns, with international politics, a country's perception is often just as important as the reality of the situation. Therefore, cyber warfare still needs a global platform where all state governments have a chance to impact the outcome.

WHY CHOOSE THE UNITED NATIONS

Bureaucratic Infrastructure and Mandate

Since its foundation in 1945, the UN mandate has and continues to address threats to international security, to promote the principles of self-determination and human rights, and to become "a centre for harmonizing the actions of nations" as they attempt to do the same.[25] As cyber warfare is intimately intertwined with each of these issues, the UN's responsibility to address the status of cyber weapons is indisputable.

To fulfill its mandate, the UN Charter establishes a comprehensive infrastructure of different subsidiary bodies, referred to in the Charter as "organs," capable of individually addressing specific aspects of multifaceted issues like cyber warfare. The unity of these various organs under a single body allows for the standardization, codification, and coordination of terms, treaties, and efforts to regulate cyberspace.

The General Assembly

The first and most well-known of these aforementioned organs is the General Assembly. The General Assembly is unique in that every member state (and some non-state actors) can participate.[26] For this reason, during certain parts of the resolution-writing process, the General Assembly is considered an equalizer among states of varying degrees of power.[27] With such a high rate of participation, the General Assembly provides what may be the only platform for discussing issues that require international consensus. Given that cyber warfare is an international issue that bleeds across geography, the General Assembly is well-poised to address issues in cyberspace.

While policy scholars are correct that the resolutions produced by the General Assembly are not legally binding,[28] these resolutions remain significant in the international community.

According to the late Oliver Lissitzyn, a renowned legal scholar, unanimous decisions like those made in the General Assembly can represent internationally recognized expectations for state behavior.[29] Discussions held in the General Assembly are equally invaluable in allowing countries to express their individual policies for specific matters of security. In effect, the General Assembly can clarify common ground between states on matters of cyber security.

The General Assembly also has the authority to launch studies into security issues like cyber warfare.[30] Such an action has already been taken by the UN under resolution A/RES/58/32, which declared the creation of a Group of Governmental Experts (GGE) to discuss the confluence of information and communication technology development and international security.[31] Since its first session in 2004, this group has produced several reports detailing concerns for interactions in cyberspace, including several of the aforementioned points found in part one of this article. These reports have effectively laid the groundwork for future efforts to regulate cyber warfare while simultaneously proving that the General Assembly can and has added meaningful contributions to the subject matter.

The Security Council

Another organ defined within the UN Charter is the Security Council. Unlike the General Assembly, the Security Council consists of five permanent members and ten additional members elected for two-year terms.[32] The Security Council has the unique capability to pass resolutions that all member states are required to follow.[33] This allows the Security Council to set legally binding precedents for international relations in areas like cyber warfare. Additionally, all initiatives passed by the Security Council have the full support of its permanent members, as a single vote by a permanent member against a resolution will prevent it from being accepted.[34] While this rule can delay the adoption of regulations, it grants the benefit of consensus from such major global powers as the United States, China, and Russia, all of which are permanent members of the Security Council.[35]

The Security Council has the authority to discuss matters that pose a significant and immediate threat to international security and human life.[36] Examples of this range from long term security situations, such as Iran's development of nuclear weapons,[37] to more specific events, such as the Six-Day War in 1967.[38] The international community can leverage the powers of the Security Council as a means to address situations where bilateralism fails to reduce tensions following a cyber-attack.

CONCLUSION

There are some well-founded concerns with using the UN to handle cyber warfare. First among these is the simple fact that the UN has failed to prescribe a definition to cyber warfare in nearly two decades of addressing the issue. As of now, most of the UN's efforts in cyberspace have been directed towards helping states build up their cyber defense capabilities. However, it is important to remember that developing taxonomies and regulations for weapons systems is normally a slow process. The term “weapon of mass destruction” was only given an internationally recognized definition in 1977 through General Assembly resolution A/RES/32/84,[39] nearly three decades after the term was first used in a UN resolution in 1947.[40] The first treaty effective at regulating chemical warfare, the Chemical Weapons Convention of 1993, was first open for signing almost eighty years after the first use of chlorine gas as a weapon in World War I.[41]

Keeping this in mind, it should come as no surprise that the international community does not yet have a mechanism to completely address and counter cyber warfare. It is indeed possible that it may take the UN another five to ten years of discussion in the General Assembly before a definition is finally decided, and still decades more before a comprehensive treaty regulating cyber warfare is organized. Nevertheless, this should not dissuade countries from taking advantage of the functions and infrastructure that the UN provides.

DISCLAIMER

The views expressed in this work are those of the authors and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, or the Department of Defense.

NOTES

1. Alexander Klimburg, ed. *National Cyber Security Framework Manual* (Tallinn, Estonia: NATO Cooperative Cyber Defense Centre of Excellence, 2012), 8, https://www.ccdcoe.org/uploads/2018/10/NCSFM_0.pdf.
2. Ibid., 17.
3. Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare*, New York: Cambridge University Press, 2013, accessed October 3, 2022, https://ebookcentral.proquest.com/lib/norwich/detail.action?docID=1113076.
4. Priyanka R Dev, ""use of Force" and "Armed Attack" Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal U.N. Response," *Texas International Law Journal* 50, no. 2 (Spring, 2015): 384, https://library.norwich.edu/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fscholarly-journals%2Fuse-force-armed-attack-thresholds-cyber-conflict%2Fdocview%2F1704865288%2Fse-2%3Faccountid%3D12871.
5. Dev, ""use of Force" and "Armed Attack" Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal U.N. Response," 385.
6. The Ministry of Foreign Affairs of the Russian Federation, “Convention on International Information Security,” Foreign Policy / Fundamental Documents, accessed April 20, 2021, https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666.
7. Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, and Julia Spiegel, "The Law of Cyber-Attack," *California Law Review* 100, no. 4 (2012): 825, http://www.jstor.org/stable/23249823.
8. Hathaway, Crootof, Levitz, Nix, Nowlan, Perdue, and Spiegel, "The Law of Cyber-Attack," 825.
9. Keir Giles, “Prospects for the Rule of Law in Cyberspace,” Carlisle, Pennsylvania: Strategic Studies Institute, United States Army War College (2017), 9, http://www.jstor.org/stable/resrep11600.
10. Charter of the United Nations arts. 2 and 51, *adopted* June 26, 1945, U.S.T. 993, U.N.T.S., https://tile.loc.gov/storage-services/service/ll/lltreaties//lltreaties-ustbv003/lltreaties-ustbv003.pdf.
11. U.S. White House, I*nternational Strategy for Cyberspace*, (Washington, DC: Government Publishing Office, 2011), 14, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.
12. North Atlantic Council, “Wales Summit Declaration,” North Atlantic Treaty Organization, August 30, 2018, https://www.nato.int/cps/en/natohq/official_texts_112964.htm?mode=pressrelease.
13. Eva-Nour Repussard, “There is No Attribution Problem, Only a Diplomatic One,” *E-International Relations*, March 22, 2020, https://www.e-ir.info/2020/03/22/there-is-no-attribution-problem-only-a-diplomatic-one/.
14. Repussard, “There is No Attribution Problem, Only a Diplomatic One.”
15. Eric Talmadge, “N. Korea calls Song, Wannacry hack charges smear campaign,” *The Associated Press*, September 13, 2018, https://apnews.com/article/80003a5e8f9440e0bb4cca664c63a132.
16. Gil Baram and Kevjn Lim, “Israel and Iran Just Showed Us the Future of Cyberwar With Their Unusual Attacks,” *Foreign Policy*, June 5, 2020, https://foreignpolicy.com/2020/06/05/israel-and-iran-just-showed-us-the-future-of-cyberwar-with-their-unusual-attacks/.
17. Donghui Park and Michael Walstrom, “Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks,” The Henry M. Jackson School of International Studies: University of Washington, October 11, 2017, https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/.
18. International Committee of the Red Cross, “Rule 1. The Principle of Distinction between Civilians and Combatants,” IHL Database, accessed April 20, 2021, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_cha_chapter1_rule1.
19. Lucas Ashbaugh, "An Analysis Of International Agreements Over Cybersecurity," *University of Maine Electronic Theses and Dissertations* April 27, 2018: 42, https://digitalcommons.library.umaine.edu/etd/2876.
20. Ashbaugh, "An Analysis Of International Agreements Over Cybersecurity," 15.
21. Paul Meyer, “Cyber-Security through Arms Control: An Approach to International Co-Operation,” *The Rusi Journal* 156, no. 2 (2011): 26, https://doi.org/10.1080/03071847.2011.576471.
22. Giles, *Prospects for the Rule of Law in Cyberspace*, 17.
23. Ibid., 21-23.
24. Ibid., 22.
25. Charter of the United Nations art. 1, *adopted* June 26, 1945, U.S.T. 993, U.N.T.S., https://tile.loc.gov/storage-services/service/ll/lltreaties//lltreaties-ustbv003/lltreaties-ustbv003.pdf.

NOTES

26. Ibid.
27. Diana Panke, “The Institutional Design of the United Nations General Assembly: An Effective Equalizer?” *International Relations* 31, no. 1 (March 2017): 13, https://doi.org/10.1177/0047117817690567.
28. Charter of the United Nations art. 10, *adopted* June 26, 1945, U.S.T. 993, U.N.T.S., https://tile.loc.gov/storage-services/service/ll/lltreaties//lltreaties-ustbv003/lltreaties-ustbv003.pdf.
29. Oliver Lissitzyn, *International Law Today and Tommorow,* 1965, quoted in Stephen M. Schwebel, "The Effect of Resolutions of the U.N. General Assembly on Customary International Law," *Proceedings of the Annual Meeting (American Society of International Law)* 73 (1979): 303, http://www.jstor.org/stable/25658015.
30. Charter of the United Nations art. 13, a*dopted* June 26, 1945, U.S.T. 993, U.N.T.S., https://tile.loc.gov/storage-services/service/ll/lltreaties//lltreaties-ustbv003/lltreaties-ustbv003.pdf.
31. UN General Assembly, Resolution 58/32, “Developments in the field of information and telecommunications in the context of international security,” December 18, 2003, https://undocs.org/pdf?symbol=en/A/RES/58/32.
32. Charter of the United Nations art. 23, *adopted* June 26, 1945, U.S.T. 993, U.N.T.S., https://tile.loc.gov/storage-services/service/ll/lltreaties//lltreaties-ustbv003/lltreaties-ustbv003.pdf.
33. Charter of the United Nations art. 25, *adopted* June 26, 1945, U.S.T. 993, U.N.T.S., https://tile.loc.gov/storage-services/service/ll/lltreaties//lltreaties-ustbv003/lltreaties-ustbv003.pdf.
34. Charter of the United Nations art. 26, *adopted* June 26, 1945, U.S.T. 993, U.N.T.S., https://tile.loc.gov/storage-services/service/ll/lltreaties//lltreaties-ustbv003/lltreaties-ustbv003.pdf.
35. Charter of the United Nations art. 23.
36. United Nations Peacekeeping, “Role of the Security Council,” United Nations, accessed April 20, 2021. https://peacekeeping.un.org/en/role-of-security-council#:~:text=The%20Security%20Council%20has%20primary,peace%20operation%20should%20be%20deployed.
37. United Nations Security Council, Resolution 1696, July 31, 2006, https://www.un.org/securitycouncil/s/res/1696-%282006%29.
38. United Nations Security Council, Resolution 242, November 22, 1967, https://undocs.org/S/RES/242(1967).
39. UN General Assembly, Resolution 32/84, “Prohibition of the development and manufacture of new types of weapons of mass destruction and new systems of such weapons,” December 12, 1977, https://digitallibrary.un.org/record/623117?ln=en.
40. UN General Assembly, Resolution 41(I), “Principles governing the general regulation and reduction of Armaments,” December 14, 1946, https://digitallibrary.un.org/record/209757?ln=en.
41. Vladimir Pitschmann, “Overall View of Chemical and Biochemical Weapons,” *Toxins* 6, No. 6 (2014):1765, www.mdpi.com/2072-6651/6/6/1761/htm.

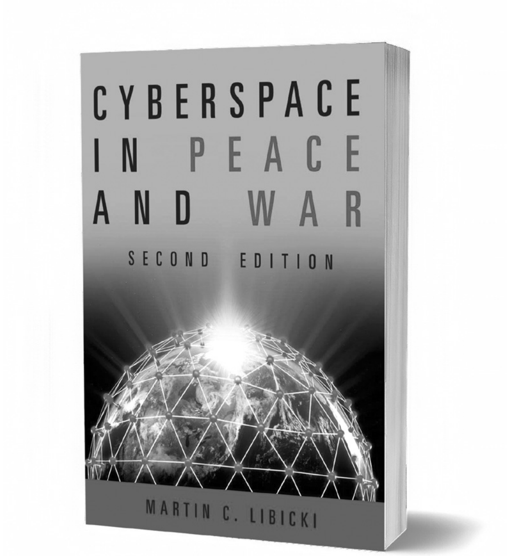
THE CYBER DEFENSE REVIEW

◇ BOOK REVIEW ◇

Cyberspace in Peace and War, 2nd Edition

By Martin C. Libicki

Reviewed by
Dr. Mark Grzegorzewski



RECOMMENDATION: Hall of Fame Worthy

EXECUTIVE SUMMARY

Martin Libicki's *Cyberspace in Peace and War* (2nd Edition) is a cyberwar strategy masterpiece. At this point in my career, rarely do I read books that are so impactful. Readers of Libicki's second edition will ultimately understand almost all aspects of deterrence, the shifting thinking on cyberspace-based effects as an element of national power, and whether cyber deterrence is achievable. Most importantly, readers will be treated to a sober assessment of "cyberwar" rather than predictions of an imminent "cyber-9/11." This important difference takes the focus off preventing a single catastrophic event and instead highlights the increasing complexity of executing cyber operations in a world of digital connectivity. Libicki claims this distinction, plus the many actors utilizing cyberspace, causes difficulties in establishing deterrence in and through cyberspace.

The updated edition, which could be used as a textbook, is out of necessity a voluminous work (250,000-words). Libicki attempts to thread the needle between computer science and strategy, two enormous individual topic areas made even more complex by their interplay. In this undertaking, he masters a complex objective, and this book should be read both the IT crowd and by military strategists (due to its non-technical approach, this book is accessible to readers without a tech background). For those, like myself, interested in the overlap of these two topics, this book is pure delight.

Mark Grzegorzewski, Ph.D., is a Resident Senior Fellow in the Department of Strategic Intelligence and Emerging Technology at the Joint Special Operations University, U.S. Special Operations Command. He has recently co-edited and contributed a chapter to a *JSOU Press* edited monograph titled "*Big Data for Generals... and Everyone Else over 40*" and published an article with *Cyber Defense Review* titled "Technology Adoption in Unconventional Warfare." He also recently co-authored a piece in *Lawfare* titled "Taking the Elf Off the Shelf: Why the U.S. Should Consider a Civilian Cyber Defense."

In the first part of the book, Libicki provides the terms of reference for any cyber discussion. By providing this overview, Libicki allows the reader to understand what is possible while not allowing their imagination from wandering into the fantastical. In the second part of the book, Libicki views cyberspace through the national security lens, including military operations, command and control, and espionage. In part three, Libicki focuses on national security strategy, more specifically deterrence. Part III is the largest portion of the book and puts Libicki's systematic approach to strategic thinking on display. In the final section of the book, Libicki brings it all together by discussing how cyberspace-based effects can be integrated into deterrence, while discussing specific deterrence strategies regarding China and Russia.

REVIEW

Cyberspace in Peace and War is broken out into four parts (Foundations, Operations, Strategies, and Norms), which on their own could be standalone books given the level of detail Libicki provides. In part I, Libicki discusses cyberspace foundations, including emblematic attacks; some basic cyber principles; how to compromise a computer; cybersecurity as a systems problem; defending against deep and wide attacks; and deterrence by denial. These sections force the reader to reconsider technology concepts that perhaps had been taken for granted (e.g., the distinction between information and instructions to computers). Cyber planners and students new to the cyberspace literature should read this section to better appreciate limitations and possibilities in cyberspace. What is possible is tempered by the reality of what is permissible, and part one lays out the guardrails on what is technologically feasible, which in turn keeps the discussion on cyber strategy from careening into fanciful ideas of what could be executed in and through cyberspace.

In part II, Libicki addresses operations that include tactical cyberwar; organizing a cyberwar campaign; professionalizing cyberwar; strategic implications of tactical cyberwar; the stability implications of tactical cyberwar; and asks if cyberspace is a warfighting domain. The theme of this section is that cyberwar's effects are overstated, which makes sense when one scrutinizes what is meant by cyberwar. In terms of how the U.S. conceptualizes cyberspace, a cyberspace operation could either deny, degrade, disrupt, or manipulate (D4M) information inside a technological system. Each of these effects are different degrees of interruptions and can be scaled and reversed. Therefore, as more information technology systems are backed up, upgraded/patched, and made more resilient, cyber operations can have lasting effects but the impacts need not necessarily be strategic, nor permanent. This nuanced point often gets lost when thinking through cyberspace operations. Many thinkers become over enchanted with what can be accomplished in and through cyberspace. These remarkable effects are real but also can be reversed with time. Therefore, Libicki concludes that most cyber effects are most effective when paired with kinetic effects.

In part III—the real meat of the book—the author unpacks strategies such as strategic cyberwar; cyberwar threats such as deterrence and compulsion; the unexpected asymmetry of cyberwar; responding to cyberattack; deterrence fundamentals; the will to retaliate; attribution; what threshold for response; a deterministic posture; punishment and holding targets at risk; cyberwar escalation; brandishing cyberwar capabilities; narratives and signals; cyberattack inferences from cyberespionage; and strategic stability. For military strategists and political scientists alike, Libicki leaves no stone unturned when examining deterrence. For those who ask, why not hack back?, Libicki demonstrates how escalation works in cyberspace, and in fact claims that actions in cyberspace are preferable since they do not often lead to real world violence. As Libicki claims, in cyberspace, nation-states are playing by Vegas rules. Put another way, in most cases, what happens in cyberspace stays in cyberspace.

In the concluding portion, part IV, Libicki address norms that include the norms for cyberspace; the rocky road to cyberespionage norms; Sino-US relations and norms in cyberspace; the enigma of Russian behavior in cyberspace; cybersecurity futures; and asks what is cyberwar good for? Aside from the norms discussion, this section may be the weakest part of the book. Nevertheless, it is still a very informative perspective for cyberspace scholar-practitioners. I particularly enjoyed Libicki bringing to the fore that, like the US, both Russia and China are still finding their way in cyberspace. Often, the US sees its adversaries as 10-foot-tall boogeymen who cannot be stopped. In the case of Russia, this impression is often fed by a misreading of the so-called Gerasimov Doctrine. In fact, US adversaries are still testing and learning in cyberspace, and they are just as vulnerable due to their own exposed attack surface. In addition, US adversaries are still developing their own thoughts on how to employ cyber effects, meaning it is a test and learn culture that currently limits the occurrence of strategic level cyber effects. The good news from the last section of the book, is that the sky is not falling due to US' adversaries use of cyberspace operations. Therefore, we should understand this as welcome news and update our thinking on the impact of cyberspace-based effects.

CONCLUSION

One minor critique I have of Libicki's work is a broader general critique of deterrence theory. Frequently, deterrence theory is broken out into a reductionist formula in which decision makers and organizations act rationally, and policymakers do not have gaps in knowledge. The risk is that someone new to the cyberspace literature will translate this information into a checkbox mentality to "achieve" cyber deterrence. This is not Libicki's purpose. Rather, Libicki takes pains to highlight the uncertainty undergirding deterrence theory. This is demonstrated by the author posing many of his subsections as questions and highlighting the limits of what we can know. The other observation is not as much a critique as a caution to the reader. Given the technical and high-level strategic focus of this book, it must be read very closely. I found myself going back and re-reading several parts of Libicki's work just to make sure I completely understood the argument. This is not due to Libicki's writing style. He does a wonderful job communicating this complex topic. Rather, the reader must make sure to completely absorb Libicki's complex proposals if they are to successfully process the book. That is the accumulative nature of the book, and if readers take the time to fully absorb Libicki's cyber deterrence argument, they will not be disappointed.

Title: ***Cyberspace in Peace and War*** (2nd Edition)
Publisher: Naval Institute Press (2021)
Hardcover: 492 pages
Language: English
ISBN-13: 978-1682470329
Price: $56.44 (Hardcover)
$45.49 (Kindle)

The Cyber Defense Review

Continue The conversation online

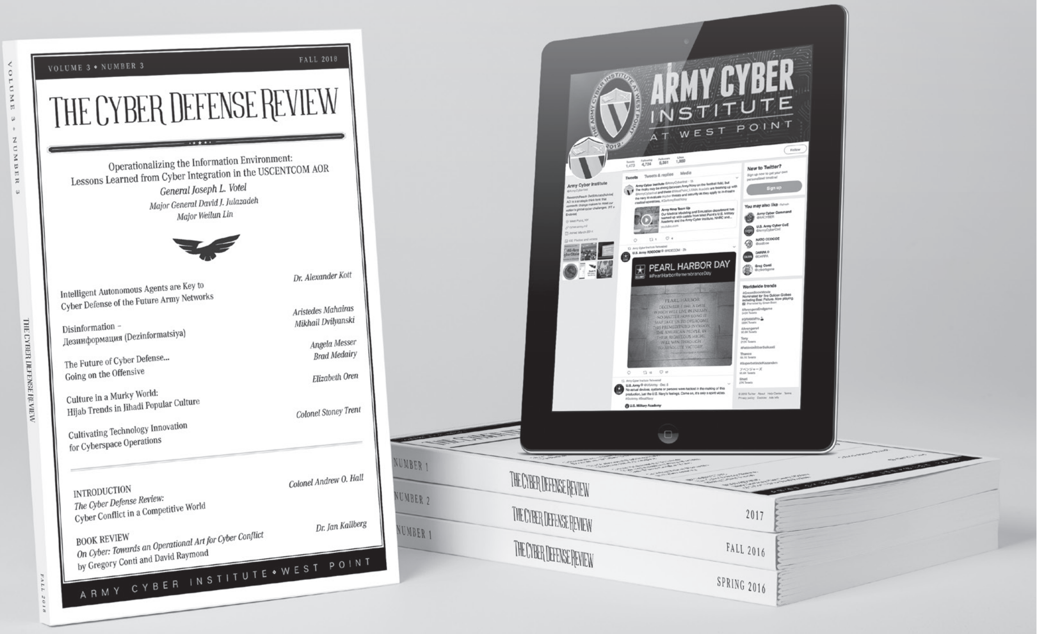
CyberDefenseReview.Army.mil

AND THROUGH SOCIAL MEDIA

Facebook @ArmyCyberInstitute

LinkedIn @LinkedInGroup

Twitter @ArmyCyberInst
@CyberDefReview



VOLUME 3 • NUMBER 3 FALL 2018

THE CYBER DEFENSE REVIEW

Operationalizing the Information Environment: Lessons Learned from Cyber Integration in the USCENTCOM AOR
General Joseph L. Votel
Major General David J. Julazadeh
Major Weilun Lin

Intelligent Autonomous Agents are Key to Cyber Defense of the Future Army Networks — *Dr. Alexander Kott*

Disinformation – Дезинформация (Dezinformatsiya) — *Aristedes Mahairas*, *Mikhail Dvilyanski*

The Future of Cyber Defense... Going on the Offensive — *Angela Messer*, *Brad Medairy*

Culture in a Murky World: Hijab Trends in Jihadi Popular Culture — *Elizabeth Oren*

Cultivating Technology Innovation for Cyberspace Operations — *Colonel Stoney Trent*

INTRODUCTION
The Cyber Defense Review: Cyber Conflict in a Competitive World — *Colonel Andrew O. Hall*

BOOK REVIEW
On Cyber: Towards an Operational Art for Cyber Conflict by Gregory Conti and David Raymond — *Dr. Jan Kallberg*

ARMY CYBER INSTITUTE • WEST POINT

ARMY CYBER INSTITUTE ◆ WEST POINT PRESS

WEST POINT
PRESS

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.