

THE CYBER DEFENSE REVIEW



Using International Law to Deter Russian Proxy Hackers

Col. Andrew D. Flor



Recruit, Train, and Retain DoD Cyber Skills Like Language Skills

Lt. Col. David R. Dixon and Capt. Patrick J. Cirenza

Killer Bots Instead of Killer Robots: Updates to DoD Directive 3000.09 may create legal implications

Lt. Col. Jon Erickson

Expanding the Dyadic Cyber Incident and Campaign Dataset (DCID): Cyber Conflict from 2000 to 2020

*Dr. Ryan C. Maness, Dr. Brandon Valeriano, Dr. Kathryn Hedgecock,
Jose Macias, Dr. Benjamin Jensen*

Synthetic Environments for the Cyber Domain: A Survey on Advances, Gaps, and Opportunities

Emily Nack and Lt. Col. Nathaniel D. Bastian

Posturing U.S. Cyber Forces to Defend the Homeland

Col. Jamel Neville

INTRODUCTION

The Army Cyber Institute:
The U.S. Army's Cyber Think Tank

Col. Jim Raftery

BOOK REVIEW

*The Smartest Person in the Room:
The Root Cause and New Solution for Cybersecurity*
by Christian Espinoza

Cadet Aaron Calhoun

THE CYBER DEFENSE REVIEW

◆ SUMMER EDITION ◆

THE CYBER DEFENSE REVIEW

A DYNAMIC MULTIDISCIPLINARY DIALOGUE

EDITOR IN CHIEF

Dr. Corvin J. Connolly

MANAGING EDITOR

Dr. Jan Kallberg

ASSISTANT EDITORS

West Point Class of '70

AREA EDITORS

Dr. Harold J. Arata III
(Cybersecurity Strategy)

Dr. Michael Grimaila
(Systems Engineering/Information Assurance)

Ms. Elizabeth Oren
(Cultural Studies)

Lt. Col. Todd W. Arnold, Ph.D.
(Internet Networking/Capability Development)

Dr. Steve Henderson
(Data Mining/Machine Learning)

Dr. David Raymond
(Network Security)

Ms. Donna Artusy, J.D.
(Cyber Law)

Dr. Michael Klipstein
(Cyber Policy/Cyber Operations)

Dr. Robert J. Ross
(Information Warfare)

Lt. Col. Nathaniel D. Bastian, Ph.D.
(Advanced Analytics/Data Science)

Lt. Col. Charlie Lewis
(Military Operations/Training/Doctrine)

Dr. David Thomson
(Cryptographic Processes/Information Theory)

Dr. Amy Ertan
(Cyber Strategy)

Dr. Fernando Maymi
(Cyber Curricula/Autonomous Platforms)

Dr. Robert Thomson
(Learning Algorithms/Computational Modeling)

Dr. David Gioe
(History/Intelligence Community)

Dr. William Clay Moody
(Software Development)

Col. Natalie Vanatta, Ph.D.
(Threatcasting/Encryption)

Dr. Dawn Dunkerley Goss
(Cybersecurity Optimization/Operationalization)

Dr. Jeffrey Morris
(Quantum Information/Talent Management)

Lt. Col. (Ret.) Mark Visger, J.D.
(Cyber Law)

EDITORIAL BOARD

Dr. Andrew O. Hall, (Chair.)
Marymount University

Dr. Michele L. Malvesti
University of Texas at Austin

Dr. Bhavani Thuraisingham
The University of Texas at Dallas

Dr. David Brumley
Carnegie Mellon University

Dr. Milton Mueller
Georgia Tech School of Public Policy

Ms. Liis Vihul
Cyber Law International

Col. (Ret.) W. Michael Guillot
Air University

Col. Suzanne Nielsen, Ph.D.
U.S. Military Academy

Prof. Tim Watson
Loughborough University, UK

Dr. Martin Libicki
U.S. Naval Academy

Dr. Hy S. Rothstein
Naval Postgraduate School

Prof. Samuel White
Army War College

CREATIVE DIRECTORS

Sergio Analco | Gina Daschbach

LEGAL REVIEW

Courtney Gordon-Tennant, Esq.

KEY CONTRIBUTORS

Sheri Beyea

Tim Boss

Col. (Ret.) John Giordano

Evonne Mobley

Alfred Pacenza

Clare Blackmon

Kate Brown

Charles Leonard

Thomas Morel

Samantha Reeves

CONTACT

West Point Press
Taylor Hall, Building 600
West Point, NY 10996

SUBMISSIONS

The Cyber Defense Review
welcomes submissions at
TheCyberDefenseReview@westpoint.edu

WEBSITE

cyberdefensereview.army.mil

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

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

This publication of the CDR was designed and produced by Gina Daschbach Marketing, LLC, under the management of FedWriters. The CDR is printed by McDonald & Eudy Printers, Inc. ∞ Printed on Acid Free paper.

INTRODUCTION

Col. Jim Raftery

9

The Army Cyber Institute:
The U.S. Army's Cyber Think Tank

SENIOR LEADER PERSPECTIVE

Col. Andrew D. Flor

15

Using International Law to
Deter Russian Proxy Hackers

PROFESSIONAL COMMENTARY

Lt. Col. David R. Dixon
Capt. Patrick J. Cirenza

39

Recruit, Train, and Retain DoD Cyber
Skills Like Language Skills

RESEARCH ARTICLES

• **Lt. Col. Jon Erickson**

51

Killer Bots Instead of Killer Robots:
Updates to DoD Directive 3000.09
may create legal implications

• **Dr. Ryan C. Maness**
Dr. Brandon Valeriano
Dr. Kathryn Hedgecock
Jose Macias
Dr. Benjamin Jensen

65

Expanding the Dyadic Cyber Incident and
Campaign Dataset (DCID): Cyber Conflict
from 2000 to 2020

RESEARCH ARTICLES

Emily Nack
Lt. Col. Nathaniel D. Bastian, Ph.D.

91

Synthetic Environments for the Cyber Domain: A Survey on Advances, Gaps, and Opportunities

Col. Jamel Neville

105

Posturing U.S. Cyber Forces to Defend the Homeland

BOOK REVIEW

Cadet Aaron Calhoun

131

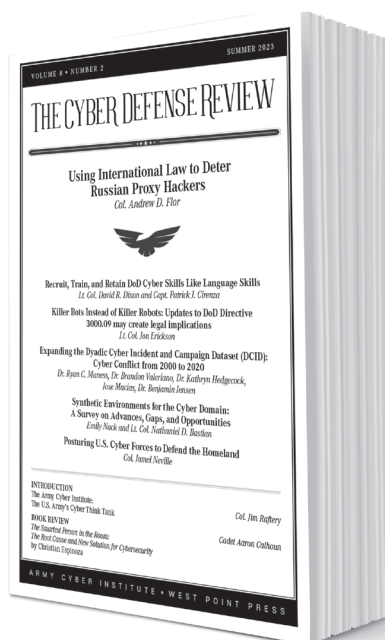
The Smartest Person in the Room: The Root Cause and New Solution for Cybersecurity
By Christian Espinoza

THE CYBER DEFENSE REVIEW

◆ INTRODUCTION ◆

The Army Cyber Institute: The U.S. Army's Cyber Think Tank

COL Jim Raftery



In his introduction to the Fall 2022 issue of *The Cyber Defense Review* (CDR), COL Jeff Erickson, the Army Cyber Institute (ACI) director at the time, opened with, “The only constant in life is change,” a phrase credited to the ancient Greek philosopher Heraclitus. COL Erickson went on to relate this idea via a list of impactful changes that had occurred within the Army’s Cyber Community in the decade since the ACI’s founding in 2012. Three years earlier, the Secretary of Defense had directed the establishment of U.S. Cyber Command as a subordinate unified command under U.S. Strategic Command, followed in 2010 by the stand-up of the U.S. Army Cyber Command. COL Erickson recounted that during this period, “the Army was trying to figure out the best approach to address the uncertain environment and growing demand for deeper understanding” in cyberspace. In my estimate, the Army saw risk in the uncertainty and took action to address and mitigate that risk by directing the creation of the ACI at West Point. Internally, the creation of the ACI was carried out by members of the Department of Electrical Engineering and Computer Science, among whom were then: COL Greg Conti, COL Tom Cook, and COL Gene Ressler. This team was advised and supported in its efforts by then, Dean of the Academic Board BG Tim Trainor and Superintendent LTG Bob Caslen. ACI was designed to be externally focused as the U.S. Army’s Cyber Think

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



COL Jim Raftery is the Head of the Department of Electrical Engineering and Computer Science (EECS) at the United States Military Academy and is a Professor of Electrical Engineering. He was commissioned into the U.S. Army Signal Corps as an ROTC Distinguished Military Graduate from Washington University in St. Louis in 1988. Following command of the 261st Signal Company in Hanau, Germany, he became a member of the Army Acquisition Corps, culminating as Product Manager Information Warfare at Fort Meade, Maryland, from 2007 to 2010. He earned a M.S. in electrical engineering from the University of Missouri - Columbia in 1996 and a Ph.D. in electrical engineering from the University of Illinois at Urbana-Champaign in 2005. He is a 2011 graduate of the Army War College and served in the Cyber National Mission Force at Fort Meade, from 2015 to 2016. His research interests include semiconductor lasers, as well as topics in power, energy, and cyber.

Tank and was organized to report directly to the U.S. Military Academy (USMA) Superintendent. Starting with the visionary leadership of its first director, COL Conti, ACI made contributions to several of the items called out in COL Erickson's list. ACI helped define and address the uncertainty, and today many of those early risks have been mitigated or retired. However, as Heraclitus offered, change is constant, and new risks, challenges, and opportunities continue to arise.

In this vein, recent changes have come to ACI. In May 2022, following coordination with external stakeholders, then Superintendent LTG Darryl Williams directed the movement of ACI from a direct report into the Office of the Dean. Leveraging a model of long-term success found in the hosting of the Office of Economic and Manpower Analysis (OEMA) within the Department of Social Sciences, the Dean, BG Shane Reeves, placed ACI within EECS. Like OEMA, ACI is externally focused to support the Army, and its organization within USMA has synergistic overlap with the intellectual capital and innovative environment found here. Once within EECS, and following a best practice drawn from OEMA, ACI sought out the support of its principal external stakeholders to reimagine the ACI portfolio. Original principal stakeholders included Army Cyber Command, Training and Doctrine Command (now represented by the Cyber Center of Excellence at Fort Gordon, GA, to be redesignated as Fort Eisenhower in October of this year), and Headquarters, Department of the Army G-3/5/7 Strategic Operations. We made the decision to add the Army's Principal Cyber Advisor to the list of stakeholders, recognizing the significance and responsibilities of this position, which followed from the 2020 National Defense Authorization Act. The Commanding General of the Cyber Center of Excellence, MG Paul Stanton, traveled to West Point in the fall of 2022 to participate in the selection process for the new ACI director, COL Stephen Hamilton.

Under COL Hamilton’s leadership, we are operating with an ACI portfolio taxonomy that allocates resources and divides the priority of effort into three “buckets.” The graphic we use shows the #1 priority as a large green bucket. The Think Tank projects that are placed into this green bucket are requested by one of the four principal stakeholders. The #2 priority is a medium-sized blue bucket, which can include projects from any source upon recommendation by the ACI director and validation by a principal stakeholder. The #3 priority is a small red bucket, which can contain projects from any source upon approval of the ACI director. In our graphic, the three buckets are drawn to scale and sized to fill a gold barrel representing the overall ACI portfolio, which is sized to match our resources. With the assistance of our principal stakeholders, we are working to put processes in place to formalize this taxonomy, though we have already begun its implementation. We are also reconstructing the ACI’s external Advisory Group to consist of our four principal stakeholders and establishing another broader-reaching community of interest from which blue or red bucket projects might be proposed.

As the current head of EECS, I wholeheartedly welcome ACI “home” to the department where the organization was imagined and created. EECS graduates more officers into the Army’s Cyber Corps than any other academic department in the nation. The complementary inclusion of the Army’s Cyber Think Tank into EECS further strengthens our academic and research programs and enhances our ability to develop leaders of character for the Army and the nation.

It is my pleasure to provide the readership of the CDR with this update on changes within the ACI. We are focused on being the Army’s Cyber Think Tank and, with the partnership and support of our principal stakeholders, we will continue to help the Army address the ever-changing cyberspace environment. In his introduction to the Spring 2023 issue, the CDR editor-in-chief, Dr. Corv Connolly, proudly announced the new home of the CDR with the West Point Press and emphasized its enduring relationship with ACI. To affirm Dr. Connolly’s efforts to continue the CDR’s robust coverage of the cyber domain and embody a commitment to the highest standards of excellence, we offer another inspiring slate of articles written by an impressive group of authors. 🍷

THE CYBER DEFENSE REVIEW

◆ SENIOR LEADER PERSPECTIVE ◆

Using International Law to Deter Russian Proxy Hackers

Colonel Andrew D. Flor

States are legally responsible for activities undertaken through “proxy actors,” who act on the State’s instructions or under its direction or control.

—Harold Koh¹

In 2014, Russia employed dozens of proxy trolls to engage in information warfare in support of its operations in Ukraine.² “Hundreds of fake social media accounts backed by Russian hackers using malware and cyber-attacks flooded the news and online community with disinformation designed to conceal the truth that these groups were backed by Russia to foment domestic dissent.”³ This hybrid warfare, developed during Russia’s 2008 campaign in Georgia, helps Russia to “destabilize surrounding countries” and induces “perception management” that provides Russia with the illusion of “legal legitimacy.”⁴ Russia’s perception management fed the false narrative that Russia had no choice but to support “Russian ethnic minorities” in Crimea who faced “Ukrainian oppression” and wanted to secede and pursue “self-determination.”⁵ When Ukrainian citizens attempted to search online for information about the impending Russian invasion, their searches found Russian disinformation spread by these proxy trolls that were legitimizing Russia’s invasion.⁶

Fast-forward to 2022 and the Russian invasion of Ukraine: Russia continues to employ proxy hackers to destabilize Ukraine and cast doubt on the legitimacy of the Ukrainian government. The “Conti ransomware gang issued a warning” shortly after the war commenced threatening they “would respond to cyber activity against Russia using all their resources ’to strike back at the critical infrastructure of an enemy.’”⁷ Other cyber proxy activity has targeted exploits in Microsoft Windows even as recently as June 2022 where the “Russian hacking group Sandworm” exploited a remote code execution vulnerability

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



COL Andrew D. Flor graduated from the United States Military Academy in 1997 with a Bachelor of Science degree in Computer Science. He commissioned as an Aviation officer and later received his Juris Doctor from the College of William and Mary School of Law in 2004 and is admitted to practice in the Commonwealth of Virginia. COL Flor holds an LL.M. from The Judge Advocate General's Legal Center and School, a Master of Strategic Studies (MSS) degree from the U.S. Army War College, and a Master of Military Art and Science (MMAS) degree from the U.S. Army Command and General Staff College. He currently serves as the Chief of Plans, Office of The Judge Advocate General (OTJAG), in the Pentagon.

called “Follina” in an effort to destabilize media organizations in Ukraine.⁸

Repeated Russian efforts to utilize this type of hybrid warfare will continue to present a problem in the future if the United States (US) and others do not impose costs on Russia. By using proxy hackers, Russia continues to obfuscate efforts to hold them accountable for invading former-Soviet Republics such as Georgia and Ukraine. The US should lead the international community in countering Russian proxy hackers through various means available under international law and norms, including criminal prosecution, sanctions on Russian officials who direct these illicit cyberspace operations, and, if necessary, the use of military force to prevent further non-State hacking efforts.

This article starts by defining proxy hackers and proxy hacking, and follows with a summary of the international law and norms that govern proxies. Recent actual and suspected proxy hacker events caused by Russia confirm some of the challenges of applying international law and norms to proxy hacking, including actions or inaction by victim States. The lack of available responses indicates an underdeveloped state of contemporary international law and reveals gaps the international community can fill by refining norms and applicable legal texts. This article concludes with specific recommendations on how to deal with the threat of proxy hackers, and otherwise deter Russia from using such hackers in the future.

Definitions and Russian Proxy Hacker Operations

Defining what constitutes a proxy hacker comes with inherent challenges. Merriam-Webster defines a proxy as “the agency, function, or office of a deputy who acts as a substitute for another.”⁹ In the cyber context, a proxy is an “actor b acting for actor a,” or more specifically that non-State actor b conducts a cyberspace operation as a substitute for State actor a.¹⁰ The first *Tallinn Manual*, a collection of international law provisions

related to cyber warfare drafted by an International Group of Experts, in Rule 6, “Legal Responsibility of States,” declares that “[a] State bears international legal responsibility for a cyber operation attributable to it and which constitutes a breach of an international obligation.”¹¹ Commonly referred to as the attribution rule, commentary to this rule describes attribution as “a quintessential principle of international law,” and that such a breach of international obligation can come from “either an act or omission.”¹² The commentary also applies this rule to non-State actors, “where [the State] has ‘effective control’ over such actors.”¹³ However, the rule limits applicability to situations where “private citizens, on their own initiative, conduct cyber operations (so-called ‘hacktivists’ or ‘patriotic hackers’).”¹⁴ The key difference in attribution comes down to situations where the State has provided “instructions, direction, or control” over the non-State proxy hackers.¹⁵ Establishing attribution through sufficient evidence of “instructions, direction, or control” occurs from any number of State actions, to include funding for proxy hackers, allowing the hackers safe-harbor in State territory, or protecting the hackers from domestic prosecution or international extradition.¹⁶

As an example, the US hires contractors to conduct cyberspace operations on behalf of U.S. Cyber Command (USCYBERCOM).¹⁷ While this type of relationship would fall within the definition above of a non-State actor, the use of contractors as a substitute for a State actor, USCYBERCOM, would not constitute the type of proxy hacker violation discussed in the *Tallinn Manual* because the contract between the US and the contractor creates a principal-agent relationship.¹⁸ A principal-agent relationship means that the behavior of the contractor (the agent) is controlled by or authorized by the US (the principal). There is no intent by the US to avoid responsibility for contractor actions, even if great efforts are made to obfuscate the US’ cyberspace operations.

Russian proxy hackers differ from USCYBERCOM contractors due to the lack of any acknowledged official relationship between these hackers and the Russian government. In some examples discussed later below, the hackers conduct their operations with minimal Russian oversight or control. In other examples, hackers, whether motivated by patriotism or self-interest, act completely on their own volition. While this independent-style action by patriotic hackers would seem to absolve Russia from responsibility for such malicious cyberspace activities, the law can attribute to Russia the acts of these patriotic hackers if Russia knows about their behavior and fails to stop them. Major General Joseph Berger, who previously served as the Army Cyber Command (ARCYBER) Staff Judge Advocate or senior legal advisor, objects to the phrase “patriotic hacker” because of the “status or imprimatur” accorded by this.¹⁹ However, regardless of status, Russia’s undeclared, and often obfuscated, support and direction of cyber hackers create an attribution challenge for the international community.

Brigadier General George Smawley, the Staff Judge Advocate to USCYBERCOM from 2019-2021, states that USCYBERCOM categorizes non-State adversaries into one of four groups: proxies, agents, aligned groups, or criminal organizations.²⁰ Each one requires different legal

authorities to address, and Russia has deployed cyberspace operations in each of these four categories.²¹

The 2018 Senate Report on Russian Interference provides an example of illicit proxy behavior, namely that “Kremlin-backed entities have spent years professionalizing a cadre of paid trolls, investing in large-scale, industrialized ‘troll farms,’ in order to obscure Moscow’s hand and advance the aims of Russia’s information operations both domestically and abroad.”²² These proxy trolls achieve their objectives through three main methods. First, they attack the media: “as Soviet-born author Peter Pomerantsev notes, ‘The Kremlin successfully erodes the integrity of investigative and political journalism, producing a lack of faith in traditional media.’”²³ Second, they remain “ideologically agnostic” and “can simultaneously support far right and far left movements, so long as they are in competition with one another,” in order to sow confusion.²⁴ Third, by “attempt[ing] to exploit societal divisions that already exist, rather than attempt[ing] to create new ruptures,” Russia can further divide the targeted country with these cyber operations.²⁵

Review of Current International Law and Norms

Proxy hackers will continue to present a major challenge for countries around the world. As Major General Berger puts it, proxy hackers are “not going away.”²⁶ Understanding international laws and norms is a prerequisite for State use of proxy hackers and responses to their use. These laws and norms have shortcomings, which will later form the basis for this article’s recommendations.

The Tallinn Manuals – International Law and Norms in Cyberspace

The *Tallinn Manual on the International Law Applicable to Cyber Warfare* (referred to here as the first *Tallinn Manual*), published in 2013, sought to summarize the state of international law and norms in cyberspace “applicable to cyber warfare.”²⁷ The use of this wording by the authors, the International Group of Experts (IGE), was a deliberate attempt to inform the readers that the manual did not cover cyber activities short of war. This created challenges in applying any of the first *Tallinn Manual* provisions to proxy hackers. The 2017 *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (referred to here as *Tallinn Manual 2.0*), published in 2017, specifically applies to “cyber operations during peacetime.”²⁸ *Tallinn Manual 2.0* experts modified some of the rules addressed in the first *Tallinn Manual*. As such, “*Tallinn Manual 2.0* supersedes the first *Tallinn Manual*.”²⁹ Yet, *Tallinn Manual 2.0* still does not “deal with international criminal law, trade law, or intellectual property . . . or domestic law.”³⁰ As a result, some of the same challenges in applying the first *Tallinn Manual* provisions to proxy hackers persist with *Tallinn Manual 2.0*.

Much of what proxy hackers do or try to achieve in cyberspace could constitute criminal behavior. Holding proxy hackers liable for their behavior starts with a criminal indictment.³¹ But Russia does not normally extradite proxy hackers, even when faced with overwhelming

attribution evidence that it approved their actions.³² Extradition illuminates the challenge of holding hackers accountable for murky, possibly State-sponsored, hacking efforts. *Tallinn Manual 2.0* discusses extradition in “International Cooperation in Law Enforcement” (Rule 13),³³ which provides that “States are not obliged to cooperate in the investigation and prosecution of cyber crime.”³⁴ Yet, Comment 8 of this rule specifies that “if extradition is refused on the basis of nationality of the person sought or because the requested State deems that it has jurisdiction over the offence, the requested State shall take action to prosecute.”³⁵ Comment 8 should help resolve problems with prosecution in most Russian proxy hacker attacks. If Russia denies extradition, then it must prosecute. Unfortunately, Russia has thus far ignored this rule with impunity.

Tallinn Manual 2.0 addresses “Internationally Wrongful Cyber Acts” (Rule 14) that expands on the first Tallinn Manual rule on “Legal Responsibility of States” (Rule 6). *Tallinn Manual 2.0* states that “A State bears international responsibility for a cyber-related act that is attributable to the State and that constitutes a breach of an international legal obligation.”³⁶ The term “cyber-related act” vice “cyber operation” deliberately “denote[s] the fact that a State sometimes may bear responsibility for acts other than cyber operations that it conducts or that are attributable to it.”³⁷ The commentary underscores a State’s responsibility to curb proxy hacker behavior: “[s]ince non-State actors such as hacktivists often launch harmful cyber operations . . . a State’s obligation to take measures to control cyber activities taking place on its territory looms large.”³⁸

Tallinn Manual 2.0 updates the attribution rule, “Attribution of Cyber Operations by Non-State Actors” (Rule 17),³⁹ providing that “Cyber operations conducted by a non-State actor are attributable to a State when: (a) engaged in pursuant to its instructions or under its direction or control; or (b) the State acknowledges and adopts the operations as its own.”⁴⁰ This modification and amplification of commentary accompanying Rule 6 from the first *Tallinn Manual* clarifies the circumstances that render a State responsible for actions of non-State actors, such as proxy hackers.⁴¹

Tallinn Manual 2.0 “Due Diligence (General Principle)” (Rule 6) reads, “A State must exercise due diligence in not allowing its territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States.” Again, *Tallinn Manual 2.0* expands on the first *Tallinn Manual* in several important ways. First, it imposes the term “due diligence” vice “knowingly” from the original rule.⁴² Second, it removes the restriction “exclusive” from governmental control, which reduces the required level of control over the territory concerned, whether territory or cyber infrastructure.⁴³ Finally, it expands the level of operations a State must control to those that “affect the rights of” or “produce serious adverse consequences for” other States.⁴⁴ This due diligence rule, combined with a new rule, “Compliance with the Due Diligence Principle” (Rule 7), “requires a State to take all measures that are feasible in the circumstances” to end all cyber operations that violate the due diligence principle.⁴⁵ Of note,

the commentary to this rule states that a majority of the IGE believe this rule requires a State to act to prevent repeated violations that occur on its territory.⁴⁶

United States Position on Tallinn Manuals

The Tallinn Manuals constitute a serious body of work backed by years of effort, but they do not establish binding authority or otherwise create an enforceable right or treaty. Generally, international law only develops when the actions of States become the customary state practice with regard to that topic.⁴⁷ The only other way for these practices and norms to become international law is through treaties or conventions, such as the Geneva Conventions.⁴⁸

The US position on the Tallinn Manuals is illuminating, given the relative cyber power ranking of the US.⁴⁹ In a 2016 speech at Berkeley Law School, Brian Egan, a former State Department Legal Adviser, summarized the United States view of the Tallinn Manuals:

The United States has unequivocally been in accord with the underlying premise of this project, which is that existing international law applies to State behavior in cyberspace. In this respect, the Tallinn Manuals will make a valuable contribution to underscoring and demonstrating this point across a number of bodies of international law, even if we do not necessarily agree with every aspect of the Manuals.⁵⁰

While this speech pre-dated *Tallinn Manual 2.0*, it remains clear that the US position has not changed since then; namely that current international law applies to State behavior in cyberspace.

In contrast, Russia did not send a representative to the IGE that drafted and advised on the creation of the Tallinn Manuals. Indeed, Russia's Defense Ministry openly opposed release of the first *Tallinn Manual* with the following language: "Russia is trying to prevent the militarization of cyberspace by urging the international community to adopt a code of conduct in this sphere, the US and its allies are already agreeing to the rules for prosecuting cyber warfare."⁵¹ Russian experts did profess optimism that "compromise is possible" on the *Tallinn Manual* provisions.⁵²

US Position on Proxy Hackers

In his Berkeley speech, Brian Egan underscored the US's strong position on proxy hackers:

Additionally, cyber operations conducted by non-State actors are attributable to a State under the law of state responsibility when such actors engage in operations pursuant to the State's instructions or under the State's direction or control, or when the State later acknowledges and adopts the operations as its own. Thus, as a legal matter, States cannot escape responsibility for internationally wrongful cyber acts by perpetrating them through proxies. When there is information—whether obtained through technical means or all-source intelligence—that permits a cyber act engaged in by a non-State actor to be attributed legally to a State under one of the standards set forth in the law of

state responsibility, the victim State has all of the rights and remedies against the responsible State allowed under international law.⁵³

This broad statement mirrors the Tallinn Manuals. Indeed, it closely tracks with Rule 17 of *Tallinn Manual 2.0* “Attribution of cyber operations by non-State actors,”⁵⁴ which makes sense given the law of State responsibility is well settled as a matter of international law.⁵⁵ Also of note is the position that the victim State can use “all of the rights and remedies” under international law.⁵⁶ This means that the US reserves the right to use military force to counter a cyber-attack conducted by non-State proxy hackers.⁵⁷

Effective Control and Due Diligence

As mentioned above, and as Brian Egan reiterates, the international law that governs States responsibly for proxy hackers is premised either because they are operating as a State organ or that the State exercises effective control over the proxy under the international law of attribution.⁵⁸ This term “effective control” has also been called “direction and control” in other contexts.⁵⁹ If a State exercises effective control over the proxy, then it assumes responsibility for the actions of the proxy in international law. This rule of effective control predates the Internet, and comes from the 1986 International Court of Justice (ICJ) case of *Nicaragua v. United States of America*.⁶⁰ That case, stemming from the Iran-Contra affair, resulted in the Nicaraguan government holding the US legally responsible for military and paramilitary Contras activities based on the “effective control” the US exercised over the Contras.⁶¹

Even absent a proxy acting under the effective control of a State or acting as an organ of the State, a State may still be held responsible under international law for supporting or enabling the proxy.⁶² The type of support varies, but could include providing software, monetary incentives, or even sanctuary from prosecution under domestic laws.⁶³ Failing evidence of attribution of support or enabling behavior by a State, a State likely cannot be held responsible for the actions of the proxy hackers.⁶⁴

However, the international law principle of due diligence may provide another avenue for holding a State responsible for the actions of proxy hackers. Due diligence, as discussed above and in *Tallinn Manual 2.0*, generally requires a State to take action both to prevent their territory and infrastructure from being used to launch cyberspace operations against another State, and to take feasible actions to stop such cyberspace operations if aware of them.⁶⁵ Due diligence does not require a nation to prevent cyberspace operations, just to stop once it becomes aware.⁶⁶ If State A knows that proxy hackers are using State B infrastructure to launch cyberspace operations against State A, and State A informs State B of these operations, then State B is duty-bound to stop the proxy hackers, if feasible. If State B refuses or is unable to stop the proxy hackers, then State A can take reasonable countermeasures to end those cyberspace operations. State A’s countermeasures against State B would normally violate international law, but due to State B’s failure or refusal to act, these countermeasures become lawful.⁶⁷

Applying the due diligence principle can be complicated because its parameters often depend upon the capabilities of both the victim State and the perpetrating State. Due diligence for the US means a fairly high standard, while due diligence for other States without as much cyberspace sophistication “migrate the standard downward.”⁶⁸ Applying the same standard to a country with minimal cyberspace infrastructure would not work in the international law context. However, States like Russia might take advantage of this lower standard. One common hacker scheme to conceal attribution is the short-term leasing of servers in various countries, including the US, from which to launch cyberspace operations. Once the operation concludes, and long before attribution is established, the hacker terminates the lease and relocates, making attribution even tougher.⁶⁹ This leasing scheme can render due diligence very difficult, if not impractical, particularly in States of modest sophistication.

Other International Laws and Norms

To reiterate, typically victim States do not employ military force to counter hackers, but rely instead on criminal prosecution, which has become an international norm. For example, the US has indicted proxy hackers in the past, as has Estonia. The US indicted Alexsey Belan three times for proxy attacks, most notably for hacking 500 million Yahoo accounts in 2012-2013.⁷⁰ Estonia charged and convicted one Estonian student from Russia, Dmitri Galushkevich, with targeting a political party website related to the 2007 cyber-attack,⁷¹ and there are other high-profile indictments of note.⁷² Again, absent effective extradition, holding Russia accountable for proxy hackers can be futile.⁷³ Indeed, Alexsey Belan remains at large and on the FBI’s most wanted list.⁷⁴

Other norms that have developed over time include the use of sanctions to deter hackers. On December 29, 2016, along with the indictments noted above, the US imposed sanctions on Belan,⁷⁵ under Executive Order 13694, “Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities,” as amended by Executive Order 13757, “Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities,” signed on December 28, 2016.⁷⁶ These sanctions froze Belan’s assets, along with the assets of another individual, Evgeniy Bogachev.

In addition to these measures, several high-profile legal advisors recommend a slow and steady approach to building international norms in cyberspace. Colonel (Ret.) Gary Corn, former USCYBERCOM Staff Judge Advocate, recommends that States not prematurely support international laws and norms in cyberspace, because nefarious actors will attempt to exploit States that artificially limit their cyberspace operations in support of these not yet fully developed laws and norms.⁷⁷ Brigadier General George Smawley recommends a gradual shaping of international norms to tackle the problem of proxy hackers.⁷⁸ Major General Berger urges a deliberate process in building norms *lex lata* (what the law is) without ceding to the international community pressure to build law *lex ferenda* (what the law should be).⁷⁹ The alternative approach would be to establish an international commission and attempt to create a

Hague treaty or a new Geneva Convention to govern cyber law. This approach, in the absence of more fully developed international norms would suffer from a lack of consensus. Indeed, even the IGE representatives who drafted the Tallinn Manuals do not always agree on the rules.⁸⁰ Even the definition of sovereignty has led to disagreements between the US and its closest allies and partners, let alone between the US and its adversaries, such as Russia.⁸¹

Colonel (Ret.) Gary Brown, USCYBERCOM's first Staff Judge Advocate, recommends the US make clear its *opinio juris* (opinion of law) regarding how international law should govern cyberspace activities.⁸² That "line in the sand" approach could advance development of international law and norms. Colonel (Ret.) Brown views the Tallinn Manuals as "a starting point from which to deviate" in this regard.⁸³

Review of Recent Proxy Hacker Events

To better understand some of the challenges of applying international law to proxy hackers, examples are summarized below.

Estonia

In 2007, Estonia suffered one of the first well-documented cyberspace operations. Early that year, the Estonian government planned to move a statue from the center of Tallinn, the Estonian capital, to a military cemetery on the outskirts of town. This Soviet Union-era statue, originally called the "Monument to the Liberators of Tallinn," but now known as the "Bronze Soldier," honored the Soviet defeat of the Nazis in Estonia in 1944.⁸⁴ The statue was controversial. Ethnic Estonians viewed the statue as a reminder of the harsh Soviet occupation from 1944 until the fall of the Soviet Union, while ethnic Russians living in Estonia saw it as a monument to victory over the Nazis and the Soviet claims on Estonia.⁸⁵ The planned statue move offended many Russians living in Estonia and offended senior officials in Russia. Sergei Lavrov, Russian Foreign Minister, threatened, "[Removal of the memorial and the ensuing clashes] is disgusting. ... There can be no justification for this blasphemy. It will have serious consequences for our relations with Estonia."⁸⁶

After the statue was moved, Russia launched a coordinated distributed denial of service (DDOS) operation, targeting the Estonian government itself, including "the President, Parliament, police, political parties, and major media outlets."⁸⁷ This DDOS lasted over three weeks and cost Estonia billions of euros.⁸⁸ The operation appeared to come from patriotic hackers sympathetic to Russia.⁸⁹ Estonia charged and convicted one Estonian student from Russia, Dmitri Galushkevich, with targeting a political party website.⁹⁰ Yet, further attribution for the DDOS operation remained elusive. Some of the sources of the operation appeared to be in Transnistria, a pro-Russian breakaway republic situated between Moldova and Ukraine, and some Russian officials claimed responsibility for the DDOS.⁹¹ Officially, Russia denied involvement, even claiming they too were victims of the DDOS operation.⁹²

This DDOS operation, combined with other physical measures implemented by Russia, had a devastating impact on Estonia. At the same time as the cyberspace operation, Russia severed rail line traffic with Estonia for “repairs.”⁹³ The DDOS operation also threatened to undermine public confidence in Estonia’s government, particularly when loss of access to banking services occurred for several hours.⁹⁴ Finally, the operation appeared tailored to avoid triggering Article V of the NATO Treaty, the collective defense provision that renders “attack against one . . . shall be considered an attack against them all.”⁹⁵ Estonia would have had difficulty describing how a DDOS operation qualified as an armed attack under this provision. While it caused losses and created confusion, such an attack does not cross the “threshold for reprisals.”⁹⁶

These cyberspace operations prompted NATO and Estonia to enhance their defenses. First, Estonia hardened its cyberspace defenses in light of this operation.⁹⁷ Second, NATO recognized and certified the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) in Tallinn in 2008.⁹⁸ Finally, the NATO CCD COE invited the International Group of Experts (IGE) in 2009 to create the first of two Tallinn Manuals (discussed earlier in this paper).

The primary principle of international law that could have been applied to hold Russia accountable for the DDOS attack was due diligence. While specific attribution remained elusive, Estonia built a compelling factual case that only Russian-backed proxy actors could have launched the DDOS attack.⁹⁹ This was true even if the Russian government did not specifically direct the proxy hackers. Additionally, the hackers that facilitated the DDOS attack from Transnistria could have been identified as mercenaries.¹⁰⁰ As a result, they could have faced criminal prosecution for their actions, assuming extradition would have allowed Estonia to gain jurisdiction over those proxy hackers.¹⁰¹ Claiming combatant immunity under international law obviously would be non-availing for the hackers.

Georgia

The 2007 attack on Estonia was just the start of Russia’s large-scale proxy cyberspace operations. In 2008, Russia invaded South Ossetia in Georgia. Simultaneously, a DDOS operation began against “fifty-four news, government, and financial websites” impacting “thirty-five percent of Georgia’s Internet networks.”¹⁰² The National Bank of Georgia “had to suspend all electronic services” for eleven days due to the attacks.¹⁰³

As with the Ukrainian example discussed at the beginning and again below, Russia launched these cyberspace-operations as part of its information warfare campaign. By disabling and disrupting the Georgian government’s ability to communicate with its people, Russia was able to fill the void with its own false narrative of the invasion and falsely claim legal legitimacy.¹⁰⁴ This false narrative did not fool international third-parties as to Russia’s claims on South Ossetia, but it did temporarily sow doubts about Russia’s invasion at the local level.¹⁰⁵

Proxy hackers conducted most of these operations against Georgia. Motivated in part by patriotism, these hackers received marching orders through hacker forums which provided “tools, vulnerabilities, and target lists” for the hackers to use.¹⁰⁶ Russia denied directing these proxy hackers, but these denials strain credulity when the timing and nature of these operations coincided with Russia’s invasion of South Ossetia.¹⁰⁷

Russia was clearly responsible under international law for the proxy hackers’ cyber-attacks on Georgia. Apart from the telltale timing coinciding with the invasion, the presence of hacker forums that supplied tools and target lists proves Russia’s control over these hackers beyond any rational doubt.

Ukraine

Russia learned from its experiences in Estonia and Georgia when launching its operations against Ukraine in 2014. Coinciding with Russia’s invasion of Crimea, Ukraine faced a massive DDOS operation 32 times the size of the attacks on Georgia.¹⁰⁸ Apart from the sheer scale, what made this DDOS operation different was Ukraine’s deployment of proxy hackers to counter by hacking Russian interests, who succeeded in defacing the Russia Today website, replacing the word Russia with Nazi.¹⁰⁹

These DDOS operations made up just one portion of the cyberspace operations conducted by both Russia and Ukraine over a period of several years. As noted above, Russia employed dozens of proxy trolls to engage in information warfare in support of their operations in Ukraine in 2014.¹¹⁰ These cyberspace operations continued throughout 2015, when Russian cyber-attacks disabled the Ukrainian power grid for several hours.¹¹¹ Later investigations revealed that the malware that disabled the grid was intended to physically damage it.¹¹² Normally only State governments have the resources to develop this type of cyber weapon, as evidenced by the Stuxnet cyber-attack against Iran.¹¹³ In October 2020, the US indicted six persons for the power grid attack in Ukraine. All six indicted individuals work as officers of Russia’s GRU military intelligence agency.¹¹⁴ Proxy hackers rarely will have access to such a dangerous type of cyber weapon.¹¹⁵ Among other take aways, the tit-for-tat cyberspace operations in Ukraine, with both proxy and non-proxy means, underscores the challenge of properly identifying cyber-attackers.

Under international law, the DDOS operation against Ukraine mirrored the Russian efforts in Georgia. Russia continued to exercise effective control over the proxy hackers and coordinated the operation to coincide with its invasion of Crimea. Separately, the sophisticated power grid cyber-attack could not have come from any source without direct Russian government involvement, as evidenced by the US indictment tying six Russian officials to the attack.

In March of 2022, Ukraine struck back with massive proxy attacks of its own, with over 300,000 people known as the “IT Army of Ukraine” working to disrupt the Russian government.¹¹⁶ This group “has organized . . . distributed denial of service attacks on Russian

state websites,” and attempted to inform the Russian people “about what is actually going on in Ukraine.”¹¹⁷

Proposed Actions to Counter Future Russian Proxy Hackers

Several theories of strategy formulation could help the US develop a policy to counter future Russian proxy hackers, coercion theory remains the most relevant and applicable. As analyzed below, this theory allows the US to gradually escalate measures against Russia in a manner that complies with international laws and norms.

Coercion Theory

Coercion theory has two main methods, both of which have importance when countering proxy hackers. The first method, deterrence, seeks to use threats to prevent an actor (State or non-State) from taking an action it might otherwise take.¹¹⁸ Deterrence threats can be threats of punishment or threats of denial.¹¹⁹ The threat of denial seeks to deter by convincing the target state that it will not achieve its aim (that the aim will be denied).¹²⁰ The threat of punishment seeks to deter by convincing an actor that the coercer will inflict retaliatory punishment that exceeds the value of the desired stake.¹²¹ In the case of cyber, deterrent threats can be used to dissuade actors from engaging in hacking and cyber-generated disruption of all forms.

Actors can be deterred for many reasons, thus allowing “enemies who have been deterred to save face,” because the reasons behind a successful deterrence remain unclear.¹²² The coercive threat might have caused the deterrent effect, or maybe something else entirely, which allows a State to attribute the reason they failed to act on whatever they can plausibly claim.¹²³

The second method, compellence, seeks to force the target State to perform an act it would otherwise prefer not to perform, or to cease an act it has already started.¹²⁴ Because successful compellence forces the actor to take an action it would prefer not to take, there is no ambiguity or ability to save face. Actors typically do not want to be humiliated; they will seek therefore to evade or resist compellent threats. Other inherent challenges also make successful compellence difficult. First, timing is important. There must be a deadline that allows sufficient time for the target State to act, but at the same time places it on notice that consequences will occur by that deadline if no action has taken place.¹²⁵ Second, the coercing state “must convey specific information to the actor being coerced.”¹²⁶ Without that specificity, compellence will fail.

Despite its drawbacks, coercion theory remains a useful framework for dealing with US adversaries. By structuring a chain of escalatory threats and actions tethered to international law, the US can succeed in deterring or terminating adverse cyberspace operations.

Defend Forward and Persistent Engagement

In 2018, the US released the Department of Defense Cyber Strategy. One key provision,

“Persistently contest malicious cyber activity in day-to-day competition,” referred to as the “persistent engagement” or “defend forward” policy, has come to define USCYBERCOM operations.¹²⁷ The goal of defend forward is “the use of Defense Department cyber capabilities during day-to-day competition to disrupt or halt malicious cyber activity at or as close as practicable to its source.”¹²⁸ Deterrence was not the specific goal of defend forward, but “[t]o the extent that defend forward contributes to deterrence, it does so incidentally by improving overall defense, reducing the likelihood of adversary operational success, and thereby constraining the adversary’s strategic options and resetting its benefit calculus.”¹²⁹

One way that defend forward constrains the enemy, and imposes costs on proxy hackers, is USCYBERCOM’s “practice of uploading malware samples to the VirusTotal website that are discovered through persistent engagement’s routine operations and campaigns.”¹³⁰ Brig. Gen. Smawley agreed that imposing direct costs on proxy hackers works.¹³¹ He described a typical defend forward operation, done with the consent of the host State, where the cyber operators search for malware and then publicly advertise the capture of the malware through cooperation with the Department of Homeland Security (DHS), which typically tweets about the operation.¹³² This causes public shaming of the hacker amongst his or her peers, and it makes worthless the money and time the hacker invested in the malware. The latter becomes worthless once DHS shares information with commercial entities that then patch systems to prevent the malware from working.¹³³

Recommendations

The US can and should use both deterrence and compellence to counter the threat from Russian proxy hackers. Both methods follow existing international law and norms to counter a threat. First, the US can seek to deter actions, or compel Russia to cease ongoing operations, by threatening to expose and publicly attribute its proxy hackers’ malicious cyberspace activities to Russia. This public attribution, backed with hard evidence of Russian involvement, can cause embarrassment to Russia in the international community. While the US has already attempted this public attribution several times in the past, such as with Alexsey Belan, some critics have noted the absence of hard evidence linking Russia to the proxy.¹³⁴ Whether or not there is hard evidence, Russia inevitably will continue to falsely claim innocence, and/or claim as they did in Estonia in 2007 to be a victim of the same attacks.¹³⁵ But calling Russia out will take a toll.

And when the threat of public embarrassment fails to deter Russia from using proxy hackers, the US should consider an escalatory campaign using all elements of national power – Diplomatic, Information, Military, and Economic (DIME). Any communicated threat that does not achieve the desired result should be followed by increasingly coercive actions to compel Russia to cease their use of proxy hackers. For example, diplomatic efforts should include specific threats of actions to be taken by a certain date if Russia does not take concrete and verifiable actions to stop proxy hackers. The specific threats could start with strong

economic sanctions and later progress to a proportional use of military force. This effort at compellence comes with definite risks of escalation, and should the US fail to back up the effort to compel with actions, Russia would then gain the upper hand because the threat of such actions would ring hollow in the future.

The table below depicts one possible progression of efforts to deter proxy hackers backed by State adversaries:

Table 1. Progression of Coercive Efforts.¹³⁶

Phases	Phase 1	Phase 2	Phase 3	Phase 4
Possible US Deterrent Threats or Compellent Actions	<ul style="list-style-type: none"> Public attribution of attacks backed by hard evidence Diplomatic conversations with specific future actions and timelines 	<ul style="list-style-type: none"> Criminal prosecution of proxy hackers Sanctions against Russian Government Officials and all known hackers 	<ul style="list-style-type: none"> Preliminary cyberspace operations against Russian interests backed by public statements Military assets aligned against the Russian interests as a show of force 	<ul style="list-style-type: none"> Serious offensive cyberspace operations against Russian interests backed by public statements Military force used against Russian cyber infrastructure
International Law or Norm Applicable	<ul style="list-style-type: none"> <i>Tallinn Manual 2.0</i> Rule 17, Attribution of Cyber Operations by Non-State Actors¹³⁷ International Norm 	<ul style="list-style-type: none"> <i>Tallinn Manual 2.0</i> Rule 13, International Cooperation in Law Enforcement¹³⁸ International Norm 	<ul style="list-style-type: none"> <i>Tallinn Manual 2.0</i> Rule 20, Countermeasures, (General Principle)¹³⁹ <i>Tallinn Manual 2.0</i> Rule 71, Self-Defence against Armed Attack¹⁴⁰ International Norm 	<ul style="list-style-type: none"> <i>Tallinn Manual 2.0</i> Rule 23, Proportionality of Countermeasures¹⁴¹ <i>Tallinn Manual 2.0</i> Rule 20, Countermeasures, (General Principle)¹⁴² <i>Tallinn Manual 2.0</i> Rule 71, Self-Defence against Armed Attack¹⁴³

The US can take additional steps where appropriate, but with the same desired effect; that is, a coerced Russia that is both deterred from supporting future proxy hacker attacks and compelled to stop proxy hackers from launching attacks from Russia.

Coercion has successfully worked in the past. One example from a real-world operation came after the downing of a \$150 million drone by Iran in 2019.¹⁴⁴ The US could arguably have responded with a kinetic armed response under the UN Charter, Article 2(4), which states “All members shall refrain in their international relations from the threat of force or the use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations.”¹⁴⁵ This article is usually invoked by States as the right to self-defense. However, the US responded with non-kinetic cyberspace operations instead.¹⁴⁶ While this bypassed lower steps in the recommended deterrence or compellence actions, it shows the flexibility of coercion theory. It also illustrates application of the principle of proportionality: as noted in the reference, Iran’s attack on the drone did not lead to a loss of life, but an armed attack against the missile base that shot down the drone almost surely would have. In other words, depending on the severity of the attack, a nation could skip directly to military force under a theory of self-defense, but proportionality may well indicate a better course of action.

CONCLUSION

As a leader in cyberspace operations, the US should, whenever possible, openly and transparently call Russia out for its flagrant violations of international law and norms and its support of proxy hackers. Absent public efforts by the US, Russia and other adversaries will continue to be emboldened to leverage proxy hackers. ~~Unchecked, proxy hacking attacks will further undermine the rule of law in cyberspace and increasingly threaten if not cause irreparable harm to the international community. Unabated, proxy hacker attacks will spread disinformation, undermine public confidence in governments and diminish the ability of countries to maneuver freely in cyberspace.~~

~~The US should prioritize efforts to continue to defend forward and impose costs on proxy hackers and their supporters. Meanwhile, specific application of deterrence and compellence theories against proxy hacker efforts by Russia, combined with an effort to further develop international law and norms will help combat the problem. Over time, the use of proxy hackers may diminish under the pressure of such sustained efforts by the US and its partners.~~ 🛡️

NOTES

1. Harold Hongju Koh, State Department Legal Adviser, “International Law in Cyberspace” (lecture, USCYBERCOM Inter-Agency Legal Conference, Fort Meade, MD, September 18, 2012), <http://opiniojuris.org/2012/09/19/harold-koh-on-international-law-in-cyberspace/>.
2. Thomas Deen, “Russian Expansion and the Development of Hybrid Warfare,” *War Room* (blog), United States Army War College, November 24, 2020, <https://warroom.armywarcollege.edu/articles/russian-expansion/>.
3. Deen, “Russian Expansion and the Development of Hybrid Warfare.”
4. *Ibid.*
5. *Ibid.*
6. *Ibid.*
7. Ionut Ilascu, “Ransomware gangs, hackers pick sides over Russia invading Ukraine,” *Bleeping Computer*, February 25, 2022, <https://www.bleepingcomputer.com/news/security/ransomware-gangs-hackers-pick-sides-over-russia-invading-ukraine/>.
8. Bill Toulas, “Russian hackers start targeting Ukraine with Follina exploits,” *Bleeping Computer*, June 13, 2022, <https://www.bleepingcomputer.com/news/security/russian-hackers-start-targeting-ukraine-with-follina-exploits/>.
9. *Merriam-Webster Dictionary*, s.v. “proxy,” accessed February 15, 2021, <https://www.merriam-webster.com/dictionary/proxy>.
10. Tim Maurer, “‘Proxies’ and Cyberspace,” *Journal of Conflict & Security Law* 21, no. 3 (2016): 387.
11. Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge, UK: Cambridge University Press, 2013), Rule 6, 29.
12. *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Rule 6, Commentary note. 2., 29.
13. *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Rule 6, Commentary note. 10, 32.
14. *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Rule 6, Commentary note. 11, 33.
15. *Ibid.*
16. Michael N. Schmitt and Liis Vihul, eds., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge, UK: Cambridge University Press, 2017), Rule 17, Commentary n. 9, 97.
17. Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge, UK: Cambridge University Press, 2018), 76-78.
18. Maurer, 76-78.
19. Major General Joseph Berger, telephonic interview by author, February 9, 2021.
20. Brigadier General George R. Smawley, telephonic interview by author, February 9, 2021.
21. Smawley, interview. The fourth category, criminal organizations, falls outside of USCYBERCOM’s jurisdiction, barring a nexus to Violent Extremist Organizations (VEOs) or an operation directed against the Department of Defense Information Network (DODIN). Criminal organizations are handled primarily by the Department of Homeland Security (DHS).
22. U.S. Senate Select Committee on Intelligence, *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 2: Russia’s Use of Social Media with Additional Views*, 116th Cong., 1st sess., 2018, S Rep. 116-290, 18-19.
23. Select Committee on Intelligence, 20.
24. *Ibid.*, 21.
25. *Ibid.*, 21.
26. Berger, interview.
27. *Tallinn Manual on the International Law Applicable to Cyber Warfare*, title page.
28. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 3.
29. *Tallinn Manual 2.0*, 1-2.
30. *Ibid.*, 3.
31. Eric Geller, “U.S. Charges Russian Hackers with Sweeping Campaign of Cyberattacks,” *Politico*, October 19, 2020, <https://www.politico.com/news/2020/10/19/russia-hackers-cyberattacks-430166>. NATO Report, *2007 Cyber Attacks on Estonia*, NATO Strategic Communications Centre of Excellence, <https://stratcomcoe.org/hybrid-threats-2007-cyber-attacks-estonia>, 61.

NOTES

32. See discussion accompanying notes 35 and 71 below regarding extradition rules and the case of Alexsey Belan, whom Russia has not extradited to the United States.
33. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 13, 75.
34. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 13, 75.
35. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 13, Commentary note. 8, 77.
36. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 14, 84.
37. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 14, Commentary note. 1, 84.
38. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 14, Commentary note. 5, 85.
39. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 94.
40. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 94.
41. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Table of Concordance, xxxviii-xli.
42. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 6, 30.
43. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 6, 30.
44. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 6, 30.
45. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 7, 43.
46. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 7, Commentary note. 14, 46.
47. Martin Libicki, “Setting International Norms on Cyberwar Might Beat a Treaty,” *US News & World Report*, June 8, 2012, <https://www.usnews.com/debate-club/should-there-be-an-international-treaty-on-cyberwarfare/setting-international-norms-on-cyberwar-might-beat-a-treaty>.
48. For example, Convention (III) Relative to the Treatment of Prisoners of War, Geneva, August 12, 1949, <https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/INTRO/375?OpenDocument>.
49. Martin Libicki, “Correlations Between Cyberspace Attacks and Kinetic Attacks,” *12th International Conference on Cyber Conflict* (Tallinn, Estonia: NATO CCDCOE Publications, 2020), 204, https://ccdcoe.org/uploads/2020/05/Cy-Con_2020_11_Libicki.pdf.
50. Brian J. Egan, State Department Legal Adviser, “Remarks on International Law and Stability in Cyberspace” (lecture, Berkeley Law School, Berkeley, CA, November 10, 2016), <https://2009-2017.state.gov/s/l/releases/remarks/264303.htm>.
51. Elena Chernenko, “Russia Warns against NATO Document Legitimizing Cyberwars,” *Russia Beyond*, May 29, 2013, https://www.rbth.com/international/2013/05/29/russia_warns_against_nato_document_legitimizing_cyberwars_26483.html.
52. Chernenko.
53. Brian J. Egan, State Department Legal Adviser, “Remarks on International Law and Stability in Cyberspace” (lecture, Berkeley Law School, Berkeley, CA, November 10, 2016), <https://2009-2017.state.gov/s/l/releases/remarks/264303.htm>.
54. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 17, 94.
55. Trevor McDougal, “Establishing Russia’s Responsibility for Cyber-Crime Based on Its Hacker Culture,” *Brigham Young University International Law & Management Review* 11, no. 2 (August 1, 2015): 67, <https://digitalcommons.law.byu.edu/cgi/viewcontent.cgi?article=1129&context=ilmr>.
56. Brian J. Egan, State Department Legal Adviser, “Remarks on International Law and Stability in Cyberspace” (lecture, Berkeley Law School, Berkeley, CA, November 10, 2016), <https://2009-2017.state.gov/s/l/releases/remarks/264303.htm>.
57. Libicki, “Correlations Between Cyberspace Attacks and Kinetic Attacks.”
58. *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Rule 6, Commentary note. 10, 32.
59. Compare *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Rule 6, Commentary note. 10, 32 (effective control) with *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 17, 94 (direction and control).
60. International Court of Justice, Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America), Judgment of June 27, 1986, para. 292, 136.
61. *Nicaragua v. United States of America*, para. 1, 16.

NOTES

62. Colonel Gary Corn, U.S. Army Retired, telephonic interview by author, February 3, 2021.
63. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 17, Commentary note. 9, 97.
64. Corn, interview.
65. Corn, interview. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 6, 30, and Rule 7, 43.
66. Corn, interview.
67. Corn, interview. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 20, 111.
68. Colonel Gary Brown, U.S. Air Force Retired, telephonic interview by author, January 29, 2021.
69. Smawley, interview.
70. “Most Wanted,” Federal Bureau of Investigation, last modified March 15, 2017, <https://www.fbi.gov/wanted/cyber/alexsey-belan>.
71. NATO Report, 61.
72. Geller.
73. See discussion accompanying note. 35 above.
74. “Most Wanted.”
75. US Department of the Treasury, “Sanctions Actions Pursuant to Executive Order 13694,” *Federal Register* 82, no. 3 (December 29, 2016): 1424, <https://www.govinfo.gov/content/pkg/FR-2017-01-05/pdf/2016-32017.pdf>.
76. Barack Obama, Executive Order 13694, “Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities,” *Federal Register* 80, no. 63 (April 2, 2015): 18077, <https://www.govinfo.gov/content/pkg/FR-2015-04-02/pdf/2015-07788.pdf>. Barack Obama, Executive Order 13757, “Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities,” *Federal Register* 82, No. 1 (January 3, 2017): 1, <https://www.govinfo.gov/content/pkg/FR-2017-01-03/pdf/2016-31922.pdf>.
77. Corn, interview. For example, the IGE has already begun work on a new Tallinn Manual 3.0. The provisions from that new Manual might change or influence State practice. The website announcement specifically states, “The comprehensive 2017 edition will be updated in the light of emerging State practice,” showing that the law is still evolving. “CCDCOE to Host the Tallinn Manual 3.0 Process,” CCDCOE, last accessed on March 14, 2021, <https://ccdcocoe.org/news/2020/ccdcocoe-to-host-the-tallinn-manual-3-0-process/>.
78. Smawley, interview.
79. Berger, interview.
80. For example, the IGE could not agree on whether a State must disclose “evidence on which attribution is based whenever taking actions in response to cyber operations that purportedly constitute an internationally wrongful act.” *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Commentary note. 13, 83.
81. Smawley, interview.
82. Brown, interview.
83. Ibid.
84. NATO Report, 53. Damien McGuinness, “How a Cyber Attack Transformed Estonia,” BBC News, April 27, 2017, <https://www.bbc.com/news/39655415>.
85. NATO Report, 56, 58.
86. NATO Report, 58. Other writers have compared the controversial nature of the “Bronze Soldier” statue to that of Confederate statues in the United States. Andrew Stuttaford, “Confederate Statues and the Bronze Soldier of Tallinn,” *National Review*, August 17, 2017, <https://www.nationalreview.com/corner/confederate-statues-and-bronze-soldier-tallinn/>.
87. NATO Report, 55.
88. NATO Report, 53.
89. NATO Report, 59.
90. NATO Report, 61.
91. NATO Report, 61.
92. NATO Report, 53, 58-59.

NOTES

93. NATO Report, 53.

94. NATO Report, 61.

95. Article V reads, in part:

The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.

The North Atlantic Treaty, Washington, DC, April 4, 1949, art. 5.

96. NATO Report, 68.

97. NATO Report, 67.

98. NATO Report, 67.

99. NATO Report, 69.

100. *Tallinn Manual 2.0*, “Mercenaries” (Rule 90), states, “Mercenaries involved in cyber operations do not enjoy combatant immunity or prisoner of war status.” *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 90, 412. This means that any proxy hacker acting under color of authority from a State cannot avoid prosecution for its actions under international law, if they meet the six-part test from Article 47 of Additional Protocol I to the Geneva Conventions. That six-part test consists of:

A mercenary is any person who: (a) is specially recruited locally or abroad in order to fight in an armed conflict; (b) does, in fact, take a direct part in the hostilities; (c) is motivated to take part in the hostilities essentially by the desire for private gain and, in fact, is promised, by or on behalf of a Party to the conflict, material compensation substantially in excess of that promised or paid to combatants of similar ranks and functions in the armed forces of that Party; (d) is neither a national of a Party to the conflict nor a resident of territory controlled by a Party to the conflict; (e) is not a member of the armed forces of a Party to the conflict; and (f) has not been sent by a State which is not a Party to the conflict on official duty as a member of its armed forces.

Protocol Additional to the Geneva Conventions of August 12, 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), June 8, 1977, art. 47, Mercenaries, <https://ihl-databases.icrc.org/ihl/We-bART/470-750057>.

101. See discussion accompanying note. 35 above.

102. Sarah P. White, “Understanding Cyber Warfare: Lessons from the Russia-Georgia War,” *Modern War Institute*, 1, <https://mwi.usma.edu/wp-content/uploads/2018/03/Understanding-Cyberwarfare.pdf>.

103. White, 1.

104. *Ibid.* 4.

105. *Ibid.* 5.

106. *Ibid.* 6.

107. David Hollis, “Cyberwar Case Study: Georgia 2008,” *Small Wars Journal* 2, January 6, 2011, <https://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf>.

108. Robert Windrem, “Timeline: Ten Years of Russian Cyber Attacks on Other Nations,” *NBC News*, December 18, 2016, <https://www.nbcnews.com/storyline/hacking-in-america/timeline-ten-years-russian-cyber-attacks-other-nations-n697111>.

109. Pierluigi Paganini, “Crimea – The Russian Cyber Strategy to Hit Ukraine,” *INFOSEC*, March 11, 2014, <https://resources.infosecinstitute.com/topic/crimea-russian-cyber-strategy-hit-ukraine/>.

110. Deen.

111. Andy Greenberg, “New Clues Show How Russia’s Grid Hackers Aimed for Physical Destruction,” *Wired*, September 12, 2019, <https://www.wired.com/story/russia-ukraine-cyberattack-power-grid-blackout-destruction/>.

112. Greenberg.

113. Josh Fruhlinger, “What Is Stuxnet, Who Created It and How Does It Work?” *CSO Online*, August 22, 2017, <https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html>.

NOTES

- 114. Geller.
- 115. David Kushner, “The Real Story of Stuxnet,” *IEEE Spectrum*, February 26, 2013, <https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet>.
- 116. Christopher Hutton, “IT Army of Ukraine: 300,000 hackers work together to fight Russia online,” *Washington Examiner*, March 15, 2022, <https://www.washingtonexaminer.com/news/it-army-of-ukraine-300-000-hackers-work-together-to-fight-russia-online>.
- 117. Hutton.
- 118. Tami Davis Biddle, “Coercion Theory: A Basic Introduction for Practitioners,” *Texas National Security Review* 3, no. 2 (Spring 2020): 98, <https://tnsr.org/2020/02/coercion-theory-a-basic-introduction-for-practitioners/>.
- 119. Biddle, 101.
- 120. *Ibid.*, 101.
- 121. *Ibid.*, 101.
- 122. *Ibid.*, 102.
- 123. *Ibid.*, 102.
- 124. *Ibid.*, 98-99.
- 125. *Ibid.*, 102.
- 126. *Ibid.*, 102.
- 127. Department of Defense, Cyber Strategy, 2018, 4, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.
- 128. Gary Corn, “SolarWinds Is Bad, but Retreat From Defend Forward Would Be Worse,” *Lawfare*, January 14, 2021, <https://www.lawfareblog.com/solarwinds-bad-retreat-defend-forward-would-be-worse>.
- 129. Corn.
- 130. Michael P. Fischerkeller and Richard J. Harknett, “Persistent Engagement and Cost Imposition: Distinguishing Between Cause and Effect,” *Lawfare*, February 6, 2020, <https://www.lawfareblog.com/persistent-engagement-and-cost-imposition-distinguishing-between-cause-and-effect>.
- 131. Smawley, interview.
- 132. *Ibid.*
- 133. *Ibid.*
- 134. Roger A. Grimes, “Why It’s So Hard to Prosecute Cyber Criminals,” *CSO Online*, December 6, 2016, <https://www.csoonline.com/article/3147398/why-its-so-hard-to-prosecute-cyber-criminals.html>.
- 135. NATO Report, 53, 58-59.
- 136. Table created by author.
- 137. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 17, 94.
- 138. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 13, 75.
- 139. Rule 20 states, “A State may be entitled to take countermeasures, whether cyber in nature or not, in response to a breach of an international legal obligation that is owed by another State.” *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 20, 111.
- 140. Rule 71 states, “A State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defence. Whether a cyber operation constitutes an armed attack depends on its scale and effect.” *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 71, 339.
- 141. Rule 23 states, “Countermeasures, whether cyber in nature or not, must be proportionate to the injury to which they respond.” *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 23, 127.
- 142. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 20, 111.
- 143. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 71, 339.
- 144. David Martin and Grace Segers, “Trump Approved Cyber Attacks against Iran, Sources Say,” *CBS News*, June 23, 2019, <https://www.cbsnews.com/news/pentagon-launched-cyber-attacks-against-iran-with-trumps-backing-sources-say/>.

NOTES

145. United Nations Charter, Article 2(4), San Francisco, CA: United Nations, June 26, 1945, <https://www.un.org/en/charter-united-nations/>.

146. Martin and Segers.

THE CYBER DEFENSE REVIEW

◆ PROFESSIONAL COMMENTARY ◆

Recruit, Train, and Retain DoD Cyber Skills Like Language Skills

Lieutenant Colonel David R. Dixon
Captain Patrick J. Cirenza

INTRODUCTION: DEFICIT IN CYBER TALENT IS A GROWING PROBLEM

How many personnel in the Department of Defense (DoD) can create and use computer code? Using what coding languages? How well? These are straightforward questions, but the answers are unknown, particularly to the personnel management system. The answers could also be a critical part of solving one of the DoD's thorniest problems: filling the ranks of the US military's cyber forces. In May 2019, then acting Secretary of Defense Patrick Shanahan said to Congress, "The scholarship and the recruitment and the retainment of cyber professionals is probably the greatest skill challenge that we have in the Department. There aren't enough software engineers in the world, and there probably never will be."¹ The situation arguably has worsened since then. The Joint Staff Chief Information Officer, Lieutenant General Dennis Crall, in April 2021 testified to Congress,

"I am concerned about pace [of cyber recruitment]. I think the divide between the need is growing compared to what we are able to fulfill. I am not sure we are closing the gap... [we need] a new approach to our thinking."²

In an increasingly cyber-dependent and volatile world with fierce recruitment competition from the private sector, the DoD needs to be more creative in recruiting, training, and retaining cyber talent.

To date, the primary focus of the DoD has been attracting cyber talent from outside.³ However, as the DoD is America's largest employer with 2.91 million employees, it is essential that it also recruit internally to see if already hired personnel can fulfill DoD cyber

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



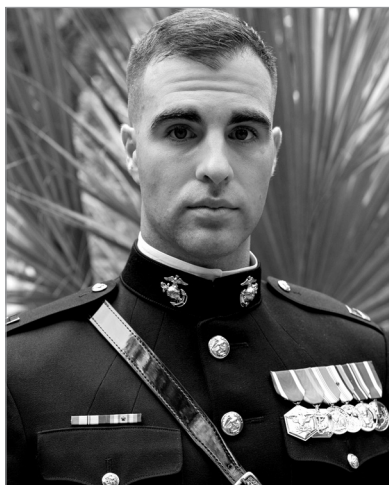
Lieutenant Colonel David R. Dixon is a Marine Corps officer and attack helicopter pilot. He deployed twice to Iraq, once to Japan, and completed flying tours aboard the USS Boxer and USS Essex. He currently works in cyber infrastructure, risk, and resilience for the Department of Homeland Security. Lieutenant Colonel Dixon attended community college before matriculating at Texas A and M University where he graduated with honors as a Lowry Mays Business Fellow. He later earned his master's degrees from the Harvard Graduate School of Education and the Stanford Graduate School of Business.

talent needs.⁴ The services have considered and tried several ways, such as the Army Reserve's Cyber Warrior Database, the Air Force Cyber Aptitude and Talent Assessment, and the Cyber Excepted Service, to find these personnel.⁵ While this experimentation has had mixed successes, the DoD already has a proven program that could perform this essential function - Foreign Language Proficiency Bonuses (FLPB). The 2021 National Defense Authorization Act mandates the DoD to create a coding program similar to FLPB within two years. The DoD uses this congressional mandate to create Coding Language Proficiency Bonuses (CLPB) not only to identify candidates, but also to incentivize the acquisition, maintenance, and development of critical and perishable cyber skills in the military.⁶

A PROVEN SOLUTION: CODING LANGUAGE PROFICIENCY BONUSES

FLPB offers a model that could readily be adapted to efforts to expand the coding language talent base. The FLPB mission is to increase strategic foreign language and dialect capabilities by:⁷

1. **Encouraging Service** members with foreign language and dialect proficiencies to identify their proficiency level.
2. **Incentivizing Service** members to acquire, sustain, and improve foreign language and dialect skills.
3. **Incentivizing Service** members whose military specialty requires a foreign language or dialect to expand their proficiency to other foreign languages and dialects.
4. **Increasing the number of language professionals** operating at proficiency levels 2-5 as defined by the Federal Interagency Language Roundtable (ILR) rating scale in languages and dialects of strategic importance to DoD.⁸



Captain Patrick J. Cirenza is a Marine Corps infantry officer who has deployed to Afghanistan and Japan. He obtained his bachelor's degree from Stanford University and his master's degree from the University of Cambridge where he wrote theses on cyber warfare and cyber espionage.

The FLPB program specifies that military personnel may receive anywhere from 100 dollars to a maximum of 1000 dollars per month if they meet a threshold standard on Defense Language Proficiency Tests (DLPT) or other tests designated by the Defense Language Institute.⁹ The language(s) must be one (or more) that the Under Secretary of Defense for Personnel and Readiness, military department secretaries, and service leadership designate on the DoD Strategic Language List.¹⁰ This leadership group annually reexamines this list and categorizes the languages by importance to current DoD mission sets. The payments are graduated based on the language's payment category, how many languages the speaker knows, and the speaker's skill level. Personnel must retest every twelve months to continue receiving the bonus. In total, the DoD pays about \$84 million a year to around 27,000 service members for certified proficiency in 120 languages and dialects of strategic importance.¹¹

If FLPB can identify people with strategically important language skills within the DoD and encourage them to maintain or expand those skills, CLPB could do the same for Python, C++, Ruby, and other coding languages.¹² Personnel who annually meet the standard on the Defense Cyber Proficiency Test or another test designated by US Cyber Command (USCYBERCOM), which establishes joint cyberspace training and certification standards, could receive the bonus.¹³ The bonus would be adjusted based on the importance of the coding language, the number of coding languages, and the skill level of the programmer. The current leadership group that determines the DoD Strategic Language List could expand to include the Commander of Cyber Command to create a separate DoD Strategic Coding Language List. Like the FLPB, the CLPB program would have the same simple, intuitive, and incentive-driven logic to motivate personnel to self-report their cyber skills as well as maintain and improve them. CLPB could also provide additional financial incentives for civilians with cyber skills to join the military.

Untapped talent potential exists in the DoD personnel pool and harnessing it requires an effective talent management solution. As one example, through one initiative to identify internal specialized skills, the Defense Digital Service found a service member who was extremely talented at calibrating sensors that had been “assigned to count pushups.”¹⁴ He now develops “low-frequency devices that detect and neutralize the threat of drones that drop grenades on special operators.”¹⁵

While it is unlikely that there is an overabundance of cyber talent hidden in the DoD that will meet all the military’s cyber needs, there is certainly some. If even 0.1 percent of DoD personnel have coding abilities that the organization does not know about (which is significantly lower than the estimated 2 to 2.5 percent of the general US population that have some professional knowledge of coding), that is almost 2,900 personnel who could potentially fill the hundreds of vacancies in the cyber forces.¹⁶ A 2017 RAND Corporation study estimates at the lower bound there may be as many as 14,201 soldiers with mid-level cyber expertise, and 890 soldiers with deep expertise, in the Army National Guard and Reserve.¹⁷ As Raj Shah, the former head of Defense Innovation Unit Experimental said, “I think these pockets [of talent] already exist [in the DoD], we just have to identify them [and] cultivate them because the best will get frustrated and leave.”¹⁸

HOW CLPB WOULD HELP RECRUIT, TRAIN, AND RETAIN CYBER TALENT

Recruit

The DoD has many of the pieces of the cyber talent management puzzle already assembled – training pipelines and schools, military occupational specialties, retention bonuses, and existing units. Skilled manpower is the missing piece, and CLPB would help to fill the gap by empowering the DoD to internally recruit and incentivize upskilling within its vast personnel pool. Either through a lack of knowledge, incentive, or directive, there are currently DoD personnel with unreported cyber talent who are not in cyber-related jobs. The main benefit of CLPB would be to have DoD personnel self-identify their cyber skills and prove them through rigorous annual testing, allowing the DoD to have better situational awareness of how they can recruit cyber talent internally – just as it does with language skills. Additionally, CLPB would be another incentivizing tool for recruiters as they look outside the military for cyber talent.

Train

A CLPB program should include annual tests and bonuses adjusted based on the proficiency and type and number of strategically important coding languages; this would provide a powerful incentive for DoD personnel to maintain and improve their cyber skills. Keeping CLPB would be the responsibility of DoD personnel, not the DoD – the powerful logic of the program is that it is driven from the ground up, not the top down. DoD personnel would keep their skills sharp either by training on their own time – as the beneficiaries of FLPB do – or by volunteer-

ing to attend schools for which CLPB could make them eligible. The Defense Language Institute Foreign Language Center (DLIFLC) provides an excellent model both for flexible, self-paced online learning and for intensive in-person courses that could be replicated for coding.

Retain

Once the CLPB program identifies, maintains, and develops latent cyber talent, it can feed DoD personnel into the multiple existing cyber retention programs and act as a force multiplier. Beyond the CLPB, there are already several bonuses and benefits with similar aims, such as the Selective Reenlistment Bonus, through which the Army pays up to \$82,000 to soldiers with cyber skills for a six-year reenlistment.¹⁹ Bonuses like CLPB on top of base pay are essential for retaining cyber talent – especially when competing with the private sector or even other government agencies. For context, beginning in 2021 the Department of Homeland Security will be able to hire cyber professionals with a salary of \$255,800 – the Vice President’s salary – or up to 150% (\$322,100) of it “in special circumstances.”²⁰

CLPB could also serve as a feeder for DoD exclusive units and mission sets. FLPB currently works in this role as a powerful retention tool that already keeps many personnel who could earn more in the private sector. Recipients of FLPB are both notified of and are eligible for jobs in the US Defense Attaché Offices, Security Cooperation Offices, and International Health Specialists, among others.²¹ CLPB could do the same with USCYBERCOM, the National Security Agency, or the Department of Homeland Security. These jobs have unique mission sets that are often not legal or found at a comparable scale in the private sector; and they would train DoD personnel in elite skills for immediate deployment rather than in a theoretical or limited capacity.

THE WAY FORWARD

How much are the answers to the questions posed at the start of this article worth to the US military? That is difficult to quantify, but the costs of the cyber skills gap are easy to estimate. Fortinet found in 2022 that 80% of organizations worldwide could attribute one or more data breaches to “to a lack of cyber skills and/or awareness.”²² IBM estimates that the global average data breach in 2022 cost \$4.35 million.²³ Malicious cyber actors have probed DoD networks millions of times a day – for years.²⁴ For fiscal year 2015, DoD requested permission from Congress for \$132 million “to help pay for identity protection and background investigations” following the Office of Personnel Management breach that affected 23 million personnel.²⁵ Surely the cost of these breaches and other incidents is many times the likely cost of the CLPB program, which would be justified by its critical role in support of the DoD cyber mission and offset by savings in external recruiting and hiring expenditures. CLPB would not be a panacea, but the cyber skills gap in the DoD must be filled and there is an untapped gold mine of coding talent in the DoD.

The 2021 National Defense Authorization Act mandates that the Secretary of Defense measure and incentivize programming skills “in a manner similar to the way the Defense Language Proficiency Test measures competency” within two years.²⁶ Thus, the legal foundation and impetus for a CLPB program are already established. Accordingly, as the DoD works to develop this program, there is no need to reinvent the wheel, because this talent management problem is not unique to cyber skills. The fundamentals of concept, organization, and implementation already exist in the easily replicable form of FLPB. The DoD can use this comparatively cheap, proven program to incentivize existing DoD personnel to self-identify, maintain, and improve their cyber talents. If the program is a success within the DoD, it could also be opened to the roughly 1.4 million non-DoD US government employees – most of whom already have the motivation to serve their country.²⁷

A CLPB program designed along the lines outlined above would be a simple but powerful step in the direction of meeting the NDAA mandate: a program with high potential to solve one of the most important and urgent talent management problems the DoD faces. Development of this program should include potential qualification standards, elucidate coding/programming needs, lay out career paths in the various coding and other cyber-related fields, and specify appropriate combinations of training, education, and experience that would best contribute to professional development along these career paths.♥

DISCLAIMER

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

NOTES

1. Williams, Laruen C, "DOD Keeps Getting 'out Recruited' for Cyber Talent, Shanahan Says," *Defense Systems*, May 15, 2019, <https://defensesystems.com/articles/2019/05/15/shanahan-cyber-talent-sasc.aspx>.
2. "Hearing to Receive Testimony on the Current and Future Cyber Workforce in the Department of Defense and the Military Services," *United States Senate Committee on Armed Services*, April 21, 2021, https://www.armed-services.senate.gov/imo/media/doc/21-22_04-20-2021.pdf.
3. Mitchell, Billy, "Army Secretary Looks to Hiring Flexibilities to Boost Cyber Talent Recruitment," *Fed Scoop*, May 17, 2022, <https://www.fedscoop.com/army-secretary-looks-to-hiring-flexibilities-to-boost-cyber-talent-recruitment/>.
Rouhandeh, Alex J, "Cyber Talent Shortage Undermines U.S. in Cyber Warfare," *Newsweek*, June 17, 2021, <https://www.newsweek.com/cyber-talent-shortage-undermines-us-cyber-warfare-1601384>.
Serbu, Jared, "Pentagon Now Using Direct-Hire Authorities for a Third of its Cyber Workforce," *Federal News Network*, April 26, 2021, <https://federalnewsnetwork.com/defense-news/2021/04/pentagon-now-using-direct-hire-authorities-for-a-third-of-its-cyber-workforce/>.
Secretary of the Air Force Public Affairs, "U.S. Space Force Conducts Innovative Talent Acquisition Process," United States Space Force, August 1, 2022, <https://www.spaceforce.mil/News/Article/3111951/us-space-force-conducts-innovative-talent-acquisition-process/>.
4. "Our Story," *U.S. Department of Defense*, <https://www.defense.gov/About/>.
5. "CWARD May Be Master Repository of Cyber Talent for Reserve Component," United States Army, November 4, 2016, https://www.army.mil/article/177889/cward_may_be_master_repository_of_cyber_talent_for_reserve_component.
Chmielewski, Dan, "U.S. DoD Identified Elite Cyber Talent with 95%+ Accuracy Using Haystack Solutions Cyber Aptitude and Talent Assessment (CATA), UMD Findings Indicate," *Business Wire*, July 15, 2021, <https://www.businesswire.com/news/home/20210715005267/en/U.S.-DoD-Identified-Elite-Cyber-Talent-With-95-Accuracy-Using-Haystack-Solutions-Cyber-Aptitude-and-Talent-Assessment-CATA-UMD-Findings-Indicate>.
6. "NSA Cyber Exercise," National Security Agency, June 3 2022, <https://www.nsa.gov/Cybersecurity/NSA-Cyber-Exercise/>.
Holmes, Allan, "Do You Have Perishable Skills?" *Nextgov*, August 9, 2010, <https://www.nextgov.com/cio-briefing/2010/08/do-you-have-perishable-skills/53667/>.
7. "DOD INSTRUCTION 1340.27 MILITARY FOREIGN LANGUAGE SKILL PROFICIENCY BONUSES," Department of Defense, August 17 2022. <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/134027p.pdf>.
8. "DOD INSTRUCTION 1340.27 MILITARY FOREIGN LANGUAGE SKILL PROFICIENCY BONUSES," Department of Defense, August 17 2022 <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/134027p.pdf>.
9. "DOD INSTRUCTION 1340.27 MILITARY FOREIGN LANGUAGE SKILL PROFICIENCY BONUSES," *Department of Defense*.
10. "Foreign Language Proficiency Bonus," *Defense Language and National Security Education Office*, <https://dlneo.org/content/flpb>.
11. "Foreign Language Proficiency Bonus," *Defense Language*.
12. "Guide to Programming Languages," *ComputerScience.org*, October 22, 2019, <https://www.computerscience.org/resources/computer-programming-languages/>.
13. "DOD Training: U.S. Cyber Command and Services Should Take Actions to Maintain a Trained Cyber Mission Force," *Government Accountability Office*, March 2019, <https://www.gao.gov/assets/700/697523.pdf>.
14. Pomerleau, Mark, "For Tech All-Stars, Working at the Pentagon Can Be a Career Killer," *Defense News*, January 25, 2019, <https://www.defensenews.com/smr/cultural-clash/2019/01/28/is-better-talent-management-the-key-to-government-attracting-silicon-valley/>.
15. Pomerleau, Mark, "For Tech All-Stars, Working at the Pentagon Can Be a Career Killer," *Defense News*, January 25, 2019, <https://www.defensenews.com/smr/cultural-clash/2019/01/28/is-better-talent-management-the-key-to-government-attracting-silicon-valley/>.
16. "How Many Developers Are There in America, and Where Do They Live?" *DQYDJ*, <https://dqydj.com/number-of-developers-in-america-and-per-state/>.
17. Porche, Isaac R, III, "Cyber Power Potential of the Army's Reserve Component," RAND Corporation, 2017, <https://apps.dtic.mil/dtic/tr/fulltext/u2/1053408.pdf>.

NOTES

18. Pomerleau, "For Tech All-Stars."
19. Miller, Jason, "To Keep Cyber Workers, Army Opens up Its Wallet," *Federal News Network*, January 28, 2020, <https://federalnewsnetwork.com/reporters-notebook-jason-miller/2020/01/to-keep-cyber-workers-army-opens-up-its-wallet/>.
20. Sganga, Nicole, "Higher Pay, Less Red Tape: U.S. Launches Effort to Recruit Talent to Fight Cyberattacks," *CBS News*, November 15, 2021, <https://www.cbsnews.com/news/cyber-talent-management-system-homeland-security-cyber-attacks/>.
21. Steeves, Brye, "Air Force Values Foreign Language Speakers, Offers Additional Pay and More Career Options," *United States Air Force*, July 12, 2018, <https://www.whiteman.af.mil/News/Features/Display/Article/1573496/air-force-values-foreign-language-speakers-offers-additional-pay-and-more-career/>.
22. "2022 Cybersecurity Skills Gap," *Fortinet*, 2022, https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2022-skills-gap-survey.pdf?utm_source=pr&utm_campaign=report-2022-skills-gap-survey.
23. Sharma, Shweta, "Average Cost of Data Breaches Hits Record High of \$4.35 Million: IBM," August 1, 2022, <https://www.csoonline.com/article/3668655/average-cost-of-data-breaches-hits-record-high-of-435-million-ibm.html>.
24. "United States Cybersecurity Policy and Threats," *Committee on Armed Services United States Senate*, September 29, 2015, <https://www.govinfo.gov/content/pkg/CHRG-114shrg22270/html/CHRG-114shrg22270.htm>.
Lawson, Sean, "Just How Big is the Cyber Threat to the Department of Defense?" *Forbes*, June 4, 2010, <https://www.forbes.com/sites/firewall/2010/06/04/just-how-big-is-the-cyber-threat-to-dod/?sh=5393647146b3>.
25. "DoD's share of the OPM data breach: \$132 million," *Federal News Network*, August 25, 2015, <https://federalnewsnetwork.com/workforce/2015/08/dods-share-opm-data-breach-132-million/>.
26. 116th Congress, "H.R.6395 - William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021." *United States Congress*, January 1, 2021. <https://www.congress.gov/bill/116th-congress/house-bill/6395/text>.
27. Rapp, Nicolas, and Clifton Leaf, "How Many People Work for the U.S. Federal Government?" *Fortune*. August 01, 2019, <https://fortune.com/longform/government-employee-count-2019/>.

THE CYBER DEFENSE REVIEW

◆ RESEARCH ARTICLES ◆

Killer bots instead of killer robots: Updates to DoD Directive 3000.09 may create legal implications

Lieutenant Colonel Jon Erickson

ABSTRACT

Whichever country successfully harnesses AI throughout its military first may obtain both a decisive advantage while also changing the character of war for future generations. Therefore, it is vital for the US to be the first to employ autonomous weapons systems in an operational environment. The Cyber Mission Forces have an urgent and operational need to augment its forces with autonomous and semi-autonomous cyberspace capabilities to meet its ever-expanding mission objectives. Exempting autonomous cyberspace capabilities in Department of Defense Directive (DODD) 3000.09 will (1) provide near-term benefits that avoid the path of a hollow Cyber force but (2) may create legal implications that could undermine the directive. Ultimately, maintaining human involvement through centaur warfighting is needed to minimize the legal implications created by the “cyber exemption” in DoDD 3000.09 and the operational risks of deploying autonomous weapons systems into an operational environment.

INTRODUCTION

2023 may mark the year the Age of AI began, as an increasing number of American commercial companies test and field AI solutions. Microsoft set the Internet ablaze when it unveiled ChatGPT release 4, the artificial intelligence (AI)-driven chatbot, to the world. Its advanced conversational capabilities prompted the founder of Microsoft, Bill Gates, to proclaim that the Age of AI had begun.¹ Gates made this claim after challenging the creators of ChatGPT to train its AI to pass an Advanced Placement Biology exam. He specifically chose biology because the exam would challenge AI to apply logic to abstract concepts – a notable weakness of many of today’s AI solutions.

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



LTC Jon Erickson, is a Cyber and Signal officer and a Functional Area 26B (Information Systems Engineer) in the U.S. Army Reserves serving as the Assistant Chief of Staff, G6 for the 200th Military Police Command. He is a graduate of the Army War College. His previous assignments include serving as a Brigade S3 and a Battalion Commander in the 335th Signal Command, and Assistant Chief of Staff, G6 for the 79th Theater Sustainment Command. LTC Erickson has three combat deployments – Iraq, Afghanistan, and Kuwait – and one overseas tour in Germany. jon.v.erickson.mil@army.mil

To Gates' amazement, instead of taking two to three years of development, ChatGPT-4 was able to finalize its product after only several months of training, with an outside expert scoring a 5 (the highest possible score) to the AI's six essay responses.²

Just as importantly, the Pentagon released a much-needed update to Department of Defense (DoD) Directive 3000.09, *Autonomy in Weapon Systems*, in January 2023. Updates were needed, as in the decade since the directive's initial release the Pentagon has conducted very limited testing of autonomous systems. Project Maven is the DoD's most visible AI project, focused on processing full-motion video and imagery from its drones.³ Meanwhile, China is testing and training its autonomous systems in military games based on real-world scenarios and Russia has deployed autonomous systems in Syria to test them in battlefield environments.⁴ Though US strategic competitors are testing their autonomous weapons systems in operational or realistic test environments, the Pentagon is decidedly emplacing the foundations to harness AI throughout the military and may be further ahead in its long-term strategy than publicly known. In this article, the terms "artificial intelligence," "autonomous systems," "AI-powered systems" and "autonomous cyberspace capabilities" are used interchangeably to describe both semi- and fully autonomous systems.

Einstein once said that if he had an hour to solve a problem, he would spend 55 minutes thinking about the problem and 5 minutes thinking about solutions.⁵ The Pentagon has taken critically important steps in actively thinking about its autonomous systems dilemma by implementing AI across its 31-plus-4 "signature system" modernization priorities⁶ and leveraging AI for its Joint All Domain Command and Control (JADC2) system.⁷ The Army Futures Command is focused on further developing autonomous systems.⁸ The Deputy Secretary of Defense launched the Artificial Intelligence and Data Acceleration (ADA) Initiative

in 2021 to expedite deployment of AI-enabled technologies to combatant commands.⁹ Perhaps most importantly, the DoD's Defense Advanced Research Projects Agency (DARPA) is developing an Explainable AI program where AI solutions can explain its output or decisions that humans can understand.¹⁰ The Government Accountability Office created the AI Accountability Framework, which ensures accountability and responsibility for autonomous systems use by federal agencies, to include the DoD.¹¹ Lastly, the just released DoDD 3000.09 establishes an Autonomous Weapon System Working Group to consider the full range of DoD interests throughout the development lifecycle for autonomous weapon systems.¹²

The updated directive will facilitate autonomous weapons systems development rather than burden developers with bureaucracy by providing a clearer process to develop and deploy AI-powered systems as well as adding a requirement to follow DoD AI Ethical Principles. Perhaps the most critical component is the exemption of "autonomous or semi-autonomous cyberspace capabilities" from this directive.¹³ On one hand, this exemption recognizes the already widespread commercial employment of autonomous cyber capabilities (from most Endpoint Detection and Response solutions to chatbots like ChatGPT). On the other, it could reflect DoD willingness to take risks in the Cyber domain to push forward its autonomous systems development efforts. The reality is that there are very little established international laws and norms for cyberspace and, of those that are established, have not managed to keep cyberspace peaceful. Thus, the "cyber exemption" in DoDD 3000.09 may also serve as recognition that the likeliest threats to the United States will originate from cyberspace and is therefore practical to exempt developers of cyberspace-based AI-powered systems to speed up their delivery of these capabilities. Another possibility is that the DoD created this cyber exemption because of its belief that its Defense Acquisition System process will 'catch' any autonomous system to allow the DoD's Chief Digital and Artificial Intelligence Officer to monitor and evaluate AI capabilities.¹⁴ "Or perhaps DoD is trusting that Cyber Command and the future iteration of its Joint Cyber Warfighting Architecture (JCWA), operating as an integrated Cyber weapons platform, will provide the oversight to control the employment of AI-powered systems in cyberspace."¹⁵ Regardless of the motives for this cyber exemption, updates to DoDD 3000.09 are well-timed, as the DoD's Cyber Mission Forces (CMF) have an urgent and operational need to augment its forces with autonomous and semi-autonomous systems.

AVOIDING THE PATH OF A HOLLOW CYBER FORCE

The use of adversarial AI-powered capabilities in cyberspace will inhibit the ability of the Cyber Mission Force to effectively defend everywhere. China's activities in the East China Sea provide a useful analogy to show the negative effects that adversarial AI could have on a CMF not augmented with autonomous cyberspace capabilities. China uses its vast quantity of military aircraft to enforce its territorial claims by flying near Japanese airspace resulting in its small number of Japanese

pilots scrambling to respond.¹⁶ On one hand, this creates a real risk of miscalculation that could turn into a larger conflict while, on the other, China's provocations are eroding Japan's air combat readiness – taking away training time, increasing stress on the pilots, and straining Japan's ability to respond to all air incursions. AI-powered attacks will have similar effects on the CMF as China is having on Japan's air force. Multi-vector distributed denial of service (MV-DDoS) cyberattacks give a glimpse of how an AI-powered attack can overwhelm the CMF. An MV-DDoS achieves its denial of service through different methods of DDoS targeting Layers 3, 4 and 7 – the network, transport, and application layers, respectively – and using amplification protocols – such as UDP, TCP SYN, DNS amplification – not only to exponentially increase the volume of data to overwhelm defenders but also to obfuscate the threat actor's identity.¹⁷ Several cyberattacks in the first half of 2021 alone have employed 27 to 31 different vectors¹⁸ and up to nine different amplification protocols.¹⁹ As DoD moves more of its workload into the cloud, multi-vector attacks powered by AI will overwhelm the human capacity to respond. Augmenting the CMF with autonomous cyberspace capabilities is not only critical for defending the DoD Information Network (DoDIN) but also crucial for defending forward.

To move from reacting to cyberattacks to proactively preventing or disrupting cyberattacks, Cyber Command implemented a key concept called “defending forward” to intercept threats and degrade capabilities before it reaches the DoDIN.²⁰ Defending forward consistently and successfully requires sufficient investments by the DoD. The Director of Operational Test & Evaluation's (DOT&E) FY21 Annual Report recommended that cyber operators are resourced at levels like kinetic warfare operators.²¹ The DOT&E report highlights that the Pentagon has not invested sufficient resources in training and equipping its cyber operators. Training is even more important with AI, as poor problem definition, faulty training data sets, or a myriad of other factors could lead to unintended engagements. Instead, the Pentagon continues to pour billions into its digital modernization strategy and emerging technologies.²² The increasing number of cyber missions and cyberattacks will detract from training time and erode CMF readiness, creating the fear of a hollow cyber force.²³

Therefore, the initial focus for integrating autonomous cyberspace capabilities should be to support Defensive Cyber Operations (DCO) focused on Internal Defensive Measures (DCO-IDM). With cybersecurity and AI being priorities of the DoD Chief Information Officer's digital modernization strategy combined with the release of updates to DoDD 3000.09, it should be anticipated that DoD will, if it has not already, employ many defensive autonomous cyberspace capabilities throughout the DoDIN and in cooperation with Allied and partner networks.²⁴ Deploying autonomous cyberspace capabilities will free cyber defenders from performing time-consuming and labor-intensive tasks such as data collection, consolidation, and correlation, which commercial AI solutions already perform.²⁵ AI-powered cybersecurity capabilities can already streamline and automate the ability to identify, protect, detect, and respond to threats without human intervention. Additionally, defense is a necessary foundation

for offense, as defensible networks protect cyber weapons such as EternalBlue from being stolen.²⁶ An April 2021 Government Accountability Office report assessed that the federal government needed to enhance its response to cyber incidents, highlighting the need for more investment in DCO-IDM tools.²⁷

Another reason to focus on cyber defensive autonomous systems is that the ability for AI to conduct offensive cyber operations (OCO) is not proven. However, AI can support OCO in the areas of (1) cyber reconnaissance, where AI-powered systems can scan, gather information, and conduct open-source searches to map adversarial cyber terrain, and (2) access development, where autonomous systems exploit vulnerabilities and trust relationships to develop cyber avenues of approach. At the same time, autonomous systems offer the CMF the ability to persistently engage in cyberspace by “manning” and operating limitless listening posts/observation posts (LP/OP) throughout cyberspace. LP/OPs are used in the physical world as the “primary means of maintaining surveillance of an assigned avenue of approach or named area of interest.”²⁸ And much like coalition operations, LP/OPs in cyberspace can be manned by allies and partners on their own networks to develop a larger and more data-rich threat intelligence network to prevent breaches or mitigate potential threats before they can cause damage. At the same time, as AI is mapping and observing the adversary’s network – identifying weaknesses and vulnerabilities as well as cyber key terrain – cyber operators can practice executing its mission on a mock-up of the adversary network similar to the Navy SEALs’ mock-up of Bin Laden’s compound before their raid.²⁹ The battlefield deployment of autonomous systems in cyberspace is critical to the readiness of the CMF. However, exemptions and ambiguities in DoDD 3000.09 may create legal implications where failures in an autonomous cyberspace capability could lead to unintended engagements or operational risk that undermines the directive.

LEGAL IMPLICATIONS OF AUTONOMOUS CYBERSPACE CAPABILITIES

While DoDD 3000.09 should facilitate development of autonomous systems in accordance with existing rules and ethical principles, no weapons system is publicly known to have gone through the review process in the decade since the directive was first published.³⁰ Deploying AI-powered systems in an operational environment should not happen by exploiting an exemption for cyberspace, as the revised directive “does not apply to autonomous or semi-autonomous cyberspace capabilities.”³¹ DoD defines cyberspace capability simply as “a device or computer program... designed to create an effect in or through cyberspace.”³² The directive’s cyber exemption creates multiple unknown legal implications and risk vectors.

The exemption for cyber raises policy questions about whether the DoD views the physical and cyber domains as separate and independent domains when it comes to autonomous systems, when in fact these two domains interact with each other in complex ways. An exemption for autonomous systems operating in the virtual world may in fact create unintended engagements in the physical world that will undermine the directive. For example,

according to the directive, an autonomous or semi-autonomous weapon system that employs non-lethal, non-kinetic force is required to undergo a thorough vetting and review process. However, under one interpretation of DoDD 3000.09, if the autonomous system creates an effect in the physical domain but through cyberspace, then it may be exempted from the directive's vetting and review process and allow a Commander to assume the risk of its use. Unless this exemption is clarified, the DoD may see a spike in unintended engagements from the ambiguity and confusion around this cyber exemption.

In the last thirteen years, several cyber attacks illustrate the concerns about the ambiguous directive's cyber exemption. Stuxnet is the first known cyberweapon to cause physical damage through cyberspace, and there have been more recent examples of attacks using non-lethal kinetic force through cyberspace. In 2015, hackers infiltrated the German steel mill's business network through social engineering to then access the mill's network that controlled its operational technology and control systems. The attackers were able to cause multiple failures that resulted in massive damage to the steel mill's blast furnace.³³ Through electric vehicles (EV) themselves or through EV charging stations, hackers could take control of the vehicle to cause a crash, steal user data, and could also use the EV or EV charging station to infiltrate the charging network to shut down fleets of electric vehicles, buses, or trucks or compromise the electric power grid.³⁴ While a traditional car requires 500-600 chips, the number of chips in a smart car has reached upwards of 5,000 chips – presenting attack vectors.³⁵ Meanwhile, a laptop uses only one chip and is responsible for a myriad number of daily cyberattacks. While the steel mill attack and EV hacks are not caused by an autonomous weapon system, it raises the question of whether an autonomous system operating only in cyberspace but causes physical damage would have been required to undergo a thorough vetting and review process in accordance with DoDD 3000.09. In the directive, the role of the DoD's Chief Digital and Artificial Intelligence Officer is merely to monitor and evaluate AI capabilities rather than approve its use.³⁶ And if this hypothetical autonomous system should have been vetted, the language in the directive is unclear and ambiguous.

One reason to clarify any ambiguities around the cyber exemption is that employing AI-powered systems in cyberspace will often be more advantageous than in the physical domains of land, sea, air and space and, therefore, be the preferred attack vector. First, nearly every military system is going to be connected to a network, allowing for remote connectivity. Stuxnet demonstrates how even air-gapped networks can be infiltrated. Second, cyberattacks do not require physically deploying Soldiers or equipment in sovereign territory, achieving similar results through cyberspace. Lastly, a cyberattack can continue to perpetuate beyond physical borders for an infinite time. Russia's NotPetya malware, discussed in the next paragraph, leveraged the NSA's EternalBlue cyber weapon to attack Ukraine and nearly crashed the world with its cyberattack.

Another reason for clarifying the directive's cyber exemption is that the military application of an unpredictable or misbehaving autonomous weapon system on a mostly civilian technology infrastructure could cause a worldwide crash. Russia's NotPetya malware is the closest example that makes the point about the need to vet and review autonomous cyberspace capabilities rather than exempt them. Russian hackers created a back door into a Ukrainian company's update server to release NotPetya, which was created to spread rapidly and indiscriminately. While Ukraine was the intended target, NotPetya crippled ports, paralyzed corporations and froze government agencies worldwide. To illustrate the speed of proliferation, the network of a large Ukrainian bank was taken offline in 45 seconds and even when computers were patched, a vulnerable computer allowed the malware to re-infect the patched computer.³⁷ The estimated damages were around \$10 billion worldwide, with 10 percent of all computers in Ukraine needing to be wiped.³⁸ Experts expect to see even more damaging malware in the future. Although NotPetya is not an autonomous system, this malware shows the challenge of confining a cyber weapon to a geography, limiting within the cyberspace domain, or to civilian versus military infrastructure. Coupled with the unpredictability of AI behavior in the real world with indiscriminate malware like NotPetya, an exemption for autonomous systems in cyberspace raises significant legal, ethical, and operational concerns that may undermine DoDD 3000.09. Regardless, maintaining human involvement as a moral agent is needed to minimize the legal implications created by the directive's cyber exemption and the risks of deploying autonomous weapons systems in an operational environment.

RESOLVING THE AUTONOMOUS SYSTEMS DEPLOYMENT CHALLENGE THROUGH CENTAUR WARFIGHTING

A human-centric approach to autonomous system design should be a foundational element of US warfighting. Additionally, human-machine teaming is paramount to multidomain operations and operating in the Age of AI. In this new operational environment, a vast majority of activities will be best served by human-machine teaming, or "centaur warfighting."³⁹ The fog of war in cyberspace will be shaped by the volume, variety, velocity, and quality of data being generated by billions of devices communicating at machine-speed. AI, speaking in machine language, can peer through the digital fog of war to deliver intelligible information. The advantage in centaur warfighting is that it combines the speed and reliability of machines with the creativity and flexibility of human intelligence while keeping humans as moral agents.

In the fog of war, there is little proof that AI will be able to operate in accordance with international laws or norms around the use of force and of armed conflict. The NotPetya malware demonstrates how poor coding can result in a cyber weapon incapable of following the *jus in bello* principles of discrimination and proportionality. Factor in intangible factors that humans face every day, to include ethical, moral, and personal values/beliefs, and it is

difficult to conclude that AI-powered systems will function as anticipated in an operational environment. In one example in 2018, Uber's driving system could not classify a pedestrian walking their bicycle across the middle of the road and away from a crosswalk. The system continued its internal deliberations traveling at 39 miles per hour when it finally alerted the driver at only 0.2 seconds before impact.⁴⁰ Artificial intelligence consistently struggles to function as intended, even in a real-world, low-stress, non-military operational environment.

The Uber accident also demonstrates the fallacy of human control over autonomous systems. A myth is that the more decisions an autonomous system can make, the less knowledge or less engagement a human operator must have. In fact, the opposite is true in that a human operator must not only know how the weapon system operates but how the autonomous system "thinks" and its "biases." While the Army's Patriot missile defense system is not an autonomous system, its automated capabilities make it a proxy concerning the dangers of trying to replace human operators. At the commencement of Operation IRAQI FREEDOM, the Patriot batteries operated in "automated mode," which meant that the system and not a human were interrogating targets.⁴¹ After the Patriot system mistakenly shot down a British aircraft, the Army put the system launchers on standby but continued to operate the Patriots in automatic engagement mode. When an American fighter jet was mistakenly identified as an incoming Scud missile, the director used the wrong language to cause the Patriot system to fire a missile.⁴² The root cause had less to do with the director using the wrong language but more so the repurposing of software biased to shoot down ballistic missiles in a less crowded upper atmosphere for re-use in a complex, crowded, dynamic lower atmosphere composed of friendly and enemy forces as well as civilian and military aircraft.⁴³ This episode highlights the third major legal implication of relying on AI-powered systems in the operational environment - the use of faulty or untrained autonomous systems or, in this case, repurposing AI from its original/intended use.

The Uber accident and Patriot incident bring to light the misplaced goal of designing AI solutions that can operate with humans "out of the loop," where AI can work independently but have the safety net of being able to hand off to humans when the AI cannot decide or act. This means that a human is engaged at the end of the process, receiving all the blame for poor decisions or inaction by the autonomous system. Operating in the Age of AI requires humans and AI to work interdependently, where both the human and AI are fully engaged. A human-centric approach to autonomous systems means designing AI solutions that extend human capabilities. To use airplane pilots as an example, AI should function as a co-pilot - always engaged, providing information, or able to take over for the human pilot - rather than as an auto-pilot button that's either on or off. In a human-centric approach to AI, the human is determining the level of AI's involvement while AI is always engaged in the background.

As a matter of clarification, human involvement does not imply human control. Human involvement can generally be roughly divided into three levels. A human can be "on the loop"

by supervising and overseeing, be “in the loop” by making decisions, or be “out of the loop” by deferring decisions to the autonomous system. Human accountability for the results of a lethal action should not be removed. However, a Soldier should not need to approve every step of the kill chain, just as Navy personnel are not required to do so with its Aegis fire control system to shoot down air threats.⁴⁴ Regardless, the ethical, operational, and strategic risks of autonomous systems increasing the likelihood of conflict or war are a real possibility. The legal implications of the cyber exemption in DoDD 3000.09 could undermine the directive, further adding to the need for human involvement through centaur warfighting.


CONCLUSION

Despite concerns about autonomous weapon systems, it is important to consider that “the United States was the first country to adopt a formal policy on autonomy in weapon systems.”⁴⁵ Though the policy only applies to the Department of Defense, the Government Accountability Office’s AI Accountability Framework ensures all federal agencies, to include the DoD, are following guidelines to ensure that AI systems are responsible, equitable, traceable, reliable, and governable.⁴⁶ Lastly, the updates to DoDD 3000.09 made some much-needed clarification that will allow the US to continue to be a leader in the legal and ethical uses of autonomous systems. For example, one major update in the directive is that autonomous weapons will “complete engagements within a timeframe and geographic area,” which would prevent the US from deploying an AI-powered cyber weapon like NotPetya that is unbounded in time or geography.⁴⁷

At the same time, it is counterintuitive for the Pentagon to exempt “autonomous or semi-autonomous cyberspace capabilities” merely because it operates in cyberspace. The Stuxnet malware and the German steel mill incident are two examples of cyber weapons that caused physical damage while only operating in the cyber domain. Therefore, human involvement through centaur warfighting is critical to minimize the legal implications created by the cyber exemption in DoDD 3000.09 and to mitigate risks of deploying autonomous weapons systems in an operational environment.

Whichever country harnesses AI throughout its military may obtain both a decisive advantage and change the character of war for future generations. Therefore, it is vital for the US to responsibly and safely employ autonomous weapons systems in an operational environment. The Cyber Mission Forces will be one of the largest beneficiaries of operating with autonomous cyberspace capabilities, as adversarial AI will not only inhibit the CMF’s ability to defend DoD mission systems but also corrode its readiness. Autonomous cyberspace capabilities not only avoids the path of a hollow cyber force but enhance the DoDIN’s defenses, which protect cyber weapons like NSA’s EternalBlue from being stolen. Additionally, AI can be trained to support offensive cyber operations in the areas of cyber reconnaissance and access development. Centaur warfighting in the Age of AI will allow the US to continue to

KILLER BOTS INSTEAD OF KILLER ROBOTS

safeguard and advance vital US national interests by harnessing the speed and reliability of machines with the creativity and flexibility of human intelligence while keeping humans as moral agents. Ultimately, maintaining human involvement through centaur warfighting is needed to minimize the legal implications created by the cyber exemption in DoDD 3000.09 and the risks of deploying autonomous weapons systems in an operational environment. 

DISCLAIMER

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

NOTES

1. Bill Gates, "The Age of AI Has Begun," GatesNotes (blog), March 21, 2023, <https://www.gatesnotes.com/The-Age-of-AI-Has-Begun>.
2. Ibid.
3. Kelsey D. Atherton, "Targeting the Future of the DOD's Controversial Project Maven Initiative," C4ISRNet. C4ISRNet, August 19, 2022, <https://www.c4isrnet.com/it-networks/2018/07/27/targeting-the-future-of-the-dods-controversial-project-maven-initiative/>.
4. Eric Schmidt et al., "Final Report: National Security Commission on Artificial Intelligence," (Washington, DC, 2021), <https://www.nsc.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf>.
5. Nell Derick Debevoise, "The Third Critical Step In Problem Solving That Einstein Missed," *Forbes*, last modified January 26, 2021, <https://www.forbes.com/sites/nelldebevoise/2021/01/26/the-third-critical-step-in-problem-solving-that-einstein-missed/?sh=1c87b9d63807>.
6. Yasmin Tadjeh, "AUSA NEWS: Army CIO Insists U.S. Still Leader in Artificial Intelligence," National Defense, October 13, 2021, <https://www.nationaldefensemagazine.org/articles/2021/10/13/army-cio-insists-us-still-leader-in-artificial-intelligence>.
7. Carol Collins, "DOD's JADC2 Strategy Leverages AI Technology, Common Data Fabric to Develop Digital Infrastructure," GovCon Wire, August 20, 2021, <https://www.govconwire.com/2021/08/dod-jadc2-concept-seeks-to-use-ai-common-data-fabric-for-digital-infrastructure/>.
8. U.S. Army Futures Command Artificial Intelligence Integration Office (AI2C), "Broad Agency Announcement for Transformative Artificial Intelligence Research and Applications," *Federal News Network*, <https://federalnewsnetwork.com/wp-content/uploads/2021/08/army-BAA-for-AI.pdf>.
9. The Office of the Director, Operational Test & Evaluations, FY2021 Annual Report, Washington, DC: Department of Defense, 2022, https://www.dote.osd.mil/Portals/97/pub/reports/FY2021/other/2021DOTEAnnualReport.pdf?ver=3D_nTNLgp-Gak8xY1bmmlQ%3D%3D.
10. Dr. Matt Turek, "Explainable Artificial Intelligence (XAI)," Defense Advanced Research Projects Agency, accessed January 24, 2023, <https://www.darpa.mil/program/explainable-artificial-intelligence>.
11. Government Accountability Office, "Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities," GAO-21-519SP, (Washington, DC: Government Accountability Office, 2021), <https://www.gao.gov/assets/gao-21-519sp.pdf>.
12. Department of Defense, *Autonomy in Weapon Systems*, DoD Directive 3000.09, Washington, DC: Department of Defense, 2023, <https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf>.
13. Ibid.
14. Ibid.
15. Mark Pomerleau, "US Cyber Command beginning to examine next-generation weapons platform," *DefenseScoop*, last modified May 5, 2023, <https://defensescoop.com/2023/05/05/us-cyber-command-beginning-to-examine-next-generation-weapons-platform/>.
16. Edmund J. Burke et al., *China's Military Activities in the East China Sea: Implications for Japan's Air Self-Defense Force*, (RAND Corporation, 2018), 12, https://www.rand.org/pubs/research_reports/RR2574.html.
17. Help Net Security, "Multi-vector DDoS attacks on the rise, attackers indiscriminate and persistent," last modified April 27, 2022, <https://www.helpnetsecurity.com/2022/04/27/multi-vector-ddos-attacks/>.
18. Responsive Technology Partners, "A Different Kind of Cyber-Attack," last modified January 10, 2022, <https://www.responsivetechnologypartners.com/2022/01/10/a-different-kind-of-cyber-attack/>.
19. Help Net Security, "Multi-vector DDoS attacks on the rise, attackers indiscriminate and persistent," last modified April 27, 2022, <https://www.helpnetsecurity.com/2022/04/27/multi-vector-ddos-attacks/>.
20. U.S. Cyber Command PAO, *CYBER 101 - Defend Forward and Persistent Engagement*, October 25, 2022, <https://www.cybercom.mil/Media/News/Article/3198878/cyber-101-defend-forward-and-persistent-engagement/>.
21. The Office of the Director, Operational Test & Evaluations, *FY2021 Annual Report*, last modified January 2022, 247, https://www.dote.osd.mil/Portals/97/pub/reports/FY2021/other/2021_DOTEAnnualReport.pdf?ver=YVOVP-cF7Z5drzi8IGPSqjw%3d%3d.

NOTES

22. Sydney J. Freedberg, "Army Network Gets Most 2022 Modernization S," *Breaking Defense*, last modified June 2, 2021, <https://breakingdefense.com/2021/06/army-network-gets-most-modernization/>.
23. *Department Of Defense Authorization for Appropriations for Fiscal Year 2018 and the Future Years Defense Program: Cyber Posture of the Services*, Senate Hearing 115-448, Part 8, May 23, 2017, 3, <https://www.congress.gov/115/chr/CHRG-115shrg35762/CHRG-115shrg35762.pdf>.
24. Department of Defense, *DoD Digital Modernization Strategy: DoD Information Resource Management Strategic Plan FY19-23* (Washington, DC: Department of Defense, 2019), 4, <https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF>.
25. Microsoft 365 Defender Team, "Inside Microsoft 365 Defender: Correlating and consolidating attacks into incidents," last modified July 9, 2020, <https://www.microsoft.com/en-us/security/blog/2020/07/09/inside-microsoft-threat-protection-correlating-and-consolidating-attacks-into-incidents/>.
26. Defense Science Board, *Task Force on Cyber as a Strategic Capability – Executive Summary* (Washington, DC: Department of Defense, 2018), 2, https://dsb.cto.mil/reports/2010s/DSB_CSC_Report_ExecSumm_Final_Web.pdf.
27. Government Accountability Office, *Information Technology and Cybersecurity: Significant Attention is Needed to Address High-Risk Areas*, GAO-21-422T, (Washington, DC: Government Accountability Office, 2022), 19, <https://www.gao.gov/assets/gao-21-422t.pdf>.
28. U.S. Army, Army Technical Publication 3-39.30, *Security and Mobility Support*, May 2020, https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN22142_ATP_3-39x30_FINAL_WEB.pdf.
29. Michael B. Kelley, "Bing Maps Show The CIA's Secret Bin Laden Training Facility In North Carolina," *Business Insider*, last modified October 9, 2021, <https://www.businessinsider.com/the-secret-bin-laden-training-facility-2012-10>.
30. Sydney J. Freedberg Jr., DoD's clarified AI policy flashes 'green light' for robotic weapons: Experts, *Breaking Defense*, February 9, 2023, <https://breakingdefense.com/2023/02/dods-clarified-ai-policy-flashes-green-light-for-robotic-weapons-experts/>.
31. Department of Defense Directive 3000.09, *Autonomy in Weapon Systems*, January 25, 2023) <https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf>.
32. Joint Publication 3-12, *Cyberspace Operations*, Joint Chiefs of Staff, Department of Defense, June 8, 2018, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.
33. Gary Cohen, "Throwback Attack: A cyberattack causes physical damage at a German steel mill," *Industrial Cybersecurity Pulse*, June 10, 2021, <https://www.industrialcybersecuritypulse.com/facilities/throwback-attack-a-cyberattack-causes-physical-damage-at-a-german-steel-mill/>.
34. Shourjya Mookerjee, "EV infrastructure vulnerabilities put cars, the grid at risk" *GCN*, May 9, 2022, <https://gcn.com/cybersecurity/2022/05/ev-infrastructure-vulnerabilities-put-cars-grid-risk/366694/>.
35. Will Fu, "How many chips does a car need?" June 17, 2022, <https://www.linkedin.com/pulse/how-many-chips-does-car-need-will-fu/>.
36. Department of Defense, *Autonomy in Weapon Systems*, DoD Directive 3000.09, Washington, DC: Department of Defense, 2023, <https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf>.
37. Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, August 22, 2018, <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/?directURL=https%3A%2F%2Fwww.wired.com%2Fstory%2Fnotpetya-cyberattack-ukraine-russia-code-crashed-the-world%2F>.
38. Ibid.
39. Paul Scharre, "Autonomous Weapons and Operational Risk: Ethical Autonomy Project," *Center for a New American Security*, February 1, 2016, 41, <https://www.jstor.org/stable/resrep06321.11?seq=1>.
40. Lauren Smiley, "'I'm the Operator': The Aftermath of a Self-Driving Technology," *Wired*, March 8, 2022, <https://www.wired.com/story/uber-self-driving-car-fatal-crash/#:~:text=In%202018%2C%20an%20Uber%20autonomous,behind%20the%20wheel%20finally%20speaks.&text=Rafaela%20Vasquez%20liked%20to%20work,assigned%20her%20the%20Scottsdale%20loop.>
41. The Guardian, "'Glorious failures' caused US to kill RAF crew," last modified October 31, 2006, <https://www.theguardian.com/uk/2006/oct/31/military.iraq>.

NOTES

42. Sydney J. Freedberg, Jr., "Artificial Stupidity: Fumbling The Handoff From AI To Human Control," *Breaking Defense*, June 5, 2017, <https://breakingdefense.com/2017/06/artificial-stupidity-fumbling-the-handoff/>.
43. Ibid.
44. Sydney J. Freedberg, Jr., "Fear & Loathing In AI: How The Army Triggered Fears of Killer Robots," *Breaking Defense*, last modified March 6, 2019, <https://breakingdefense.com/2019/03/fear-loathing-in-ai-how-the-army-triggered-fears-of-killer-robots/>.
45. Gregory C. Allen, "DOD Is Updating Its Decade-Old Autonomous Weapons Policy, but Confusion Remains Widespread," *Center for Strategic and International Studies*, June 6, 2022, <https://www.csis.org/analysis/dod-updating-its-decade-old-autonomous-weapons-policy-confusion-remains-widespread#:~:text=The%20United%20States%20was%20the,good%2C%20but%20also%20well%20understood>.
46. Government Accountability Office, "Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities," GAO-21-519SP, (Washington, DC: Government Accountability Office, 2021), <https://www.gao.gov/assets/gao-21-519sp.pdf>.
47. Department of Defense, *Autonomy in Weapon Systems*, DoD Directive 3000.09, Washington, DC: Department of Defense, 2023, <https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf>.

Expanding the Dyadic Cyber Incident and Campaign Dataset (DCID): Cyber Conflict from 2000 to 2020¹

Dr. Ryan C. Maness
Dr. Brandon Valeriano
Dr. Kathryn Hedgecock

Jose M. Macias
Dr. Benjamin Jensen

ABSTRACT

This article provides an overview of updates to the Dyadic Cyber Incident and Campaign Dataset (DCID). Whereas most efforts to catalogue cyber incidents focus on curated lists and attack typologies, the DCID uses a standardized set of coding procedures consistent with best practices in social science. As a result, the analysis reveals there is a tendency to exaggerate the use and impact of cyber operations, obscuring their role as an instrument of disruption, espionage, and sabotage, and complements to larger coercive campaigns. The article outlines the construction of version 2.0, which documents rival, state-to-state use of cyber operations as an instrument of power. The expanded dataset introduces additional incidents based on various web-searching methods and human coder cross-validation while also adding new variables for ransomware, supply chain attacks, and connections to ongoing information operations. DCID 2.0 contains 429 incidents representing a critical attempt to scope the domain of conflict among strategic rivals.

INTRODUCTION

In the 21st century, cybersecurity is an increasingly critical issue for competition and conflict among all actors in the international system. The cyber domain,² which encompasses digital competition across the physical, logical, and persona layers of cyberspace is not only a site of contestation but a focal point for debates about strategy, defense spending, and alignment of human capital to national security priorities.³ It is now common to argue that cybersecurity is a top tier security threat that will dominate future battles through the speed of interaction and the fast pace of technological advancement.⁴

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



Ryan C. Maness (Ph.D., University of Illinois, Chicago, 2013) serves as an assistant professor at the Naval Postgraduate School (NPS), where he oversees the curriculum on information strategy and political warfare. He also directs the DoD Information Strategy Research Center at NPS, which will host its third annual Symposium on Information Strategy and Political Warfare in June 2023. Maness's research includes a state-initiated cyber incidents project, the Dyadic Cyber Incident and Campaign Dataset (DCID) 2.0, which tracks incidents from 2000-2020. He also studies escalation in cyberspace and cyber operations' role in the Russo-Ukraine war. Currently under contract for a book on Modern Hybrid Warfare, Maness has also published works on cyber strategy and Russia's coercive diplomacy. He teaches courses on cyberspace conflict, computer network attack and defense, and conflict in Europe at NPS.

Due to the increasing connectivity of the modern world, competition and conflict in information space are the new norm and international interactions increasingly take place in and through the cyber domain. From digital thefts that sustain authoritarian regimes, to attempts to destabilize the foundations of democracy, digital connectivity provides new options for state and non-state actors to engage in contentious politics. Cyber connectivity is thus a risk as much as it is an opportunity. Since security was not built into these networks, and still is often an afterthought, this pattern of contestation is likely to continue. Therefore, researchers owe the public and policymakers new datasets that identify patterns and trends defining how major state actors use cyber operations against their rivals. This article suggests one set of data collection variables that attempt to address this issue.

Constant threats from adversaries hasten the need for clear, open-source, and timely data on cyber incidents to counter and defend rival cyber operations, which are becoming an ever-growing threat to global stability and connectivity. Cybersecurity is an operational domain of conflict functioning almost wholly without data that might illuminate observers on the scope of the issue. The field has no clear awareness of the baselines for cybersecurity incidents and few methods of collecting information to rectify this problem. This challenge was noted in the policy community, culminating in the Cyberspace Solarium Commission's failed recommendation of a Bureau of Cyber Statistics to collect cybersecurity data.⁵

This article details the expansion of the Dyadic Cyber Incident and Dispute (DCID) Dataset first produced by Valeriano and Maness⁶ and expanded into version 1.5 with Maness, Valeriano, and Jensen.⁷ Version 2.0 represents a new statement of comprehensive data coding for state-to-state based cyber conflict. With this data expansion, we add additional incidents, expand the timeline, and add in new variables for such factors



Brandon Valeriano (PhD) recently joined Seton Hall University's School of Diplomacy and the Royal Danish Defence College. He also serves as a Distinguished Senior Fellow at the Marine Corps University and Senior Advisor to the Cyberspace Solarium Commission 2.0. He has published six books and dozens of articles on cyber security and international security. Dr. Valeriano has provided testimony on cyber conflict for the United States Senate, the Canadian Senate, and the Parliament of the United Kingdom, also serving as a Senior Advisor to the Cyberspace Solarium Commission. Ongoing research explores conflict escalation, the space-cyber nexus, and data/metric applications for cyber security. Dr. Valeriano is the Area Editor in International Relations for the *Journal of Cybersecurity* and the Series Editor of *Disruptive Technology and International Security* for Oxford University Press.

as ransomware, supply chain attacks, and connections to ongoing information operations. DCID 2.0 has 429 incidents representing a critical attempt to scope the domain of conflict among strategic rivals. An exhaustive search of other data sources has been consulted to identify any missing cases ensuring that this data supersedes all previous efforts to catalog the domain.

In this article, we put cyber data in context, explain our design choices, and outline our early findings. We then review our coding procedures and report reliability statistics. Finally, we report new results on the number and impact of cyber operations over time, demonstrating that cyber operations are on the rise, used differently by each state based on their interests, and that the U.S., its allies, and partners can develop more coherent policies by understanding how and when their adversaries are using the cyber interactions maliciously. Additionally, the best course of action to deter and discourage malicious cyber actions is suggested.

Cybersecurity Data

Current literature and research provide an incomplete picture of the cyber landscape. Organizations that collect cyber event data often encounter extreme roadblocks since cybersecurity operates as a covert or clandestine instrument of power – often undeclared and unattributed.⁸ Limited efforts to provide data exist because automated coding of reports of incidents, including using natural language processing methods are complicated by the lack of available non-proprietary data. Transparency of incidents due to monetary or reputation costs also leaves many incidents incomplete or undisclosed in the public record, thereby, complicating data collection.

Four types of data exist in the literature. First, event lists provide information to researchers. Second, annual documents by cybersecurity companies report summaries of information and statistics of known cyber events. Third, while not exclusively data, the wider



Kathryn Hedgecock is an Assistant Professor of International Affairs at the United States Military Academy in West Point, NY. Major Hedgecock's research interests include deterrence and attribution of state-sponsored cyber operations, the impact of emerging technology on the future of warfare, the relationship of public and private entities in cyber defense, and the public response to non-conventional operations short-of-force. She holds a Ph.D. and M.A. from Stanford University in Political Science, a M.Sc. from the University of Oxford in Russian and East European Studies, and a B.S. from the United States Military Academy.

body of literature uses case studies, anecdotes, and analogy to inform strategy. Finally, attack typologies that classify attack types as well as techniques and procedures to support real-time cyber defense operations are included.

For the first category, various organizations have sought to provide data in the form of lists to the community. The Council on Foreign Relations (CFR) Cyber Operations Tracker and the Center for Strategic and International Studies (CSIS) Significant Cyber Incidents provide short summaries of available incidents.⁹ The Carnegie Institute also produces a smaller list of attacks involving financial institutions.¹⁰

These lists lack the ability to provide comparative variables, primarily categorical but also interval, because they do not limit incidents relative to analysis.¹¹ Instead, these lists serve as a qualitative summary of incidents according to their respective criteria but not formatted in a manner consistent with the scientific study of conflicts.¹² Furthermore, no summary statistics or quantitative products are provided alongside, limiting their true potential to social science. Without awareness of the norms and process of dataset collection, these sources fail to build what is typically thought of as a dataset, a well-planned effort to catalog existing efforts in a community including associated variables and information to support replication.¹³ What is included, and excluded, plus the reliability checks of the data are missing, leaving the community largely in the dark without valid sources of data.

A graphical representation (Figure 1) outlines the types of data available to researchers. CSIS and CFR code known incidents regardless of target and attacker. Comparing all known incidents from one time to another provides little insight for comparative analysis due to unclear selection methods. For the specific purpose of measuring the political impact of attributed incidents and testing of theories on escalation, deterrence, and



Jose M. Macias is a Master of Public Policy (M.P.P.) candidate at The University of Chicago's Harris School of Public Policy and a Fellow with The Pearson Institute for the Study and Resolution of Global Conflict. Born and raised in Calexico, CA, he's a first-generation Chicano graduate with dual B.A.s in International Relations and Political Science from UC Davis. Jose has an extensive background in national security studies and cyber conflict research, with professional experiences with the U.S. Department of Defense, Army Cyber Command, U.S. Congress and the Center for Strategic and International Studies (CSIS). Now at Harris, he serves as a Teaching Assistant for R programming and co-leads a cyber incident coding project at the Naval Postgraduate School with Dr. Ryan C. Maness and Dr. Brandon Valeriano.

persistent engagement, DCID collects incidents with reasonable attribution of responsibility and evidence in the public record. Additionally, since the purpose is to capture activity of contentious states, DCID collects only incidents involving nation-state historic rivalries.¹⁴

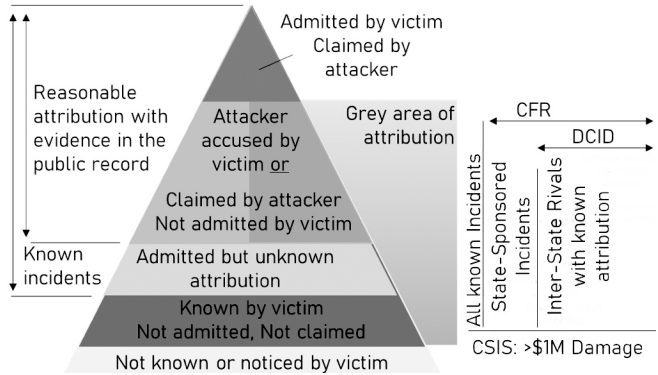


Figure 1: Types of Cyber Incidents

Second, cybersecurity companies produce several annual reports with claims of increasing quantity and severity of attacks, all released for a significant fee. Yet, these statistics limit the scope to the clients of their software or services. Little comprehensive data without significant bias exists to provide statistics that can withstand academic scrutiny, with compilations of secondary and tertiary sources crowding out primary sources and surveys in these reports.¹⁵ Additionally, cybersecurity companies do not reveal or share proprietary data, making compilation, fact checking, or comparison of statistics difficult to impossible.

Third, the quality of research methods across cyber strategy literature varies significantly, with several well-researched case studies. However, much of the literature relies on logic and analogy, rather than facts. The existing academic debates on cyber strategy continue to diverge in their conclusions rather than converge, with deterrence advocates and persistent engagement advocates becoming more entrenched in their convictions.¹⁶ This divergence occurs because little to no convincing data exists to persuade either side of what the



Dr. Benjamin Jensen is a Senior Fellow at CSIS for future war, gaming, and strategy in the International Security Program and is also a Professor at Marine Corps University School of Advanced Warfighting. Over the past decade, Dr. Jensen has shaped defense analysis, crisis response, and military planning through his partnerships with numerous military, government, and international bodies, including DARPA, NATO, and the U.S. Army. Author of four influential books, his most recent work centers on military innovation and AI. He served as the Senior Research Director and lead author for the U.S. Cyberspace Solarium Commission. Dr. Jensen holds a PhD from the American University School of International Service and continues to serve as a reserve officer in the U.S. Army.

facts are to uphold any claims of one side or criticism of the other.

Attack typologies can be useful for defense but lack systematic comparisons, and do not help establish patterns and trends outside of attack types. It is therefore a different level of analysis, where it is not about statecraft and more about technical dimensions of best practices in terms of technical defense. One attack framework created by MITRE Corporation named ATT&CK, utilizes a mixed method of technical and behavioral collection methods, and could be incorporated into our collection processes in subsequent versions of DCID.¹⁷

Overall, there are multiple types of social science analyses available to researchers, but the genre of quantitative social science, is largely missing from current analysis, thereby revealing the precarious foundations of the field of cybersecurity.¹⁸ As outlined in previous versions of DCID, a codebook exists to ensure researchers understand how the data was coded.¹⁹ Previous publications outline the data collection fields that include the countries involved, the date, website sources, and ten additional categorical classifications. New to this dataset are binary indicators for supply chain, ransomware, and information operations, as well as a categorical variable on the infrastructure sector, as outlined by the NIST cybersecurity framework.²⁰

The peace science data collection revolution brings us to the methods utilized for the collection of the data contained in DCID. Two datasets, the Militarized Interstate Dispute Data (MID) and International Crisis Behavior Data (ICB), are efforts that contributed to this revolution.²¹ Over the decades, researchers in the international relations field moved beyond narrative descriptions absent structured, coding methodologies that lent themselves to replication studies and searching for aggregate patterns. In the case of Cold War era pioneering data efforts, the use of early punch card computing and coding schemes was designed to under-

stand the causes of war and which crises were more likely to escalate. It was academics trying to serve the broader policy community. Here, we make a similar intervention, trying to take an inductive approach to knowledge construction that facilitates bridging the gap and offering empirical data other researchers can use and policymakers can review to develop cyber policies and strategies.²²

The state of data collection leaves cybersecurity, national security, and social science research in a vacuum. Those researching trends in cyber incidents are left without clear sources of unbiased, peer-reviewed information. These pathologies provide the motivation for this project as we bring the DCID data into the new decade.

Coding Cyber Incidents

To code cyber incidents means isolating in time and space given available information regarding attempts by rival states to launch a major cyber operation in pursuit of foreign policy objectives. This definition sets the term “incident” apart from everyday cybercrime and constitutes a range of activities from leveraging patriotic hackers to high-end cyber tools exploiting configuration vulnerabilities in national networks. Each incident might include hundreds if not thousands of individual attempts to breach a network and deposit malware – just as a major military operation encompasses countless tactical engagements and battles. In the same way that earlier work on militarized disputes and crises isolated particular acute state interactions, the DCID attempts to isolate how states compete in and through cyberspace.

As the United States (U.S.) struggles to implement breach data notification reporting laws that would provide data for awareness of cyber incidents, a series of consequential cyber operations occurred from 2020 to 2021.²³ From SolarWinds to the Microsoft Exchange vulnerability to the Colonial Pipeline ransomware attack, the U.S. is reacting to incidents with little comprehensive awareness of trends and patterns. Data are necessary to anticipate future challenges and to measure the effectiveness of our current strategy.

There are three reasons the national cyber strategists require a publicly available database of cyber operations. First, there is the issue of strategic planning and budget justification. In the U.S., DoD must demonstrate that it is meeting the requirements for cyber forces at the strategic level. Publicly available data can provide an open-source method for general analysis that demonstrates the requirements for offensive and defensive forces. The rationale for funding and resources does not withstand public scrutiny without a medium to communicate trends in cyber operations.

Second, publicly available data provide an indication of what is known for larger audiences, and not just military practitioners. Data that engage public sources can be leveraged to understand how cyber operations become known to the public, from what sources, and for what purpose. We also have no reason to assume that what is revealed publicly is not a representative sample of the presumably larger, covert operations.

Finally, and perhaps most importantly, the international community is interested in the sponsorship of public goods that allow the academic community to participate and contribute to scholarship that advances the theoretical aspects of cyber conflict theory. As such, our dataset is a public good that is free to access and use for the academic community. Academics debate persistent engagement, deterrence, coercion, and escalation, but do so with little hard data to demonstrate the efficacy of each of their theories.²⁴ Without data, evidence on the competition of theories is absent, and new theories will not mature, which leads to suboptimal policy.

We manage the collection of the data in a novel manner, using a combination of academics, U.S. military staff officers, and student interns. For this research, a cadre of researchers provided guidance to twelve student interns in the Virtual Student Federal Service (VSFS).²⁵ Using an interactive process, the team developed a method of collecting, reviewing, and filling out the data needed to create a full and original dataset that included a plethora of independent variables and sourcing information.

After an introduction to the existing academic literature, including journals, books, blogs, websites, and prior data collection efforts, the students used publicly available information (PAI) to expand on the DCID 1.5 dataset, which gathered data through 2016.²⁶ For inclusion of cyber incidents in this dataset, there must be open-source evidence that a nation-state is culpable for the cyber operation in question.²⁷ After an initial round of data gathering, the students cross-reviewed the work of other students. To ensure data quality, a team of experienced researchers reviewed the students' work. At the end of their efforts, reliability statistics were collected after a review of the final coding outcomes.

As outlined in previous versions of DCID, the codebook exists to ensure researchers collect data accurately.²⁸ Previous publications outline the data collection fields, which include the countries involved, the date, website sources, and ten additional categorical classifications. New to this dataset are binary indicators for supply chain, ransomware, and information operations, as well as a categorical variable on the infrastructure sector, as outlined by the NIST cybersecurity framework.²⁹ Since the researchers are primarily English speakers, we accept the Anglophone bias inherent in our research methods and acknowledge this caveat.

Due to the covert or clandestine nature of cyber operations, as well as the limited public reporting on state-initiated action in the domain, the coding processes for this project are human-driven. Although machine learning web-scraping processes have been proposed,³⁰ we concluded that the nuance and meticulous procedures needed for coding cyber operations require a human touch. Training processes include the instruction of uniform search terms and procedures by project leaders so that accuracy and replicability are assured. Project leaders then verify all incidents coded for final inclusion or exclusion into the dataset.

Researchers should be aware of biases and caveat results when conducting analysis using the DCID. This issue is common across all datasets; here we provide an open-source dataset that others can use and modify to suit their needs. We also review all other publicly known incidents

coded in other datasets to ensure complete coverage. Many incidents were discarded due to incomplete sourcing, the likelihood that are criminal operations and not state directed, and the bias to report incidents that attack financial systems. For example, some datasets include an overabundance of cryptocurrency attacks that we could not attribute to state action, or even external attacks, since many operations are insider attacks.

Dataset Details

The core of any dataset is the explicit original variables identified and documented. In DCID 2.0, there are several variables coded for each cyber incident. The first are the start dates and end dates for each incident, reported as accurately as possible. For the start date, most reports analyzed gave approximate month and specific year. The end date given for each operation is the approximate earliest public reporting of the termination of the incident.

While multiple terms for actions in cyberspace exist across the academic databases, the term “incident” has a very specific meaning in U.S. code,³¹ which we build on here.³² “The term “incident” means an occurrence that (a) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system, or (b) constitutes a violation or imminent threat of violation of law, security, policies, security procedures, or acceptable use policies.”³³ We generally avoid the term cyber-attack since it is contested and devoid of meaning in popular usage.³⁴

Next is the cyber method variable, which consists of four overall categories. The first is Vandalism (Website defacements, propaganda) where hackers use SQL injection or cross-site scripting (forms of command code) to deface or destroy victims’ web pages. Although rather benign, these attacks may have important psychological effects on their intended audience. The second category is denial of service (DDoS, Botnets, data blocking): DDoS attacks flood particular Internet sites, servers, or routers with more requests for data than the site can respond to or process. Such attacks are coordinated through “botnets,” or a network of computers that have been forced to operate on the commands of an unauthorized remote user. The primary impact of DDoS attacks via botnets is the temporary disruption of service. The third category is network intrusions (“trapdoors” or “trojans” and backdoors).³⁵ Spear phishing is utilized to inject these cyber methods into networks. Here the initiator sends emails to employees or contractors of the targeted network and, if the email is opened, the intrusion is introduced to the system. Finally, the fourth category is network infiltration with examples of attacks including logic bombs (wiper malware), viruses, worms, and keystroke logging.³⁶ These methods force computers or networks to undertake tasks they would normally not undertake.

Target type is the next variable coded and comes in three forms. The first is private/non-state includes targets such as the financial sector, power grid, or multinational corporation (MNC). The second is government non-military variable, with the U.S. State Department and Department of Homeland Security (DHS) government websites, or the Office of Personnel Management

(OPM) as primary examples. Last is the government military variable, where entities such as DoD, U.S. Cyber Command, or U.S. Strategic Command are primary examples here.

The next category for the cyber variables coded in DCID is titled “strategic objective for initiators” and comes in four forms: 1) Disruption: Examples include taking down websites or disrupting online activities. These are usually low-cost, low-pain incidents such as vandalism or DDoS techniques. 2) Short-term espionage: These are acts that gain access which enables a state to leverage critical information for an immediate advantage. 3) Long-term espionage is an event that seeks to manipulate the decision-calculus of the opposition far into the future through leveraging information gathered during cyber operations to enhance credibility and capability, an example being China’s theft of Lockheed Martin’s F-35 plans. Finally, 4) De-grade is the category that includes attempts of physical degradation of a target’s capabilities.

Our next variable is binary and labeled “cyber-enabled information operation” (CIO). For our purposes, we want to distinguish information warfare operations from the more universal awareness of attacks in and through cyberspace as conceived by the public. We also want to avoid the broad definition of information operations as defined by the U.S. military, which includes electronic warfare, psychological operations, and social network exploitation, among others. To avoid muddying the waters more, we instead focus on information operations in the midst of cyber incidents, what we call cyber-enabled information operations (CIO).³⁷

The restriction to operations launched during ongoing cyber operations allows us to focus on how information and data are weaponized adjunct to cyber incidents and campaigns. Rather than documenting more broad attacks on truth and meaning, we seek to understand how information can be manipulated and utilized to message in a psychological operation against a target. Its plausible that CIO’s are improved using demographic or personal data stolen from initial cyber incidents, to personalize or tailor a specific message to manipulate a specific audience.

The next variable is titled “objective achievement” and is binary: Did the cyber incident achieve its intended purpose is the main question asked of coders. For example, did the disruptive attack successfully shut down a website via denial of service? Did an espionage technique breach the intended network and steal the information it sought to acquire? Did the degradation achieve damage to its intended target?

The “Concession” variable is where a binary score of the presence or absence of a concessionary behavioral change. Coding behavior change can be considered quite subjective, and therefore collaboration with multiple peers and researchers has been utilized in the coding of this variable. If there is an observable change in foreign policy by the target state as a result of the initiator’s cyber operation, we code the presence of a concession. These events are quite rare, as it has been found that there are limitations on the coercive power of cyber operations.³⁸

In terms of the severity of the impact of each cyber incident, a revised severity scale is included in this version of DCID. The scale is interval and is numbered 1 through 10, with “1” indicating

the least severe cyber operation and “10” denoting the most severe possible incident. It must be noted that in the DCID version 2.0, no state-initiated cyber operation has evoked a severity score above “6.”³⁹ For a cyber incident to be coded with a severity score, there must be a successful breach, where widespread destruction has been found on either a single or multiple networks. An example of an incident with this score is the Iranian degradation attack on Saudi Arabia’s oil giant Aramco, in which wiper malware erased the hard drives on nearly 30,000 workstations in 2012.

Cyber incidents coded with severity scores 1 through 5 have traits as follows: an incident coded as “1” are the more passive cyber operations, where packet sniffing and probing, as well as spyware that has not been activated and is found before it has been, are examples of these low-level operations. Incident levels labeled as “2” are forms of cyber harassment, propaganda, and events that deny access to information or disrupt daily activity on a network for a short duration. Incidents that are coded with a severity score of “3” are most espionage campaigns, in which we see the theft of valuable or classified information from a single network. Cyber incidents that are given a “4” severity score are coded as such when there are multiple network and widespread data breaches and espionage activity from the initiating state. Finally, incidents receiving a “5” severity score are those that infiltrate either a single or multiple critical networks and attempt physical destruction.

Next is “Damage Type” conceptualized from scholars and is categorical ranging from 1 to 4.⁴⁰ Where (1) refers to “Direct and immediate” damage and costs that are felt immediately. Then (2) “Direct and delayed” damage by an incident that takes months if not years to disrupt or damage. Next is (3) “Indirect and immediate” damage which was not the original intent of the imitator. Examples include reputational damage or loss of confidence in the target by an audience. Lastly, (4) “Indirect and delayed” damage and costs for incidents that would be felt at a future point in time.

Finally, the last variable carried from DCID 1.5 is “Specific political objective.” The aim is deciphering why the cyber incident was launched in the first place. For example, for the Sony Hack the objective was to stop the release of the movie *The Interview*. A maximum of two political objectives is allowed.

Considering the changing trend of cyber incidents and to improve analysis, the authors updated DCID with three new variables. The first variable is categorical and labeled “Critical Infrastructure” (CI). This additional variable differentiates between targets vital to national and economic security of the nation as designated by DHS and the Cybersecurity and Infrastructure Security Agency (CISA).⁴¹ Further, CI is coded 1-16 to represent the 16 sectors. In addition, noticing a blind spot, the authors added “17” to represent academic institutions that produce critical and innovative research for the nation.⁴² The categorization of entities will help policymakers and industry alike understand the evolution of targets as rivals shift interest and seek influence across sectors.

Our second addition is a binary variable labeled “Supply Chain.” We consider targeted companies that serve or provide a service to any of the critical infrastructures listed (1-17). Further, the service or product to the critical infrastructure may be in different forms such as software for network, technology, or IT management. For example, it may include billing systems, cloud services, or remote access systems like a virtual private network (VPN). SolarWinds serves as a reminder that cyber actors target supply chain firms and attempt to manipulate products for backdoors, steal passwords or relevant data, and disrupt or engage in espionage.

The final addition is a binary variable labeled “Ransomware.” An incident is coded as ransomware if a target suffers from a loss of data, control, unauthorized encryption, or otherwise locked out of their systems until a “Ransom” is paid in currency, either hard or digital. Previously recorded incidents were retroactively updated with the new variables for a complete set.

In practicality, any set of incidents gathered in a dataset includes only a biased subset of existing cyber actions. The bias is important for international security analysis, as it represents those attacks publicly known between two actors.⁴³ This provides a semi-complete picture of the landscape for deterrence, persistent engagement, and escalation studies, as well as comparative statistics between time periods. *Despite the limitations of data collection efforts, comprehensive data of what is known is more valuable than speculation on what is unknown.*

The Devil is in the Details – Cyber Relations over Time

Figure 2 shows a graphical representation of cyber incidents categorized by strategic objective for initiators for the years 2000-2020. Espionage campaigns make up over 61 percent of the data, indicating that the battle for information and intelligence is where states are finding utility with cyber operations. Whether it be short-term espionage incidents that aid in operations in the information environment, or long-term ones that steal intellectual property to fill a technological gap in one’s military organization, it is information asymmetries and intelligence gathering that provide tangible value to initiating states’ national security objectives.

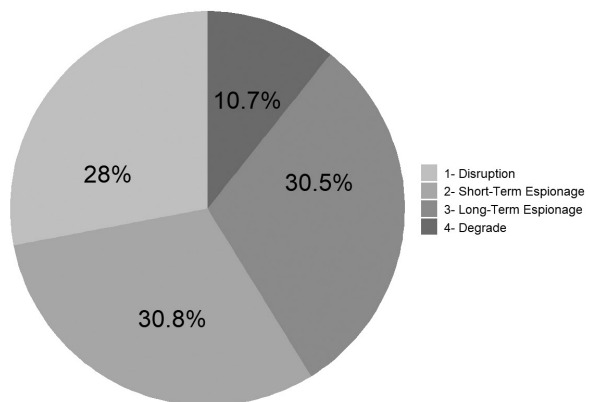


Figure 2: Incidents by Strategic Objective: 2000-2020

Disruptions are utilized roughly 28 percent of the time, are low-risk and inflict pain, but can be interpreted as a type of ambiguous signal intended to demonstrate displeasure with a previous action of the target state.⁴⁴ Degradations, utilized just over 10 percent of the time, are riskier and escalation-prone as their intent is to permanently deny the target a capability it once previously

had. These types of cyber incidents are also the most likely to produce concessions from the target state.⁴⁵ However, they are expensive as well as risky, and are usually only developed and deployed by the powerful states, making them rarer.

Table 1 shows the strategic objective categories parsed by the initiating country for the previous iteration of DCID that covers 2000-2016. China, Russia, Iran, and North Korea, the four major cyber adversaries of the U.S., lead the world in terms of initiating countries, and target the world’s only superpower often. This will be used in Table 2, which provides the updated list of strategic objective initiators.

Table 1. DCID 1.5: 2000-2016

Initiating Country	Disruption	Short-term espionage	Long-term espionage	Degrade	Total
China	17	37	18	2	74
Russia	19	23	12	11	65
Iran	8	9	12	4	33
North Korea	13	3	6	4	26
United States	0	1	9	11	21
Pakistan	11	1	1	0	13
Israel	1	0	7	1	9
India	6	1	0	0	7
South Korea	4	3	0	0	7
Japan	3	0	0	0	3
Ukraine	1	0	0	1	2
Turkey	1	1	0	0	2
Georgia	1	0	0	0	1
Syria	1	0	0	0	1
Taiwan	0	1	0	0	1
Vietnam	0	0	0	1	1
Total	86 (32%)	80 (30%)	65 (24%)	35 (13%)	266

Source: Data from Maness, Valeriano, and Jensen, 2019.

Table 2 shows the updated descriptive statistics by strategic objective, with the four authoritarian countries leading the pack once again. Given the fact that most democratic countries around the world are restrained from launching frequent cyber operations, this is not surprising. In the U.S., for example, for a long time the authority to launch an offensive cyber operation (OCO) lay solely with the President. After the revision of the DoD Cyber Strategy in 2018, the commander of USCYBERCOM now has Title 10 authority to launch cyber operations that are considered below the threshold of armed conflict, with the President retaining the sole authority for those considered to be above that threshold.⁴⁶ Furthermore, the U.S. does keep most of its cyber methods and actions classified, making this open-source data more than likely undercounting U.S. cyber operations as a result.

EXPANDING THE DYADIC CYBER INCIDENT AND CAMPAIGN DATASET (DCID)

Table 2. DCID 2.0 Update: 2000-2020

Initiating Country	Disruption	Short-term espionage	Long-term espionage	Degrade	Total
China	22	49	42	2	115
Russia	28	39	30	16	113
Iran	13	21	21	10	65
North Korea	24	10	19	6	59
United States	1	1	9	9	20
Pakistan	13	4	3	0	20
Israel	2	0	7	1	10
India	6	2	0	0	8
South Korea	4	3	0	0	7
Japan	3	0	0	0	3
Ukraine	1	0	0	1	2
Turkey	1	1	0	0	2
Georgia	0	1	0	1	2
Syria	1	0	0	0	1
Taiwan	1	0	0	0	1
Vietnam	0	1	0	0	1
Total	120 (28%)	132 (31%)	131 (31%)	46 (11%)	429

China and Russia still top the list as the most frequent initiators of cyber operations, with their great power adversary, the U.S., being the primary target. China has continued its espionage campaigns, and these have largely increased during the years 2016-2020. After a slight détente with the U.S. in 2015 following the Office of Personnel Management (OPM) hack, it seems that China is back to its old ways. Russia’s hacking has also spiked considerably, with the U.S. and Ukraine targeted the most by these recent cyber operations. Iran has increased its cyber presence in the Middle East, and North Korea has turned to cybercrime, including cryptocurrency theft, to bulk up its numbers during these four years.

Table 3 shows the countries that have been victims of cyber operations in descending order of frequency. The U.S., South Korea, Ukraine, India, and Israel have been subject to cyber operations with the greatest frequency. Increased intensity between rivals is the likely culprit behind this increase. The U.S. continues to be barraged by Russia and China; South Korea and North Korea continue their intense rivalry in cyberspace; Ukraine is on the brink of a Russian invasion at the time of this writing; and the India-Pakistan and Israel-Iran rivalries continue to endure. Furthermore, Table 3 indicates the percent increase in cyber incidents each state has experienced between DCID 1.5 and DCID 2.0. While most nations have continued to see increased frequency of operations, the United Kingdom and Turkey stand out as the two countries experiencing the greatest increase in operations, mainly due to low-incident frequency in a database that includes exclusively rival dyads.

Table 3. Countries by Frequency of Target
(Comparison of DCID 1.5 & DCID 2.0)

Targeted Country	DCID 1.5	DCID 2.0	Percent Increase
United States	82	138	68
South Korea	26	46	59
Ukraine	15	28	87
India	20	28	40
Israel	11	20	82
Japan	13	18	38
Iran	14	17	21
United Kingdom	3	13	333
Russia	11	12	9
Saudi Arabia	7	12	71
Taiwan	7	12	71
Turkey	4	11	175
Georgia	6	8	33
Pakistan	7	8	14
Vietnam	4	8	100
Philippines	5	8	60
China	7	7	0
Lithuania	4	6	50
Germany	3	5	67
France	3	4	33
Estonia	4	4	0
Canada	2	3	50
Poland	3	3	0
Syria	1	1	0
Lebanon	1	1	0

Figure 3 displays the frequency of cyber incidents in the data over time. The year represents the end date of the operation. DCID 2.0 includes operations as recent as 2021 and subsequently captures additional operations that were not yet public upon release of version 1.5. Since the significant jump in 2014, the prevalence of cyber operations has remained high. However, the increase in initiated cyber operations remains concentrated among authoritarian countries, while democracies continue to be targeted at increased rates, demonstrating the imbalance between these two types of systems.

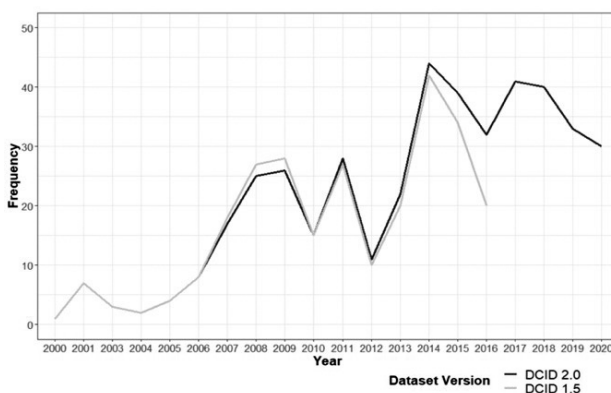


Figure 3: Frequency of Cyber Incidents Over Time (DCID 1.5 vs. DCID 2.0)

A critical question often ignored in cybersecurity is the efficacy of operations. Do cyber operations achieve their objectives when hacking their targets? Other key questions include the participation of third parties or the connection to information operations. Table 4 represents the percentage of cyber operations that have generated concessions, have had multiple initiators, have a cyber-enabled information operation result in the initiation, and have achieved their intended objective in terms of breaching the targeted network. With the addition of new incidents into DCID 2.0, the efficacy of the operations has dropped across all dimensions. There have been no new observable behavioral changes as a direct result of a cyber operation for the years 2016-2020. China has focused on disinformation campaigns along with its more tailored espionage operations, which are arguably less coercive.

In this dyadic dataset, we also see very few joint state initiatives, as countries seemed to keep to themselves when launching their operations. In this version of the data, cyber-enabled information operations cover about a fifth of the dataset. As influence operations and disinformation

continue to be weaponized, we expect this trend to grow as future updates of the data are produced. There is a clear connection between cyber operations and digital influence operations, but the basis for this is unclear.

Table 4. Incident Categorization, Count, and Percent of Incidents

	Total Incidents	Concession	Third Party Initiator	Information Operation	Objective Achievement
DCID 1.5	266	12 (4.5%)	25 (9.4%)	73 (27.4%)	242 (91%)
DCID 2.0	429	12 (2.8%)	32 (7.5%)	96 (22.4%)	368 (85.8%)

Severity and Impact

Figure 4 shows cyber incident severity over time. Although the number of cyber operations continues to grow as states integrate them into their foreign policy and military strategies, the relative severity over time has remained quite constant. Most cyber operations have severity scores between “2” and “4,” which ranges from disruptions and propaganda to network espionage in these types of operations we see states find the utility of cyber incidents as force multipliers in hybrid operations. Russia utilizes cyber operations to sow chaos and confusion by spreading propaganda in target countries. China’s espionage campaigns, in its view, are contributing to its rise as an economic and military superpower. It is these types of operations we expect to see more in the future as governments learn the primary utility of cyber operations.

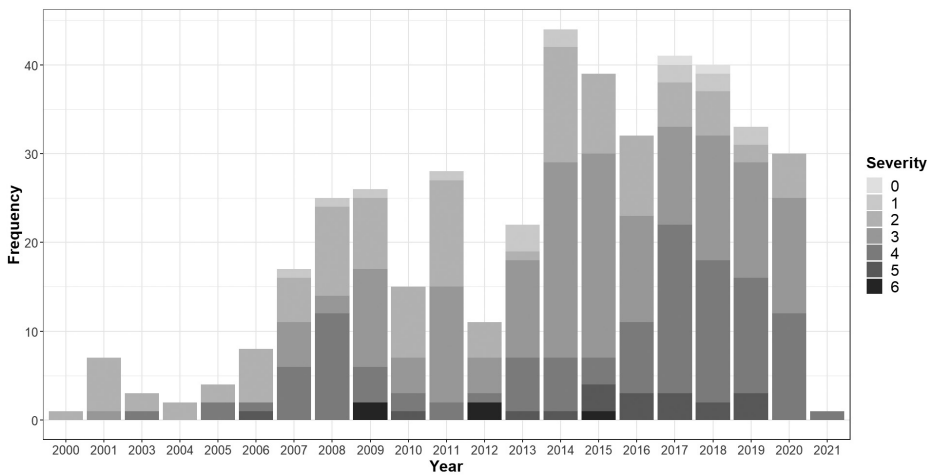


Figure 4. Severity of Incidents Over Time: DCID 2.0

Table 5 shows which severity levels have increased the most between DCID version 1.5 and 2.0. As expected, we see severity levels “3” and “4” rise the most, as these categories encompass primarily espionage campaigns. Attempted physical destruction, which are operations under severity level “5” have also risen sharply. Strategic sabotage is being attempted more often, but with limited success.⁴⁷

In terms of the severity levels between “7” and “10,” we have yet to observe these more

dangerous operations. States have yet to leverage cyberspace to take down financial markets, turn out the lights for a long period of time, or intentionally contribute to the loss of life. There are deterrence and restraint mechanisms at play here, as no nation wants to be the first to take these more severe actions, which would likely lead to a more dangerous and unstable cyberspace.⁴⁸

Ransomware, Supply Chain, and Critical Infrastructure

Ransomware attacks are attributed to only four states during the years 2000-2020. Looking at Table 6, acts of ransomware remain a motivation of non-state actors, primarily cyber-criminal groups. The Russia-based, non-state group REvil became internationally known due to its role in the Colonial Pipeline incident, which shocked oil supply as well as prices in the Eastern U.S. in 2021.⁴⁹ The group has since been disbanded and its members arrested by the Russian government. Russia has launched false ransomware incidents, such as NotPetya, to act as smokescreens so that it can more freely maneuver within Ukrainian government networks, but this method is not common.⁵⁰

Table 6. Frequency of Ransomware Incidents between DCID 1.5 and 2.0

Initiating Country	DCID 1.5	DCID 2.0	Percent Increase
Russia	3	4	33
China	1	3	200
North Ko-rea	0	3	300
Pakistan	1	1	0
Total	5	11	120

Given the potential lucrative earnings that successful ransomware attacks produce, these operations benefit states with limited gross domestic product output and trade. As such, we can expect isolated and desperate actors like North Korea to continue to use ransomware as an alternative, low-cost method to fund its regime. North Korea has grown quite adept in cybercrime in recent years, with the theft of cryptocurrency as well as the famous WannaCry ransomware operation being prime examples. In 2021, the North Korean regime stole nearly \$400 million in cryptocurrency.⁵¹ WannaCry, launched in 2017, led to nearly \$4 billion in losses globally.⁵² Whether to earn currency for the regime or cause global disruptions, North Korea is punching above its weight regarding damaging criminal operations.

Table 7 highlights how cyber incidents targeting supply chains are increasing in recent years. China, Russia, Iran, the U.S., and North Korea are the most active states, with 88 percent of all incidents. Exploiting global supply chains and supply-side trust entities with malware is now a common tool in the cyber domain. The reason is simple, affiliates and trusted entities generally spend less on cyber defenses, focus less on updating their equipment, and are ripe targets for phishing attacks. Attacking the weaker third-party actor is a viable means of penetrating the hardened bunker that is usually state-based cyber entities.

Analyzing supply chain incidents further, Figure 5 visualizes the share of supply chain incidents by Initiator from 2000 to 2020. Through the years, there has been an average of

Table 5. Cyber Severity Changes between DCID 1.5 and 2.0

	0	1	2	3	4	5	6
DCID 1.5	0	9	92	97	53	12	3
DCID 2.0	2	15	115	159	115	18	5
Percent Increase	200	67	25	64	117	50	67

EXPANDING THE DYADIC CYBER INCIDENT AND CAMPAIGN DATASET (DCID)

8 supply chain incidents per year among all initiators. In the first decade (2000-2010), China targeted the highest quantity of supply chain entities with 16 incidents out of 37 for the entire decade, with a sharp drop in the final year (2010). The U.S. follows China with 9 incidents, followed by Russia with 5. However, in the next decade (2011-2020), there is a significant growth in targeting supply chains by Russia with a total of 33 incidents, overtaking China (31), Iran (19), North Korea (11), and the U.S. with only 4 incidents. In all, the first decade of the twenty-first century, supply chains experienced 37 incidents compared to 110 incidents for the second decade. This is a 197% increase and highlights the strategic focus of China, Russia, Iran, U.S., and North Korea.

Table 7. Frequency of Supply Chain Incidents between DCID 1.5 and 2.0

Targeted Country	DCID 1.5	DCID 2.0	Percent Increase
China	32	48	50
Russia	23	38	65
Iran	10	19	90
U.S.	10	13	30
North Korea	5	12	140
Israel	5	6	20
Pakistan	1	4	300
South Korea	2	2	0
Vietnam	1	1	0
India	1	1	0
Taiwan	1	1	0
Turkey	1	2	100
Ukraine	1	1	0
Total	93	148	59

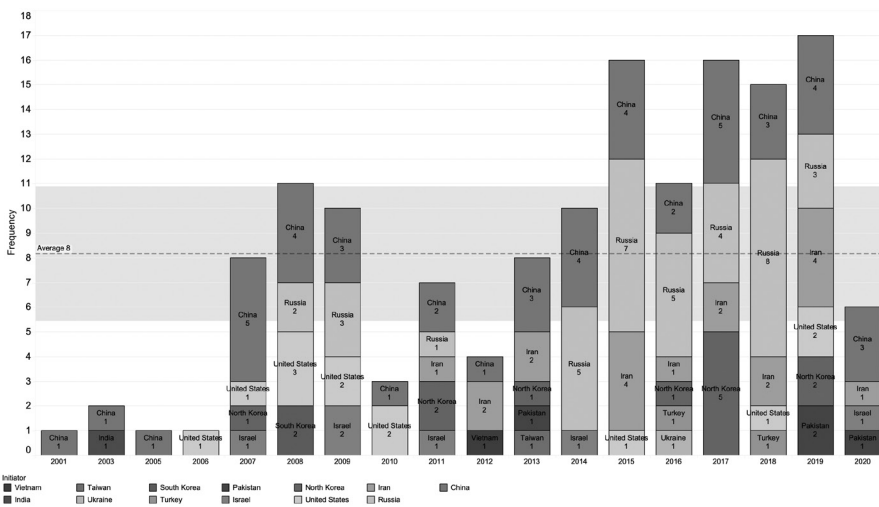


Figure 5. Supply Chain Incidents Over Time DCID 2.0

* Note: The researchers found no supply chain incidents in the years: 2000, 2002, 2004 and are therefore absent from this time-series graph.

Table 8 breaks down the frequency of attacks on Critical Infrastructure (CI) between DCID 1.5 and 2.0. The most targeted CI among both versions is government facilities, with about 42% of the total share. The next most frequent CI sectors targeted are the academia and information technology sectors, which make up around 10 percent each. With strategic competition among states on the rise, we expect these sectors to continue to be targeted.

Public health facility targeting is on the rise, which is concurrent with the rise in ransomware

Table 8. Frequency of Critical Infrastructure Incidents between DCID 1.5 and 2.0

CI Sector	DCID 1.5	DCID 2.0	Percent Increase
Government Facilities	128	179	40
Academia	18	41	128
Information Technology	29	44	52
Financial Services	18	31	72
Energy	18	29	61
Defense Industrial Base	12	19	58
Public Health	4	17	325
Communications	7	16	129
Transportation	7	14	100
Commercial Facilities	12	12	0
Nuclear Reactors, Materials, Waste	8	13	63
Chemical	2	5	150
Critical Manufacturing	3	4	33
Water and Wastewater Systems	0	3	300
Dams	1	1	0
Emergency Services	0	0	0
Non-CI	1	1	0
TotalS	268	429	60

attacks during the COVID-19 crises during 2020 and 2021. Despite conventional wisdom, there is no significant evidence of increased attacks on nuclear facilities, financial services (economic cyber warfare), or water treatment facilities. This finding does not invalidate the need to protect these sectors, but the idea of a dramatic increase in these sorts of attacks is not evidenced by this version of the data.

To analyze CI further, Figure 6 visualizes CI according to initiating state. Once again, China, Russia, Iran, and North Korea take the lead in targeting CI over the U.S.. Where China has conducted the most operations against CI, it focused primarily on Government Facilities (54), followed by Academia (13) and Information Technology (12).

Russia follows China closely in focusing more on Government Facilities (56), then Academia (10) and Energy (9).

lights that, while both advanced in cyber capabilities, each has separate aims in its operations. China is focused on cyber operations that steal information from the private and public sectors for diplomatic aims or improving its markets through intellectual property theft. On the other hand, Russia is less interested in improving its domestic market through intellectual property theft and more interested in cyber as a tool of disruption.

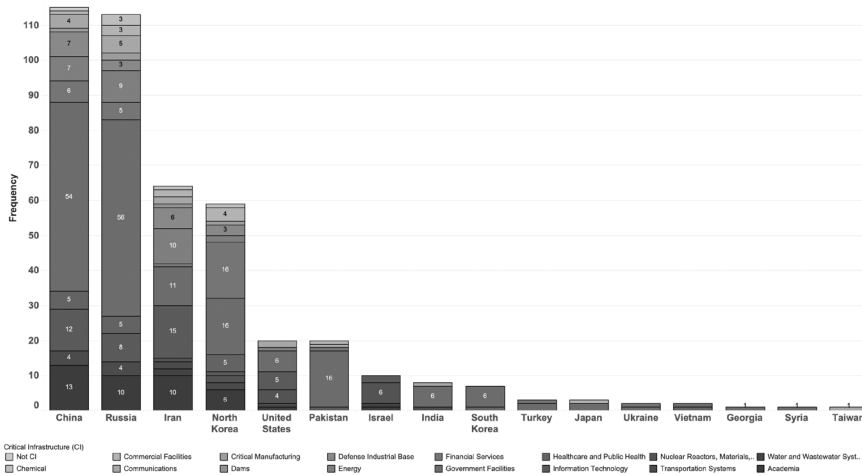


Figure 6. Critical Infrastructure Incidents by Initiator

Next are the nascent but rapidly improving cyber states. Iran focused on Information Technology (15), then Government Facilities (11), and tying for third is Academia and Energy for 10 incidents each. Instead, Iran’s cyber operations are tailored less on circumventing international sanctions and toward a diplomatic end. Iran seeks a regional power rebalance by targeting its top rivals, Israel and Saudi Arabia, signaling its resolve.

North Korea pursues a different approach as the other nascent power. This is because its top two targets are Financial Services and Government Facilities, with 16 incidents each, and its third target is Academia (6). North Korea uses cyber operations to circumvent international sanctions to fund their regime, spy on South Korea and academia that influences policymakers. With unsuccessful diplomatic efforts under the Trump administration, North Korea is likely to explore other ways to leverage its cyber operations in seeking sanction relief.

By contrast, as an advanced cyber actor, the U.S. is showing restraint, owning only 5 percent of all CI incidents across 20 years. This might be in part due to the covert nature of U.S. cyber operations, the desire to maintain asymmetrical capabilities a secret, or leadership refraining from declaring operations against rivals. This could also be explained by the lack of technical analysis available by cybersecurity firms when analyzing suspected U.S.-initiated incidents.

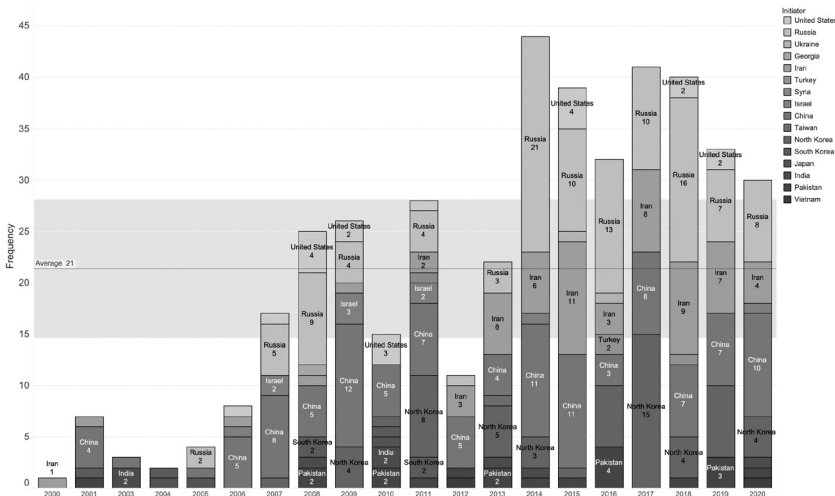


Figure 7. Critical Infrastructure Over Time DCID 2.0

* Note: The researchers found no incidents in the year 2002 and is therefore absent from this time-series graph.

To provide a time series analysis on CI, Figure 7 visualizes CI incidents by initiator from 2000 to 2020. Across the years, there is an average of about 21 incidents per year among all initiators. In the first decade (2000-2010), China targeted the highest number of CI at

41 out of 108 incidents, or a share of about 38 percent for the entire decade. However, like the trends in Figure 6, Russia increased its targeting of CI from 2011 to 2020 to 93 incidents representing about 29 percent of the 321 incidents recorded for that decade. China followed closely with 73 incidents (23 percent), next Iran with 59 incidents (18 percent), and finally North Korea with 53 incidents (17 percent).

In the first decade of the 21st century, Critical Infrastructure experienced 108 incidents compared to 320 in the second decade. This is a 196 percent increase and further highlights the investments made by China, Russia, Iran, North Korea, and the U.S. in their capabilities to initiate cyber operations. Further, the data indicate that nefarious actors actively target critical infrastructure, and governments around the globe need to exercise resilience and continue to improve their defenses.

Future Directions and Conclusion

This new dataset provides the basics for research into the efficacy of the strategies of persistent engagement, deterrence, and restraint. Future work includes four key areas of data collection. Combining this data with political speeches and signaling demonstrations, military exercises and conventional military incidents, and other forms of engagement and conflict short of war, as competition and engagement, deterrence, and escalation occur in multiple domains.

It is also important to note that the cyber incident data can link to other existing data, including Department of Justice and FBI indictments and sanctions reported publicly through the Congressional Research Service,⁵³ Department of Treasury,⁵⁴ and the Global Sanctions Data Base⁵⁵ to produce the cross-database linkages of possible cause and effect. In the past, some have linked this data to event datasets to expand analysis to different domains.⁵⁶ Additional data fields also can provide a richer dataset for analysis, such as the Advanced Persistent Threat (APT) attributed to each attack and the corporate targets of the attack.

The next update of DCID will include 2021-2022, pivotal years as they include the Russian invasion of Ukraine, a key point for cybersecurity scholars, and the rise of ransomware attacks during the Pandemic. The project team will continue the legacy of data collection on cybersecurity, hopefully expanding all hybrid warfare actions in the near future.

DCID 2.0 provides a way for cybersecurity research to undertake quantitative data of cyber incidents for the academic and research communities. These data allow for a social science standard for changes over time periods, trend analysis, and hypothesis testing, where data that lacked ratio qualities did not exist. Although the data are an incomplete record because of the unique aspects of cyber, they do capture a sample useful for the study of deterrence, persistent engagement, and escalation. With these data, we hope qualitative claims can be backed by empirical support rather than speculation. This process,

sometimes called normal science, will allow us to learn the correlations and hypothesize the causation of changes in cyber incident trends. Our hope is the data will converge and clarify arguments with statistical facts, rather than continuing to allow them to diverge into conjecture or gross assumptions that jump centuries. 🛡️

DISCLAIMER

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

NOTES

1. This research would not be possible without our Virtual Student Federal Service data collection team which includes Katrina Villacisneros, Brian Wheat, Ingrid Fontes, Kim Chamberlain, Bridget Flynn, Thomas Deen, Catherine Smith, Nicholas D'Onofrio, Alexandra Restrepo, Siddharth Suman, Sarah Chen, Zachery Gagnon and Jason Niro. Furthermore, this project includes members of the scholarly community who actively work for the U.S. government and the Department of Defense. Our ability to cover and dissect U.S. directed events is limited. We do not attribute the 20 U.S.-responsible cyber incidents to the U.S. government, and included them as strictly the opinions of private sector actors and organizations. As a resource to the wider cybersecurity community, we provide the tools for others to cover global cyber events and build on this work in a comprehensive manner.
2. Branch, Jordan, "What's in a Name? Metaphors and Cybersecurity." *International Organization* 75, no. 1 (2021): 39-70.
3. Senator Angus King and Representative Mike Gallagher, United States of America Cyberspace Solarium Commission, March 2020, 1, <https://www.solarium.gov/report>.
4. UKGCHQ, The Cyber Threat, 2016. Accessed February 9, 2022, <https://www.gchq.gov.uk/information/cyber-threat>.
5. Senator Angus King and Representative Mike Gallagher, United States of America Cyberspace Solarium Commission, March 2020, 1, <https://www.solarium.gov/report>. Pg. 78, 4.3
6. Valeriano, Brandon and Ryan C. Maness, "The Dynamics of Cyber Conflict between Rival Antagonists, 2001-2011" *Journal of Peace Research* 51, no. 3 (2014): 347-360.
7. Maness, Ryan C., Brandon Valeriano, and Benjamin Jensen, "The Dyadic Cyber Incident and Dispute Data, Version 1.5," (June 2019) <https://drryanmaness.wixsite.com/cyberconflict/cyber-conflict-dataset>.
8. Poznansky, Michael, and Evan Perkoski, "Rethinking secrecy in cyberspace: The politics of voluntary attribution." *Journal of Global Security Studies* 3, no. 4 (2018): 402-416.
9. See CSIS: Significant Cyber Incidents, 2022, <https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents>, and CFR: Cyber Operations Tracker, 2022, <https://www.cfr.org/cyber-operations/>. In addition, CSIS mixes criminal attacks with government-focused and-funded attacks. CFR limits its data to state-sponsored actors, for both accuracy and purpose of its dataset.
10. Carnegie Endowment for International Peace, "Timeline of Cyber Incidents Involving Financial Institutions," 2022, <https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline>.
11. CSIS' criteria are "cyber-attacks on government agencies, defense and high-tech companies, or economic crimes with losses of more than a million dollars." CFR's criteria are "a database of the publicly known state-sponsored incidents that have occurred since 2005." Moreover, "The tracker only contains data in which the perpetrator, also known as the threat actor, is suspected to be affiliated with a nation-state."
12. See the Correlates of War Project at <https://correlatesofwar.org>. Singer, J. David. "Correlates of War." *New York* (1979). [Vol. 1 is 1979 and Vol 2. 1980]
13. Valeriano, Brandon, and Ryan C. Maness, "How we stopped worrying about cyber doom and started collecting data." *Politics and Governance* 6, no. 2 (2018): 49-60.
14. Klein, James P., Gary Goertz, and Paul F. Diehl. "The new rivalry dataset: Procedures and patterns." *Journal of Peace Research* 43, no. 3 (2006): 331-348, and Thompson, William R., "Identifying rivals and rivalries in world politics." *International Studies Quarterly* 45, no. 4 (2001): 557-586.
15. Carlson, Brian, "Top Cybersecurity Statistics, Trends, and Facts," CSO, October 7, 2021, <https://www.csoonline.com/article/3634869/top-cybersecurity-statistics-trends-and-facts.html>.
16. See Lawfare, Topics: Cybersecurity at <https://www.lawfareblog.com/topic/cybersecurity> and Texas National Security Review, Topics Cyber at: <https://tnsr.org/search/cyber/>.
17. For more details about the MITRE ATT&CK methodology, see <https://attack.mitre.org/>.
18. Palmer, Glenn, Roseanne W. McManus, Vito D'Orazio, Michael R. Kenwick, Mikaela Karstens, Chase Bloch, Nick Dietrich, Kayla Kahn, Kellan Ritter, and Michael J. Soules, "The MID5 Dataset, 2011-2014: Procedures, coding rules, and description." *Conflict Management and Peace Science* (2021): <https://doi.org/10.1177/073889422199574>.
19. DCID 1.5, <https://drryanmaness.wixsite.com/cyberconflict/cyber-conflict-dataset>.
20. National Institute of Standards and Technology, "Critical Infrastructure Resources," December 8, 2021, <https://www.nist.gov/cyberframework/critical-infrastructure-resources>.

NOTES

21. Palmer, Glenn, Vito D'Orazio, Michael R. Kenwick, and Roseanne W. McManus, "Updating the militarized interstate dispute data: A response to Gibler, Miller, and Little." *International Studies Quarterly* 64, no. 2 (2020): 469-475. Brecher, Michael, Jonathan Wilkenfeld, Kyle Beardsley, Patrick James, and David Quinn (2021). *International Crisis Behavior Data Codebook*, Version 14. <http://sites.duke.edu/icbdata/data-collections/>.
22. Montgomery, M., B. Jensen, E. D. Borghard, J. Costello, V. Cornfeld, C. Simpson, and B. Valeriano, *Cyberspace Solarium Commission Report*. (2020), Washington, DC. <https://www.solarium.gov/report>, Valeriano, Brandon and Benjamin Jensen "Building a National Cyber Strategy: The Process and Implications of the Cyberspace Solarium Commission" in T. Jančárková, L. Lindström, G. Visky, P. Zotz (eds.) *Going Viral* (Report: 2021, 13th International Conference on Cyber Conflict 2021, NATO CCDCOE Publications, Tallinn, Estonia).
23. Uchill, Joe, "Breach Reporting Requirement Sputters as House Passes NDAA," December 8, 2021, <https://www.scmagazine.com/analysis/breach/breach-reporting-requirement-sputters-as-house-passes-ndaa>.
24. Borghard, Erica D., and Shawn W. Loneran, "The logic of coercion in cyberspace." *Security Studies* 26, no. 3 (2017): 452-481. Borghard, Erica D., and Shawn W. Loneran, "Cyber operations as imperfect tools of escalation." *Strategic Studies Quarterly* 13, no. 3 (2019): 122-145. Kreps, Sarah, and Jacquelyn Schneider, "Escalation firebreaks in the cyber, conventional, and nuclear domains: moving beyond effects-based logics." *Journal of Cybersecurity* 5, no. 1 (2019): tyz007. Healey, Jason, "The implications of persistent (and permanent) engagement in cyberspace." *Journal of Cybersecurity* 5, no. 1 (2019): tyz008, Brantly, Aaron F., ed. *The Cyber Deterrence Problem*. Rowman & Littlefield Publishers, 2020.
25. For more information, please see <https://vsfs.state.gov/>.
26. Valeriano, Brandon, Benjamin M. Jensen, and Ryan C. Maness, *Cyber strategy: The evolving character of power and coercion*. Oxford University Press, 2018.
27. Healey, Jason, "Beyond Attribution: Seeking National Responsibility in Cyberspace," Atlantic Council, February 22, 2012, <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/beyond-attribution-seeking-national-responsibility-in-cyberspace/>.
28. Maness, Ryan C., Brandon Valeriano, and Benjamin Jensen, "The Dyadic Cyber Incident and Dispute Dataset (DCID) Version 1.5", Codebook, 2019: <https://drryanmaness.wixsite.com/cyberconflict/cyber-conflict-dataset>.
29. National Institute of Standards and Technology, "Critical Infrastructure Resources," December 8, 2021, <https://www.nist.gov/cyberframework/critical-infrastructure-resources>.
30. Whyte, Christopher, Brandon Valeriano, Benjamin Jensen, and Ryan Maness. "Rethinking the data wheel: Automating open-access, public data on cyber conflict." In *10th International Conference on Cyber Conflict (CyCon)*, 9-30. IEEE, 2018.
31. Cornell Law School, "44 U.S. Code § 3552- Definitions," <https://www.law.cornell.edu/uscode/text/44/3552>.
32. CFR uses the term "operation," while CSIS uses the term "incident."
33. Cornell Law School, "44 U.S. Code § 3552 - Definitions," <https://www.law.cornell.edu/uscode/text/44/3552>.
34. Wolff, Josephine, "Why We Need to Be Much More Careful About How We Use the Word *Cyberattack*," *Slate*, March 30, 2017, accessed February 8, 2022, <https://slate.com/technology/2017/03/we-should-be-careful-when-we-use-the-word-cyberattack.html>
35. Trapdoors or Trojans are unauthorized software added to a program to allow entry into a victim's network or software program to permit future access to a site once it has been initially attacked. The purpose of trapdoors is to steal sensitive information from secured sites.
36. (1) Logic bombs, or wiper malware, are programs that cause a system or network to shut down and/or erase all data within that system or network. (2) Viruses are programs which attach themselves to existing programs in a network and replicate themselves with the intention of corrupting or modifying files. (3) Worms are essentially the same as viruses, except they do not need to attach themselves to existing programs. (4) Keystroke logging is the process of tracking the keys being used on a computer so that the input can be replicated in order for a hacker to infiltrate secure parts of a network.
37. Foote, Colin, Ryan Maness, Benjamin Jensen, and Brandon Valeriano, "Cyber conflict at the intersection of information operations: Cyber-enabled information operations, 2000-2016," in *Information Warfare in the Age of Cyber Conflict* (Routledge, 2020), 54-69.
38. Valeriano et al., 2018, *Cyber Strategy*.
39. For detailed information on the DCID severity scale and events coded 7-10, see Maness, Ryan C., Brandon Valeriano, Kathryn Hedgecock, Jose M. Macias, and Benjamin Jensen, "The Dyadic Cyber Incident and Campaign Dataset, version 2.1, *Codebook*, 2022, <https://drryanmaness.wixsite.com/cyberconflict/cyber-conflict-dataset>.

NOTES

40. Rid, Thomas, and Ben Buchanan, "Attributing cyber-attacks." *Journal of Strategic Studies* 38, no. 1-2 (2015): 4-37.
41. See 16 critical infrastructure sectors at <https://www.cisa.gov/critical-infrastructure-sectors>.
42. For a complete breakdown of CI please see Maness et al., 2022.
43. In multiple locations the authors previously have discussed the limitations of coding cyber incidents in the public knowledge and have pointed the reasons why this is possible despite assumptions to the contrary. Due mainly to the importance of the topic, the awareness of the news media, and the rush to provide information to trumpet the ability of cybersecurity incident response firms, much information is available on cyber operations despite most being covert operations.
44. Valeriano et al., 2018, *Cyber Strategy*.
45. Valeriano et al., 2018, *Cyber Strategy*.
46. Department of Defense, DoD Cyber Strategy 2018, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.
47. Here we summarize severity level six, "Single/multiple critical network infiltration and widespread destruction" from our codebook as strategic sabotage.
48. Valeriano, Brandon, and Ryan C. Maness. *Cyber war versus cyber realities: Cyber conflict in the international system*. Oxford University Press, USA, 2015.
49. DiMaggio, John, "A History of REvil," *Analyst 1*, 2022, <https://analyst1.com/file-assets/History-of-REvil.pdf>
50. McAfee, "What is Petya and NotPetya Ransomware?" 2017, <https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/petya.html>.
51. BBC News, "North Korea hackers stole \$400m of cryptocurrency in 2021, report says," [bbc.com](https://www.bbc.com/news/business-59990477#:~:text=Separately%2C%20in%20February%20last%20year,the%20Department%20of%20Justice%20said), January 14, 2022, available at <https://www.bbc.com/news/business-59990477#:~:text=Separately%2C%20in%20February%20last%20year,the%20Department%20of%20Justice%20said>.
52. Berr, Jonathan, "'WannaCry' ransomware attack losses could reach \$4 billion," *CBS News*, May 16, 2017, available at <https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/>.
53. See, for example, Katzman, Kenneth, "Iran Sanctions (RS20871)," Congressional Research Service, 2022, <https://crsreports.congress.gov/product/details?prodcode=RS20871>.
54. U.S. Department of Treasury, "Consolidated Sanctions List (Non-SDN lists)," December 16, 2021, <https://home.treasury.gov/policy-issues/financial-sanctions/consolidated-sanctions-list-non-sdn-lists>.
55. Felbermayr, Gabriel, Aleksandra Kirilakha, Constantinos Syropoulos, Erdal Yalcin, and Yoto V. Yotov, "The global sanctions data base." *European Economic Review* 129 (2020): 103561.
56. Maness, Ryan C., and Brandon Valeriano, "The impact of cyber conflict on international interactions." *Armed Forces & Society* 42, no. 2 (2016): 301-323, Valeriano et al., 2018, *Cyber Strategy*.

Synthetic Environments for the Cyber Domain: A Survey on Advances, Gaps, and Opportunities

Emily Nack

Lieutenant Colonel Nathaniel D. Bastian, Ph.D.

ABSTRACT

The need to understand cyber vulnerabilities and information in real time is imperative and often mission-critical in battlefield scenarios. As technologies continue to evolve, a need arises for more time-efficient and effective solutions within the cyber domain. With the growing popularity of synthetic environment technologies such as Augmented Reality (AR), Virtual Reality (VR), and Mixed Reality (MR) in a variety of fields, the question emerges: How can applications of this technology be applied to the field of cyber and what impact can they have? In this article, we survey the body of knowledge, both theoretical and empirical, of existing works exploring AR, VR, and MR technologies as solutions to common cyber challenges, as well as discuss the advances, gaps, and opportunities of this technology within the cyber domain.

CYBER APPLICATIONS OF SYNTHETIC ENVIRONMENTS

Synthetic environment technologies such as AR, VR, and MR allow users to experience a different reality, either by enhancing their perception of the real world (AR), creating a completely artificial environment (VR), or by combining elements of both (MR). These technologies have been used in various fields, including education, gaming, and healthcare, and have recently been adopted in the field of cybersecurity. We provide an overview of AR, VR, and MR in the cyber domain, highlighting the relevant technologies and their current applications within the field.

In Cybersecurity Training and Operations

AR, VR, and MR technologies have been increasingly used in cybersecurity training and operations due to their ability to provide analysts with realistic, immersive, and interactive environments.

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



Emily Nack is an Information Technology Specialist serving within the Data and Decision Sciences Division at the Army Cyber Institute (ACI) within the Department of Electrical Engineering and Computer Science at the United States Military Academy at West Point. She also serves as Research Lab Manager where she provides research and engineering technical support and systems management across the ACI's Intelligent Cyber-Systems and Analytics Research Lab, ACI's Internet of Things Research Lab, and ACI's Cyber Modeling and Simulation Research Lab. She holds an A.S. degree in Computer Information Systems from Hudson Valley Community College, along with a B.S. degree in Game Design and Development from the Rochester Institute of Technology.

AR technology has been utilized to enhance learners' understanding of complex cybersecurity concepts and scenarios by providing interactive visualizations of cyber threats and countermeasures. For instance, the use of AR technology, specifically Microsoft's HoloLens, was explored to aid human operators with computer network operations tasks.¹ Multiple applications were developed to demonstrate alternative approaches to network security operations by simulating environments and events that closely align with the daily tasks of operators. The AR-based cybersecurity training applications enabled users to visualize and interact with virtual cyber attacks and defense mechanisms in a real-world environment. This approach provided users with a visual representation of the threat landscape, enabling more engaging and interactive learning environments, and preparing users to make informed security decisions in the event of a real attack.

Both VR and MR technology have been used to create realistic and immersive simulations that allow users to practice defending against cyber attacks in a safe and controlled environment. The use of VR and MR to support defensive cyber operations and training was discussed, as researchers reviewed new capabilities being developed and theorized by the U.S. Army C5ISR Center Cybersecurity Service Provider (CSSP).² Several combined VR and MR environments were developed to facilitate collaboration between analysts and provide the virtual real estate needed to monitor cyberspace effectively. The Visual Intrusion Detection System (VIDS) was developed to visualize Intrusion Detection System (IDS) alerts in a three-dimensional (3D) space, allowing cybersecurity analysts to view, categorize, and find correlations between alerts quickly.³ This provides analysts with the necessary visualizations to detect and defend efficiently against incoming cyber attacks.



LTC Nathaniel D. Bastian, Ph.D., is an Academy Professor and Cyber Warfare officer at the United States Military Academy at West Point. He serves as Division Chief, Data and Decision Sciences and Senior Research Scientist at the Army Cyber Institute (ACI) within the Department of Electrical Engineering and Computer Science, as well as Assistant Professor of Operations Research and Data Science with a dual faculty appointment in the Department of Systems Engineering and the Department of Mathematical Sciences. He also serves as the ACI's Chief Data Scientist, directing the ACI's Intelligent Cyber-Systems and Analytics Research Lab, Internet of Things Research Lab, Cyber Modeling and Simulation Research Lab, and Cognitive Security Research Lab. He has co-authored 90+ refereed publications, received \$4M+ in externally-funded research monies, served as Visiting Research Fellow at the Johns Hopkins University Applied Physics Lab, and served as Distinguished Visiting Professor at the National Security Agency.

To summarize, AR, VR, and MR technologies have been increasingly used in cybersecurity training and operations to provide users with realistic, immersive, and interactive learning experiences. These technologies enable users to practice their cybersecurity skills in a safe and controlled environment and enhance their understanding of complex cybersecurity concepts and scenarios.

Network Security Monitoring and Data Visualizations

AR, VR, and MR technologies are changing the field of network security monitoring and data visualization by making it easier and more efficient to analyze security threats. These technologies offer new ways to visualize and interact with complex data, allowing analysts to identify potential security risks quickly.

AR technology enables visualizations of network traffic and security events. One developed application is a 3D network visualizer that displays network topologies from both a global and local perspective.¹ Users are prompted with randomly generated alerts that simulate emergent problems requiring attention. When users interact with alerts, a local network topology is imported and dynamically generated, including routers, switches, and computers represented as 3D objects interconnected via links. As the HoloLens enables eye-tracking, users can glance over the topology, with individual objects and links highlighted when observed. Interacting with objects reveals mockups of different network diagnostic windows, emulating actions that cybersecurity analysts take when visualizing data and monitoring security risks. This environment provides analysts with a more intuitive and interactive view of the network and can help identify network traffic anomalies and respond to potential security threats.

VR technology can create immersive environments for network and data visualization. With VR, users can explore data and network structures in a 3D space, allowing for more intuitive interaction with the information. VRNetzer is an interactive data exploration platform that facilitates the visualization and analysis of large-scale, complex data, allowing users to gain a deeper understanding of the information presented.⁴ Although not designed with cybersecurity in mind, VRNetzer's functionality is powerful and can enable analysts to parse through complex data and identify cyber vulnerabilities efficiently.

MR technology combines aspects of AR and VR technologies, providing a more immersive and interactive environment for data visualization. Researchers explored the use of MR as an improved approach to visualizing big data.⁵ By using MR for visualization, access to large amounts of data is convenient and can provide a view from multiple perspectives, allowing for smooth navigation and minimal perceptual inaccuracies in data analysis. Such visualization provides the necessary infrastructure to improve network security monitoring and reduce the time it takes to understand fully the complexity of cybersecurity data.

Overall, AR, VR, and MR technologies are revolutionizing the way security professionals visualize and analyze network data. These technologies provide increasingly sophisticated tools for identifying and mitigating security threats, improving analysts' workflow and reducing response times. As these technologies continue to evolve, they will play a significant role in network security monitoring and data visualization.

Cyber Incident Response and Situational Awareness

AR, VR, and MR technologies can enhance situational awareness and improve decision-making in cyber incident response. By providing analysts with a more comprehensive and immersive view of the cyber threat landscape, these technologies can enable faster and more effective threat detection and response.

AR technology can offer real-time information overlays, including alerts and threat information, improving situational awareness and enabling faster response times. For instance, researchers proposed an Augmented Reality-based framework that uses AR to present data, make forecasts, conduct analyses, and support decision-making.⁶ This framework can help cybersecurity specialists in high-performance computing (HPC) environments combat the increasing cyber-physical threats that HPC data centers with heterogeneous compute servers and networks face. The framework sends notifications to an AR device to alert analysts of any hardware issues, and a navigation tool helps locate the damaged device. Once located, a 3D visualization tool can reveal the issue and, in the future, detailed animations can demonstrate how to fix the detected issues. Using AR to provide a visual representation of cyber infrastructure helps analysts understand the scope and impact of threats to physical systems.

VR and MR technology can provide a 3D visualization of the cyber environment, allowing incident responders to see attack surfaces and understand potential attack vectors in a more

immersive way. It can also help with post-incident analysis by recreating cyber incidents, allowing responders to identify the root cause, determine the scope of the attack, and develop strategies to prevent similar incidents in the future. For instance, this was explored in the Vids Cyber Defense Visualization Project, which is an interactive 3D environment for visualizing network Intrusion Detection System (IDS) data.³ Vids builds upon an earlier visualization project, called VIDS,² which focused solely on visualizing IDS alerts in a 3D space. Vids is currently implemented as a 2D representation of a 3D space, allowing the platform to be used for testing and visualization concepts and gathering feedback from users. In the long term, the platform is intended to integrate with a VR or MR environment. Vids has several uses that enable cyber incident response and situational awareness, including providing a visual reference model to explain events or incidents, identifying “known unknowns” or “unknown unknowns” through multidimensional analysis, and enabling collaboration among multiple parties involved in different stages of research, development, or user chains.

Leveraging the power of AR, VR, and MR technologies in cyber incident response and situational awareness empowers organizations to not only stay ahead of evolving cyber threats, but also enhance their overall cybersecurity posture. By integrating these technologies into their strategies, organizations can significantly mitigate the impact of cyber attacks and protect critical assets and information from sophisticated adversaries. The immersive and comprehensive view provided by AR, VR, and MR enables analysts to make faster and more informed decisions, detect threats more effectively, and respond with greater agility.

GAPS, OPPORTUNITIES, AND CURRENT EFFORTS

The use of AR, VR, and MR technologies in the cyber domain has the potential to improve cyber defense significantly by enhancing situational awareness, enabling effective training, and improving incident response accuracy and speed. However, there are still significant gaps in understanding how to fully leverage these technologies for cybersecurity. This section will explore new opportunities for utilizing AR, VR, and MR to address cybersecurity challenges and bridge these gaps. Specifically, it will focus on utilizing these technologies to further enhance cybersecurity training, network visualization, and situational awareness. By highlighting these new opportunities, this section aims to provide insights into how these technologies can effectively address the evolving challenges presented within the cyber domain.

Serious Games for Improved Cybersecurity Training and Awareness

The combination of AR technology and serious games offers numerous opportunities for cybersecurity training and awareness. One of the key advantages of leveraging this technology is the ability to provide hands-on training experiences that simulate real-world cyber threats and attack scenarios, enabling users to develop practical skills and a deeper understanding

of cybersecurity concepts. A good example is the “CybAR” game,⁷ which creates a virtual training environment where users can experience the consequences of careless cybersecurity habits and learn how to defend against them. Additionally, the gamification of cybersecurity training can make it more engaging and enjoyable for learners, promoting the retention of information and development of critical thinking and problem-solving skills. “CybAR” was designed as a competitive game, utilizing gamification elements such as point systems, leader boards, and achievements to motivate players to continue playing and increase their awareness of cybersecurity practices.

Furthermore, AR technology can create more immersive and realistic training environments, increasing motivation and interest in the field. While the “Red vs Blue, Cyber-security Simulator” game⁸ does not utilize AR, the implementation of the technology could enhance realism and facilitate remote collaboration and teamwork among players. The game splits players into three teams (White, Red, and Blue), which must work together to strategize cyber attacks and defenses, promoting decision-making at the operational cybersecurity level.

AR and serious games can also be used to raise awareness about cyber threats and best practices for cybersecurity, educating employees and the general public about the importance of cybersecurity and how to protect against cyber attacks. “Riskio” is a good example, providing an active learning environment where players build knowledge on cybersecurity attacks and defenses by playing the roles of both attacker and defender of critical assets in a fictitious organization, raising awareness about cybersecurity threats and mitigation tactics.⁹

Overall, the combination of AR and serious games has exciting potential for improving cybersecurity training and awareness. Future research can further explore the impact of this technology on cybersecurity education and its potential for providing high-quality and scalable cybersecurity training and awareness programs.

Real-Time Network Visualization Using Mixed Reality

With today’s constantly evolving threat landscape, real-time network visualization plays a critical role in responding to emerging threats and preventing catastrophic data breaches. However, despite the potential benefits of using MR technology for real time network visualization in cybersecurity, there are currently few applications that exist. This may be due to the challenges of implementing MR and displaying large amounts of data in real-time. As this technology continues to advance, approaches and potential opportunities for using MR can be explored.

One proposed approach to using MR for visualizing real-time data for cyber situational awareness was discussed, as authors developed a prototype for displaying network data as a holographic overlay on physical network devices.¹⁰ In their proposed model, live data was

indexed in real time using IDS, Security Incident Event Message (SIEM), and Unified Threat Management (UTM) to detect threats. A Simultaneous Localization and Mapping (SLAM) algorithm was then used to map the environment, and unique tags with MAC addresses were placed on machines to identify their physical locations when a threat was detected. The model utilized Microsoft HoloLens to identify suspicious activities and guide the user to their location, where information was augmented on the device using surface detection. This prototype demonstrated the potential of MR for real-time network visualization and highlighted the benefits of displaying network data in a more intuitive and immersive way.

Two use cases that demonstrate the benefits of using MR technology for visualizing real-time Internet of Things (IoT) data were proposed.¹¹ The first use case was for smart cities where IoT devices collected real-time data on temperature, humidity, and noise throughout the city. The data was then filtered, aggregated, and visualized on a 3D map of the city using MR technology. The second use case was for cybersecurity, in which an MR application was used to filter incoming real-time data based on Indicators of Compromise (IOC) and to visualize the propagation of malware among infected devices during a cyber attack. Both of these use cases highlighted the advantages of using MR to visualize real-time IoT data, including faster and more intuitive data analysis, improved decision-making, and better communication between users.

While these opportunities demonstrate the potential of MR for real-time network visualization in cybersecurity, there is still much work to be done to realize fully the potential of this technology. Further research is needed to explore the effectiveness of MR-based network visualizers in real-world cybersecurity scenarios and to address the challenges of displaying large amounts of data in real time. However, with the increasing need for real-time network monitoring and the continued advancements in MR technology, it is likely that MR-based network visualizers will become an important tool for cybersecurity professionals in the future.

Visualizing Geospatial Data with Augmented Reality

AR technology has the potential to be a powerful tool for visualizing geospatial data in the field of cybersecurity. By using AR, cybersecurity professionals can quickly and accurately understand the location of threats and their potential impact, allowing them to take faster and more effective actions.

One potential application of AR for geospatial data visualization is in the visualization of cyber threats and attacks in real time, overlaid on a map. This idea was minimally explored with the 3D Network Visualizer app, which mapped network topologies at the global view, displaying interconnected nodes and edges atop a 3D globe. By using gesture-based input capabilities, users could scale and rotate the globe, while random nodes were selected from

the network topology to simulate emergent alerts. When further inspected by the user, the local network view for the affected node would be displayed, allowing users to understand and respond to the alert. This functionality coupled with real-time geospatial data could help cybersecurity professionals identify the location of attacks and their potential impact on critical infrastructure, enabling faster and more effective response.

To enhance situational awareness in both physical and cyber spaces, AR can be used to create immersive experiences that visualize geospatial data. This can be especially important in critical infrastructure and other areas where visualizing the location of threats and their potential impact is crucial. As an example, a cybersecurity team could use AR to display real-time data on the physical location of devices on a network, along with their status and vulnerabilities. This concept was discussed in various studies, where authors described unique frameworks for visualizing geospatial data in both operational and defensive settings.^{6,10,12} By utilizing AR technology to create immersive experiences that visualize geospatial data, cybersecurity professionals can gain a better understanding of the physical locations and status of threats in real time, allowing them to take faster and more effective actions.

Overall, the integration of AR with geographical data presents a range of opportunities for improving cybersecurity, from real-time threat visualization to enhanced situational awareness and training. As the technology continues to advance, it will be interesting to see how these opportunities are further developed and applied in real-world contexts.

Digital Twin Technology with AR for Increased Cyber Situational Awareness

Digital twin technology and AR offer significant opportunities to enhance cyber situational awareness. Digital twins are virtual representations of physical objects or systems that can simulate their behavior and performance in real time. This enables predictive analytics, remote monitoring, and maintenance.¹³ AR can provide a visual overlay of digital twin data onto the physical world, allowing for more intuitive and interactive access to information. Combining these two technologies provides cybersecurity professionals with a comprehensive understanding of cyber threats, empowering them to take faster and more effective actions.

One potential application of digital twin technology and AR for cyber situational awareness is in visualizing cyber-physical systems (CPS) and IoT devices.¹³ These systems and devices are increasingly prevalent in critical infrastructure, and cybersecurity professionals need to understand their behavior and vulnerabilities to protect against cyber threats. Digital twins offer a key advantage: users can analyze the environment based on geography, sensing, and timing to identify vulnerabilities in tactical operations.¹⁴ For example, users can evaluate the effectiveness of observation posts in detecting targets or explore multiple phenomena, including physical, cyber, and human behavioral effects. These analyses can help users target specific areas of concern and minimize overall system costs.

By creating a digital twin of CPS and IoT devices, cybersecurity professionals can simulate their behavior and monitor for anomalies in real time. AR can then overlay this data onto the physical world, providing a visual representation of the CPS or IoT device and its status. This enables cybersecurity professionals to identify potential threats quickly and respond accordingly. AR can also be dynamic, adaptive, and persistent, and can be used to signal the presence of sensors that are not apparent or in low-visibility areas, indicate positions of critical resources or assets, suggest defensive positions, and identify and label enemy forces for training and testing purposes.¹⁴

The integration of digital twin technology and AR offers a promising avenue for improving cyber situational awareness. With the ability to represent physical systems virtually and overlay critical cybersecurity information onto the real world, cybersecurity professionals can more effectively understand and respond to potential threats. As these technologies continue to evolve, it will be exciting to see how they are further leveraged in practical contexts to enhance cybersecurity and protect against emerging threats.

Novel Approaches to Addressing Research Gaps and Opportunities

As we researched current applications and the advances/gaps in using AR, VR, and MR technologies within the cyber domain, it quickly became apparent that there were limited tangible solutions which exist for real-time network visualization and threat detection and mitigation. Here we discuss the work we have done in developing a real-time network visualizer using AR technology. Our research aims to address the gaps and opportunities presented earlier in this article, particularly exploring real-time network and geospatial data visualization. Traditional network visualizations often involve 2D static representations that can be challenging for users to interpret in real time. Our work uses AR technology to create an interactive and dynamic visual representation of network data. By leveraging the capabilities of AR, our visualizer allows users to experience network data in a more intuitive and engaging way, enabling interaction with data and exploration of network relationships in real time.

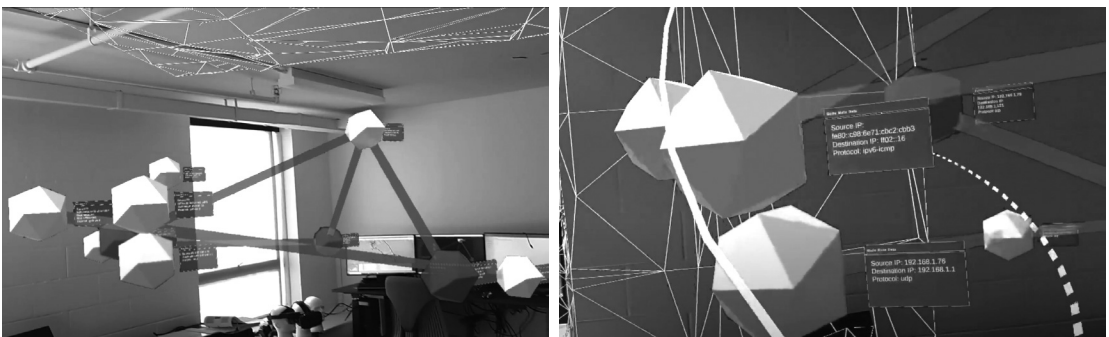


Figure 1: Real-Time AR Network Visualizer

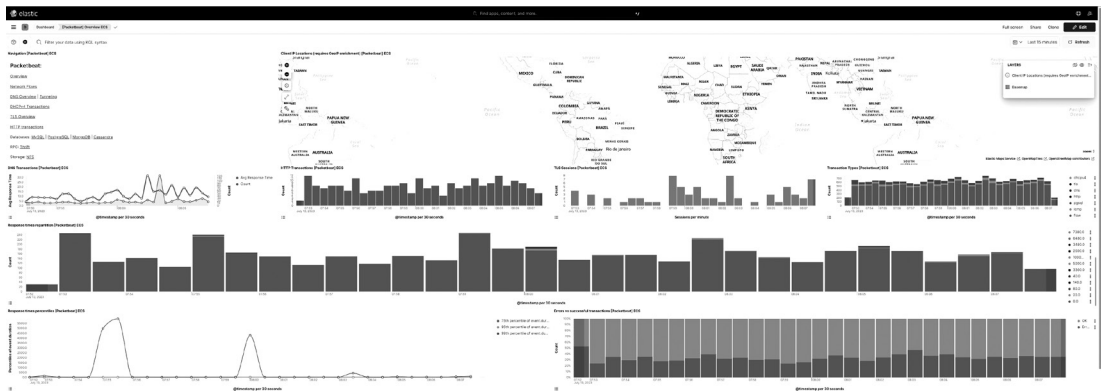


Figure 2: Packetbeat Dashboard in Kibana Visualizing Real-Time Network Data

Our network visualizer, as seen in Figure 1, was developed in Unity and uses data collected from Elasticsearch's Packetbeat,¹⁵ pictured in Figure 2, to create game objects dynamically in real time that represent source and destination IPs as nodes and their communication via edges. As data is updated, the game objects are updated with new information, reconnecting source nodes to their appropriate destinations and recoloring game objects based on protocol. As of now, the visualizer creates the game objects at random positions within the room, spatially mapped using Microsoft HoloLens' built-in capabilities and Microsoft's Mixed Reality Toolkit¹⁶ to update the mapping in Unity in real time. This allows game objects to be properly scaled within the room space and allows for physics-based collision using object detection.

In the future, we plan to use geospatial data to map the game objects based on location. With Elasticsearch's Packetbeat, location data can be collected, which presumably means we should be able to extract geospatial data and assign it to game objects in the same way we do for network data. We also plan to use our visualizer for threat detection and mitigation by generating alerts and highlighting anomalous nodes for the user to explore further. We can leverage security tools like Suricata,¹⁷ which can be configured to send intrusion detection data to Elasticsearch and write custom scripts to access and store the data within Unity. Alerts can be generated and visualized based on the signature-based rules Suricata offers, and users can drill down into suspect nodes, potentially performing actions to mitigate threats directly from the AR visualizer.

There is still much work to be done to help address the gaps of using AR for real-time data visualization and threat detection and mitigation in the cyber domain, but with our research we have proved that it can be done. The future work planned for the visualizer, including the integration of geospatial data and the generation of alerts and highlighting of anomalous nodes, demonstrates the potential for continued advancements in AR technology for cybersecurity. By leveraging AR technology, real-time data visualization and threat detection in

the cyber domain can become more accessible and intuitive, leading to more effective cybersecurity practices. Furthermore, the use of Elasticsearch's Packetbeat and security tools like Suricata highlights the potential for integrating existing cybersecurity tools with AR technology for real-time threat detection and mitigation. This integration can provide a more comprehensive approach to cybersecurity and help identify and address threats in a timely and effective manner. Our work contributes to the advancement of AR technology in cybersecurity and provides a foundation for further research and development in this field.

CONCLUSIONS AND FUTURE WORK

As technology continues to advance, new tools and techniques have emerged to improve our ability to combat cyber threats. One area of development in this field is the use of synthetic environment technologies like AR, VR, and MR in cybersecurity. While these technologies have the potential to transform how we approach cyber defense by enhancing situational awareness, enabling more effective training and improving the accuracy and speed of incident response, there are still gaps in our understanding of how best to apply them to this field. This article explored the current state of research in this area and has identified both the gaps associated with AR, VR, and MR in the cyber domain and new opportunities for how this technology can enhance the field.

To leverage these technologies fully, future work should focus on exploring innovative ways to integrate them into existing cybersecurity workflows. This may involve developing new software and hardware solutions that are specifically designed for cyber defense, as well as incorporating existing AR, VR, and MR technologies into current cybersecurity training and simulation programs. Additionally, it is important to continue exploring the potential of these technologies for threat hunting, incident response, and other key areas of cyber defense. By staying up to date with the latest advancements in AR, VR, and MR technology, we can unlock the full potential of these technologies to better protect our digital assets and critical infrastructure.🔒

NOTES

1. Beitzel, Steve, Josiah Dykstra, Paul Toliver, and Jason Youzwak. "Exploring 3d Cybersecurity Visualization with the Microsoft HoloLens." In International Conference on Applied Human Factors and Ergonomics, 197-207. Springer, 2017.
2. Kullman, Kaur, Matt Ryan, and Lee Trossbach. "VR/MR Supporting the Future of Defensive Cyber Operations." IFAC-PapersOnLine 52, no. 19 (2019): 181-86.
3. Edwards, Joshua, and Gregory Shearer. "Vids Cyber Defense Visualization Project." In Vids Cyber Defense Visualization Project. ICF, 2020.
4. Pirch, Sebastian, Felix Müller, Eugenia Iofinova, Julia Pazmandi, Christiane V. R. Hütter, Martin Chietini, Celine Sin, et al. "The VRNetzer Platform Enables Interactive Network Analysis in Virtual Reality." *Nature Communications* 12, no. 1 (2021): 1-14.
5. Olshannikova, Ekaterina, Aleksandr Ometov, Yevgeni Koucheryavy, and Thomas Olsson. "Visualizing Big Data with Augmented and Virtual Reality: Challenges and Research Agenda." *Journal of Big Data* 2, no. 1 (2015): 1-27.
6. Sukhija, Nitin, Cory Haser, and Elizabeth Bautista. "Employing Augmented Reality for Cybersecurity Operations in High Performance Computing Environments." In Proceedings of the Practice and Experience in Advanced Research Computing on Rise of the Machines (Learning), 1-4, 2019.
7. Alqahtani, Hamed, and Manolya Kavakli-Thorne. "Design and Evaluation of an Augmented Reality Game for Cybersecurity Awareness (CybAR)." *Information* 11, no. 2 (2020): 121.
8. Yamin, Muhammad Mudassar, Basel Katt, and Mariusz Nowostawski. "Serious Games as a Tool to Model Attack and Defense Scenarios for Cyber-Security Exercises." *Computers & Security* 110 (2021), 102450 .
9. Hart, Stephen, Andrea Margheri, Federica Paci, and Vladimiro Sassone. "Riskio: A Serious Game for Cyber Security Awareness and Education." *Computers & Security* 95 (2020), 101827 .
10. Joshi, Tapas Dipakkumar. "A Mixed-Reality Approach for Cyber-Situation Awareness." Florida Tech, 2017.
11. Andrade, Tiago, and Daniel Bastos. "Extended Reality in Iot Scenarios: Concepts, Applications and Future Trends." In 5th Experiment International Conference (Exp. at'19), 107 -12. IEEE, 2019.
12. Kammerer, Klaus, Rüdiger Pryss, Kevin Sommer, and Manfred Reichert. "Towards Context-Aware Process Guidance in Cyber-Physical Systems with Augmented Reality." In 4th International Workshop on Requirements Engineering for Self-Adaptive, Collaborative, and Cyber Physical Systems (RESACS), 44-51. IEEE, 2018 .
13. Böhm, Fabian, Marietheres Dietz, Tobias Preindl, and Günther Pernul. "Augmented Reality and the Digital Twin: State-of-the-Art and Perspectives for Cybersecurity." *Journal of Cybersecurity and Privacy* 1, no. 3 (2021): 519-38.
14. Raybourn, Elaine M., and Ray Trechter. "Applying Model-Based Situational Awareness and Augmented Reality to Next-Generation Physical Security Systems." In *Cyber-Physical Systems Security*, 331-44. Springer, 2018.
15. Elasticsearch. "Packetbeat: Network Analytics Using Elasticsearch," 2023. <https://www.elastic.co/beats/packetbeat>.
16. Microsoft. "MRTK2-Unity Developer Documentation." 2022.
17. Suricata. "Suricata," n.d., <https://suricata.io/>.

Posturing U.S. Cyber Forces to Defend the Homeland

Colonel Jamel Neville

ABSTRACT

On March 21, 2022, the White House warned that Moscow is exploring options to attack US critical infrastructure in response to economic sanctions levied on Russia following its 2022 invasion of Ukraine. On May 25, 2023, the U.S. State Department issued a similar warning regarding Beijing's capabilities and intentions. As revisionist powers seek to disrupt the international order and cyber threats to critical infrastructure persist, the Department of Defense (DoD) must effectively position its cyber forces and capabilities to defend against cyber-attacks before they hit the homeland. An attack against the US power grid could result in multiple failures in life-sustaining infrastructure and significantly impact Joint Force power-projection capabilities. U.S. Northern Command (USNORTHCOM) must work closely with U.S. Cyber Command (USCYBERCOM) to orchestrate federal and non-federal stakeholders' cyber authorities, capabilities, and equities to posture DoD cyber forces to respond with speed and agility. However, the myriad of federal cyber laws, regulations, authorities, and public and private sector stakeholder equities could impede DoD's response efforts. National cybersecurity is "a team sport," but players tend to use different playbooks or play by different rules. Tools such as a DoD "Complex Catastrophe Cyber Stakeholders, Communications, Authorities, and Narratives" (C3 SCAN) framework could enable USNORTHCOM and USCYBERCOM to foster collaboration, validate plans and orders, enumerate and prioritize mission-relevant terrain in cyberspace, and ensure readiness for Defense Support to Cyber Incident Response (DSCIR).

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



Colonel Jamel Neville is the Marine Corps Cyberspace Warfare Group Commanding Officer. Previously, he served in various capacities throughout the U.S. Cyber Mission Force, including a joint force headquarters and joint task force director of operations (J3); cyber combat mission team and cyberwarfare task group commander; and deputy director for current operations (G33). Before becoming a cyberspace warfare officer in 2018, Col Neville served as a communications officer following his commissioning in 2000. He deployed to Operations ENDURING FREEDOM and FREEDOM'S SENTINEL and in response to defense support of civil authorities (DSCA). Col Neville also worked in the private sector as a defense consultant to The Joint Staff and Defense Threat Reduction Agency for several years. He has earned a Master's in strategic studies, a Master's in military studies, an MBA in information technology management, and a Bachelor's in fine arts. Col Neville is a certified information system security professional (CISSP).

POSTURING U.S. CYBER FORCES TO DEFEND THE HOMELAND

When a cyber-attack can deliver the same damage or consequences as a kinetic attack, it requires national leadership and close coordination of our collective resources, capabilities and authorities.

— *The President's National Infrastructure Advisory Council*¹

Enemy attacks resulting in infrastructure damage are not new. As war raged throughout the European and Asia-Pacific regions, adversaries penetrated and maneuvered throughout key United States East Coast supply chain nodes starting in January, which eventually resulted in the deaths of thousands of people over the following several months. In February, adversarial attacks against one Southern California oil refinery generated mass hysteria across the West Coast. Adversaries operated undetected throughout the spring despite shared threat intelligence and lessons from the United States' allied partner in the weeks and months preceding the initial attacks. During the February attack, electricity and electromagnetic spectrum outages across Los Angeles and San Diego stemmed from the inability of the U.S. military and local authorities to coordinate responses, which exacerbated the already chaotic and confusing situation that day. Due to the war overseas, the military committed the preponderance of its focus and effort to operations abroad, resulting in an inability to surge forces to counter adversaries' asymmetric attacks against the homeland. While new federal authorities enabled innovative public and private sector partnerships and capabilities to thwart the malicious activities, the impact on the Northeast fuel

supply chain forced nationwide gasoline rationing throughout the next two years because of Germany's Operation Drumbeat, launched on January 14, 1942.

INTRODUCTION

In the above vignette, German and Japanese submarine attacks against vulnerable targets along America's shorelines at the onset of World War II are an example of a complex catastrophe, which the federal government defines as:

Any natural or man-made incident, including cyberspace attack, power grid failure, and terrorism, which results in cascading failures of multiple, interdependent, critical, life-sustaining infrastructure sectors and causes extraordinary levels of mass casualties, damage or disruption severely affecting the population, environment, economy, public health, national morale, response efforts, and/or government functions.²

Operation Drumbeat illustrates how the U.S. was unprepared to counter the asymmetric attacks against merchant shipping across the East Coast by the Germans and the Santa Barbara Bankline Company aviation fuel storage farm by the Japanese, nor could it handle their non-kinetic effects.³ The ominous potential for increased attacks threatened to plummet national oil supplies to intolerable levels, harming American and Allied war efforts and resulting in the death of thousands of seamen and civilians.⁴ The grim outlook compelled greater unified action between the federal government, public, and private sector to detect and thwart the adversary.⁵

Though cyber-attacks on U.S. critical infrastructure may likely not produce the same devastating effects as German U-boats, America's fragmented and disorganized coastal defenses and delayed and unsynchronized military response actions in 1942 are worth some reflection.⁶ Today, sophisticated cyber actors have the potential to exploit information and communication systems vulnerabilities to establish undetected access and control of these systems and produce detrimental effects.

As the Russo-Ukrainian war continues, Moscow increases its aggression against the West, U.S.-China tensions over Taiwan and other issues increase, and the U.S. faces the threat of sophisticated cyber-attacks against its critical infrastructure. On March 21, 2022, the White House warned that Moscow is exploring options to attack U.S. critical infrastructure in response to economic sanctions on Russia following its full-scale invasion of Ukraine. On May 25, 2023, the U.S. State Department warned that Beijing could launch cyber-attacks against oil and gas pipelines and rail systems after Microsoft analysts identified the campaign, dubbed Volt Typhoon, "could disrupt critical communications infrastructure between the United States and Asia region during future crises."⁷

While the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) collaborates with organizations to protect U.S. critical infrastructure, their efforts are more passive.⁸ The Department of Defense (DoD) is ultimately responsible for posturing cyber forces for active defense against complex cyber-attacks by countering and blunting the offensive efforts of foreign adversaries. However, the myriad of federal cyber laws, regulations, and authorities; DoD inter- and intra-organizational relationships (e.g., interagency and intelligence community); and public and private stakeholder equities could hinder DoD's ability to prepare and respond with speed and agility in cyberspace.⁹ National cybersecurity is "a team sport," as fittingly described by the U.S. Cyber Command (USCYBERCOM) Commander and Director of the National Security Agency (NSA), General Paul Nakasone.¹⁰ Still, players on the same team may use different playbooks or play by different rules.

This article provides a methodology on how the DoD should team with CISA, the FBI, and other federal and non-federal stakeholders to counter, prevent, or minimize the impacts of large-scale cyber-attacks against US critical infrastructure networks. Russian aggression, geopolitical tensions, and future strategic threat assessments highlight the need for unified action in cyberspace. DoD – specifically, U.S. Northern Command (USNORTHCOM) and supporting cyber forces from USCYBERCOM – must understand the laws and policies that could affect (either hinder or enable) DoD cyber protection and offensive operations before, during, and after a complex cyber-attack against the homeland. While DoD cyber force and capability positioning are important planning factors, DoD's ability to effectively orchestrate stakeholders' cyber authorities, capabilities, and equities to protect against, prevent, mitigate, respond to, and recover from complex catastrophes of this scope and scale is paramount.¹¹

Background

In 2018, the then-USNORTHCOM Commander, General Terrance O'Shaughnessy, proclaimed that the U.S. homeland is no longer a sanctuary.¹² He aptly forecasted that cyber-attacks exploiting against personal, commercial, and government infrastructure vulnerabilities would continue to increase. During conflict, the United States should expect attacks against critical defense, government, and economic infrastructure.¹³ Some of the ways in which the US has sought to prepare for such attacks include: General O'Shaughnessy's proclamation, National Security Presidential Memorandum-13, "United States Cyber Operations Policy;" the work of the Cyberspace Solarium Commission, the White House's Executive Order on Improving the Nation's Cybersecurity, and National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems. These have all laid the foundational steps to reduce the likelihood and impact of significant consequences from cyber-attacks against critical infrastructure.¹⁴ They and other National cybersecurity policies and legislative reforms signify a notable shift by the federal government from the status quo.¹⁵

National Security Memorandum (NSM)-8, "Improving the Cybersecurity of National Security, Department of Defense and Intelligence Community Systems," released on January 19,

2022, is especially noteworthy. In essence, the memorandum makes Executive Order 14028 more effective.¹⁶ Specifically, the order calls for unity of effort and collaboration between the National Manager for National Security Systems (also the Director of NSA and Commander of USCYBERCOM) and the CISA Director.¹⁷ These new roles and responsibilities allow DoD to orchestrate cyber authorities, capabilities, and stakeholders' equities to best posture the Joint Force to detect, deter, and defeat malicious cyber-attacks targeting vulnerable critical infrastructure.¹⁸

Strategic Threat Assessment

Current assessments from the U.S. intelligence community indicate that peer adversaries seek to employ cyber warfare capabilities to degrade DoD networks, hold national infrastructure at risk, and delay and disrupt US ability to project forces globally.¹⁹ Joint Force power projection is both a critical military capability and critical vulnerability as more than 80% of U.S. critical infrastructure is owned and operated by the private sector.²⁰ And given the open and interdependent nature of the Internet, the U.S. and other democratic nations are more susceptible to cyber-attacks against critical infrastructure than countries with restrictive Internet systems.²¹ Due to these vulnerabilities and the capability of adversaries, these threats could result in significant damage across the United States, severely impacting national security.

Nation-states like Russia and China and non-state criminal actors can target and temporarily disrupt critical infrastructure with their existing cyber capabilities.²² For example, at midnight on December 23, 2015, the Russian threat actor, Sandworm, infiltrated and shut off a Ukrainian power grid, leaving over 225,000 people without power for six hours in temperatures near zero degrees Fahrenheit.²³ This attack is even more concerning after Sandworm targeted and infiltrated U.S. energy facilities in 2014 with the malware discovered in Ukraine's critical infrastructure cyber-attacks. It illustrates Russia's ability to assess capabilities on other critical infrastructures before utilizing them to meet strategic objectives.²⁴ On July 19, 2021, the U.S. Department of Justice (DOJ) indicted four Chinese cyber actors for their illicit computer network exploitation activities targeting victims in the defense industrial base, the federal government, manufacturing, maritime, and transportation sectors, amongst others.²⁵ DOJ also indicted three Russian officials on March 24, 2022, for their targeted hacking campaigns against U.S. energy sector computer hardware, software, and operational technology systems between 2012 and 2017.²⁶ These examples highlight Russia and China's intentions and cyberwarfare capabilities targeting U.S. critical infrastructure, enabling Moscow and Beijing to make effective defenses difficult to establish.²⁷

U.S. Power Grid and Implications of Complex Catastrophes

The continental United States (CONUS) consists of three power grids – Eastern Interconnection, Western Interconnection, and Electric Reliability Council of Texas (ERCOT), as depicted in Figure 1. Three components comprise power grids: generation, transmission, and distribution.

Generation consists of traditional power plants utilizing fossil fuels, renewable power sources, and energy storage equipment for variable power sources like wind power. Transmission is the long-distance power lines and the step-up and step-down substations to transform the power for long-distance travel. Distribution consists of the assets that deliver power to the customers, private and commercial, and managed privately in regulated states.

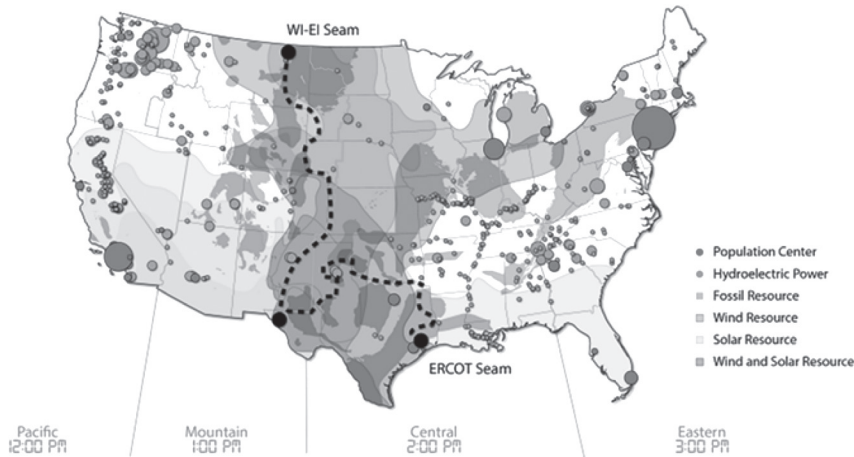


Figure 1. Continental United States' Three Power Grid Sectors²⁸

The 2013 Presidential Policy Directive-21, “Critical Infrastructure Security and Resilience,” identifies the energy sector as vital because it enables all critical infrastructure sectors.²⁹ Following a sophisticated cyber-attack, a catastrophic failure in one or more of the three grids could lead to significant casualties, especially in colder or hot climates. The hundreds of lives lost during the winter 2021 ERCOT power outage illustrate the potential impact of unmitigated power failure.³⁰

A shared understanding of DoD inter- and intra-organizational relationships, roles, responsibilities, and stakeholder equities would increase preparedness across the federal government, public, and private sector. Under joint doctrine, USNORTHCOM and U.S. Indo-Pacific Command (USINDOPACOM) are responsible for “defending against, mitigating, and defeating cyberspace threats.” However, only USCYBERCOM possesses the cyber expertise and intelligence apparatus to respond to such a crisis.³¹ In short, USNORTHCOM and USINDOPACOM are the supported commands, and USCYBERCOM is the supporting command in complex catastrophes in the homeland.³²

In 2012, Commander of USNORTHCOM, General Charles Jacoby, Jr., forecasted that USNORTHCOM’s role could be much broader than Defense Support of Civilian Authorities (DSCA) operations.³³ During a complex catastrophe in CONUS, USNORTHCOM would likely activate one or more of its Joint Task Forces (JTFs) and execute DSCA operations following requests for assistance for cyberspace incident response, law enforcement support,

or other domestic activities.³⁴ In particular, Defense Support to Cyber Incident Response (DSCIR) – included within the DSCA framework – authorizes the DoD to support federal departments and agencies for asset and threat response to cyber incidents outside the DoD Information Network.³⁵

According to several authors, a scenario involving a cyber-attack against the U.S. power grid highlights the perennial challenges of the increasing volatility, uncertainty, complexity, and ambiguity in the current environment and forecasted future. A complex catastrophe is an intractable crisis that is predictable but not influenceable.³⁶ In other words, the federal government can acknowledge that a cyber-attack could occur but cannot prevent or effectively respond because required capabilities exceed those of the public and private sectors. USNORTHCOM DSCIR operations thus continually require that federal and non-federal governmental stakeholders to enumerate DoD's mission-relevant terrain in cyberspace (e.g., key servers, systems, and network infrastructure), integrate cyber response capabilities, and ensure unified action.³⁷

Unified Action in Cyberspace

DoD must prepare cyber forces to, directly and indirectly, enable DSCIR operations, either directly or indirectly and for prolonged periods, because current and future challenges in cyberspace require sustained speed, agility, and ready resources. Building capability and capacity for DoD cyber protection and offensive cyberspace operations should focus on posturing forces with appropriate cyber authorities and knowledge of stakeholders equities. Cyber forces must effectively collaborate with federal government, public, and private stakeholders as cyber authorities and capability employment may require support or advocacy from these entities.

Unified action in cyberspace requires USNORTHCOM to synchronize and coordinate USCYBERCOM, CISA, and other federal and non-federal entities' cyber authorities and capabilities to achieve unity of effort before and throughout a complex catastrophe.³⁸ As many DoD mission functions rely on privately-owned information technology companies (e.g., cloud computing, Internet service providers, and global supply chain), DoD must build trust with these companies since the military has no direct authority over them.³⁹ General Nakasone recognizes this challenge and is actively working to bridge the gap by engaging with industry, academia, and international partners to establish bidirectional information exchanges to prevent and bolster the nation's defenses against cyberthreats, including launching the NSA Cybersecurity Collaboration Center in 2021 and expanding the USCYBERCOM Under Advisement program.⁴⁰

The unregulated information environment makes people more susceptible to misinformation, propaganda, and/or radicalization, and this poses additional challenges in DoD's efforts to counter and thwart adversaries' attempts to exploit critical infrastructure vulnerabilities. This misinformation may negatively impact DoD cyberspace operations with public and private sector stakeholders.⁴¹ Throughout a complex catastrophe and DSCA response operations, an adversary could launch an influence campaign to sow fear, doubt, and confusion amongst the American people. In addition to the impacts of denial, degradation, disruption, or destruction

of critical infrastructure, foreign and domestic mis- or disinformation could erode the public trust vital for the federal government and DoD to respond to and restore cyber and infrastructure security. For example, attacks on media outlets could cause news blackouts and impede the federal government’s ability to communicate directly with citizens, sowing additional uncertainty and fear.⁴² USCYBERCOM could support here as it increases its efforts to link cyberspace operations with information operations more tightly.⁴³

To make timely and accurate decisions concerning these events, commanders require the necessary information and intelligence to coordinate with other DoD, the federal government, and public and private sector stakeholders. Commanders’ staff and subordinate commanders must rapidly and accurately capture, manage, process, and act upon the deluge of data and information to enable decision-making throughout a complex catastrophe, as illustrated in Figure 2.

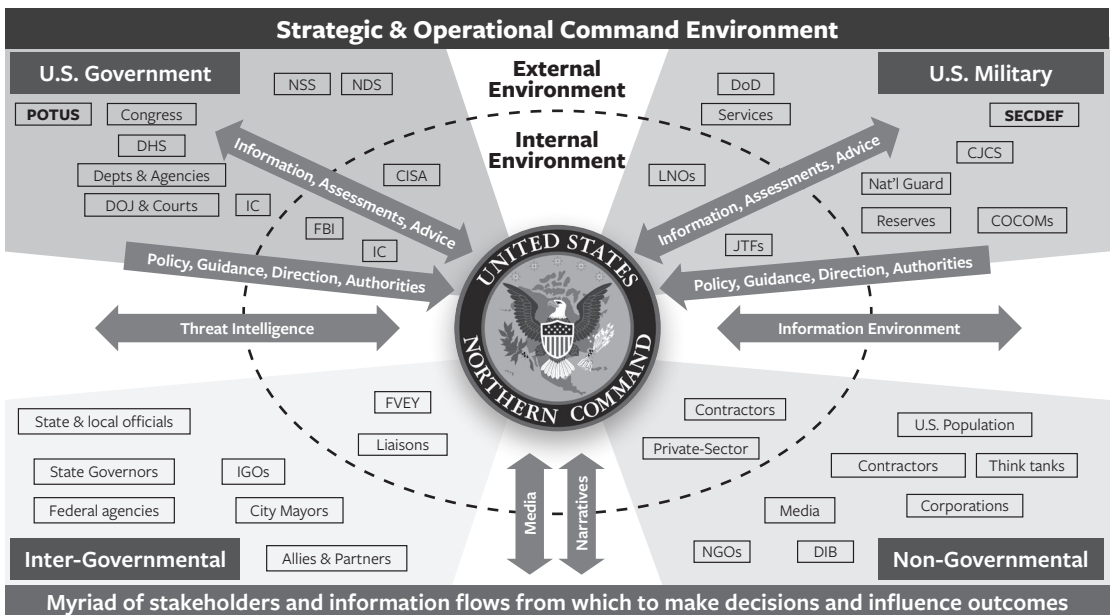


Figure 2. Complex Catastrophe Information Flows and Stakeholders⁴⁴

Joint Force commanders, planners, and cyber forces must integrate across the diplomatic, informational, military, economic, finance, intelligence, and law enforcement instruments of national power in various arrangements of supported and supporting relationships. This level of coordination requires a firm understanding of each governmental agency’s current cyberspace authorities and a great emphasis on the information and intelligence instruments in the initial hours and days of the complex catastrophe. Additionally, public and private sector stakeholders also require timely cyber threat intelligence information. Rapid detection and attribution of malicious cyber activity efforts enable the federal government, allies, and partners to leverage appropriate authorities to expel adversaries from network infrastructure and impose costs on them.⁴⁵

According to the U.S. Department of State, when allied and partner nations contribute, attribution becomes more impactful to deterrence and legitimizes responsive actions.⁴⁶ Critical intelligence-sharing between the U.S. and Ukraine exposed Russia's malign intentions before its 2022 invasion of Ukraine. When Russian forces began deploying on Ukraine's borders in late 2021, USCYBERCOM deployed a "hunt team" to collaborate with mission partners and "gain critical insights that have increased homeland defense for both the United States and Ukraine."⁴⁷ Overall, unified action enhances DoD's ability to deter and respond to cyber threats and attacks with speed and agility.⁴⁸

Cyber Mission Force Authorities to Defend the Homeland

Suppose DoD's "defend forward" operations should fail.⁴⁹ In that case, adversaries penetrating America's borders with a sophisticated cyber-attack against the U.S. power grid would impact energy, banking, finance, transportation, communication, and the defense industrial base.⁵⁰ The DoD will respond to a catastrophe of this type as outlined in Presidential Policy Directive-41, "United States Cyber Incident Coordination."⁵¹ Specifically, USCYBERCOM's Cyber National Mission Force teams would detect, deter, and, if necessary, defeat adversaries in cyberspace. Cyber protection teams would also hunt for adversaries in DoD networks and non-DoD mission partners or critical infrastructure networks.⁵² The Fiscal Year (FY) 2019 National Defense Authorization Act (NDAA) authorized USCYBERCOM to enable Joint Force and Inter-agency partners - namely DHS, the Department of Energy, and the FBI - to work on energy infrastructure security.⁵³ Given its mission to defend the homeland, USNORTHCOM must have a shared understanding of command relationships and authorities with USCYBERCOM, CISA, and the FBI. This clarity will enable USNORTHCOM to coordinate and deconflict cyber forces' operations with other interagency activities.

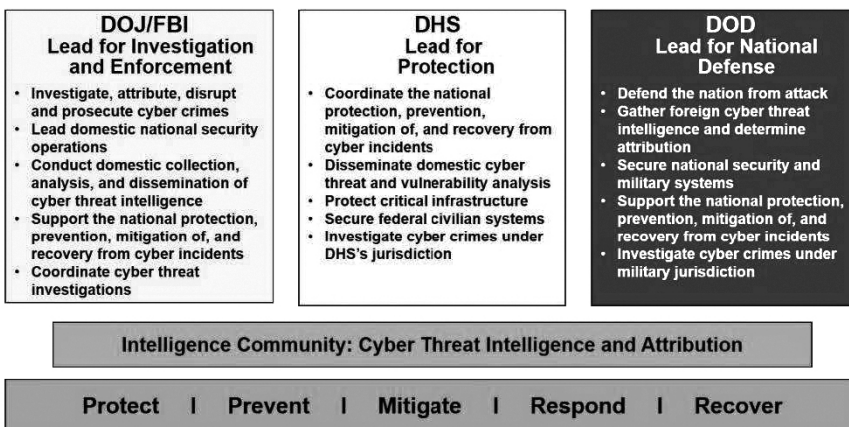


Figure 3. National Cybersecurity Roles and Responsibilities⁵⁴

As depicted in Figure 3, DoD's (i.e., USNORTHCOM and USCYBERCOM) close coordination with DHS/CISA and the greater interagency and intelligence community would enable cyber forces to detect, target, attribute and respond to complex cyber-attacks against the homeland. For example, USCYBERCOM's operations following adversaries' attacks against the Colonial Pipeline and José Batista Sobrinho (JBS) U.S.A. beef plants in 2021 demonstrated the successful level of coordination required between these agencies.⁵⁵ During these events, DoD contributed directly and indirectly to the intelligence community's attribution processes; hence, sound information-sharing and knowledge management activities – key components of cyberspace joint targeting coordination – were effectively executed.⁵⁶ Likewise, Joint Force cyberspace operations planners must clearly understand capabilities, requirements, operational limitations, liaisons, and legal considerations to optimize intelligence coordination.⁵⁷

Looking externally, USNORTHCOM – in partnership with USCYBERCOM – must build consensus with decision-makers and public and private sector stakeholders before, during, and after a complex catastrophe. As outlined in Figure 4, USNORTHCOM and DoD cyber forces must understand and leverage several titles of the U.S. Code when collaborating with stakeholders to detect, deter, and defeat cyber-attacks against the U.S. power grid and other critical infrastructure.⁵⁸

U.S. Code – U.S. Government Cyberspace Operations Authorities

Continental U.S. Complex Cyber-Attack Response Planning Considerations (USNORTHCOM)

- **Title 6 (Domestic Security)** – Assigns the Secretary of Homeland Security statutory authority to secure U.S. cyberspace.
 - In addition to USCYBERCOM's authority to enable DHS/CISA Title 6 cybersecurity efforts, cyber forces assigned to USNORTHCOM could partner with DHS/CISA in a supported and supporting capacity.
- **Title 10 (Armed Forces)** – Assigns the Secretary of Defense statutory authority to organize, train, and equip U.S. forces for military operations in cyberspace.
 - USCYBERCOM and USNORTHCOM should ensure the adequate capability and capacity of supporting cyber forces and liaison officers, and routinely validate Request for Forces packages.
- **Title 18 (Crimes and Criminal Procedure) and Title 28 (Judiciary and Judicial Procedure)** – Assigns the Attorney General statutory authority to conduct crime prevention, apprehension, and prosecution of criminals operating in cyberspace.
 - In addition to USCYBERCOM's authority to enable DOJ/FBI Title 18 cybersecurity efforts, cyber forces assigned to USNORTHCOM could partner with DOJ/FBI in a supported and supporting capacity.
- **Title 32 (National Guard)** – Statutory authority for Army and Air National Guard forces to conduct domestic consequence management.
 - The National Guard operates under Title 10 authorities if activated for federal service.
 - State governors may employ National Guard CPTs in a State Active Duty status at a state governor's direction, non-Title 10 or 32.
- **Title 40 (Public Buildings, Property, and Works)** – Statutory authority for all federal departments and agencies to establish and enforce standards for the acquisition and security of information technologies.
 - USNORTHCOM and supporting cyber forces should collaborate with federal government critical infrastructure stakeholders via Title 40, leveraging other titles under the U.S. Code (e.g., Titles 6, 10, 32).
- **Title 44 (Public Printing and Documents)** – Statutory authority for all federal departments and agencies to perform activities outlined in DoD Instruction, 8530.01, Cybersecurity Activities Support to DoD Information Network Operations.
 - USNORTHCOM and supporting cyber forces should collaborate with DoD stakeholders via Title 44, leveraging other titles under the U.S. Code.
- **Title 50 (War and National Defense)** – Statutory authority for Commands, Services, and agencies under the DoD and intelligence community agencies aligned under the Office of the Director of National Intelligence to secure U.S. interests by conducting military and foreign intelligence operations in cyberspace.
 - USNORTHCOM and supporting cyber forces should work and collaborate with the intelligence community, leveraging other titles under the U.S. Code.

Figure 4. United States Code and DoD Cyberspace Operations Authorities⁵⁹

In addition to USNORTHCOM and DoD cyber forces leveraging the above authorities and respective federal agencies to counter, blunt, and actively defend the homeland in cyberspace, aspects of Title 10 and 18 warrant additional analysis. First, Chapter 13 of Title 10 (also known as the “Insurrection Act”) and the Robert T Disaster Relief and Emergency Assistance Act grant the President of the United States to use the Armed Forces to help restore public order.⁶⁰ Next, Section 1835 of Title 18, the Posse Comitatus Act (PCA), prohibits the use of the U.S. military in civilian law enforcement.⁶¹ However, homeland defense is a Constitutional exception to the PCA.⁶² Thus, USNORTHCOM and supporting cyber forces can leverage Title 18 and the PCA to coordinate DoD cyber response operations with DOJ/FBI. Further, the Computer Fraud and Abuse Act of 1986 permits U.S. law enforcement and intelligence agencies to conduct lawfully authorized activities and does not constrain military cyber operations.⁶³

The U.S. Cyberspace Solarium Commission made considerable progress between 2019 and 2021 in removing national cybersecurity legislative barriers. As of 2022, notable milestones included 1) the establishment, nomination, and confirmation of a National Cyber Director; 2) provisions to strengthen CISA; 3) codification of Sector Risk Management Agencies; 4) establishing a Joint Cyber Planning Office; and 5) a force structure assessment of the U.S. Cyber Mission Force. Furthermore, the President's Budget Request included \$20 million to establish a Cyber Response and Recovery Fund to support asset-response activities and provide technical assistance following the declaration of a “cyber state of distress” by the Secretary of Homeland Security, in consultation with the National Cyber Director.⁶⁴ Despite this progress, laws such as the Defense Production Act and Federal Power Act may hinder DoD's cyber protection operations as private sector entities or public utilities may be reluctant to join or refrain altogether from efforts to mitigate dependencies on foreign-sourced information and communications technology and remediating cybersecurity vulnerabilities under the federal government's direction.⁶⁵

Given these dynamics and new legislation, USNORTHCOM, its JTFs, and supporting cyber forces must remain aware of and sensitive to private and public stakeholders' interests and find common ground. Private and public entities primarily tend to the prosperity and success of their enterprises, while the federal government focuses on the US and its security. Additionally, private companies have global business partnerships and work with federal and non-federal entities.⁶⁶ International business relations can put U.S. companies in tricky situations, making decisions that may accommodate one entity but offend another. In short, establishing shared trust between the DoD, federal government, and public and private sector stakeholders is complex but essential in protecting and defending critical infrastructure.⁶⁷

In addition to its ongoing “Shields Up” campaign – launched during Russia's build-up for its invasion of Ukraine – CISA has taken significant steps to build trust, including creating the Joint Cyber Defense Collaborative (JCDC) in August 2021, following provisions outlined within the FY 2021 NDAA. The goals of the JCDC are to “unify defensive actions and drive

down risk in advance of cyber incidents occurring” and “strengthen the nation’s cyber defenses through planning, preparation, and information sharing.”⁶⁸ Key U.S.-based, non-governmental JCDC partners include Microsoft, Google Cloud, Amazon Web Services, and cybersecurity providers, such as CrowdStrike, Mandiant, Palo Alto Networks, Cisco, and Symantec.⁶⁹ Additionally, Congress’ passage of cyber incident-reporting legislation on March 11, 2022, enables CISA to collaborate and receive cyber threat intelligence reports from the private sector to protect, defend, and respond to cyber-attacks on critical infrastructure.⁷⁰ Sharing information makes good business sense due to the cost of adversarial attacks and legal impacts affecting public and private sector organizations. Most notably, due to the potential cyber-attacks by Russia in retaliation for the US response to the invasion, US Congress enacted the Cyber Incident Reporting for Critical Infrastructure Act into law on March 15, 2022. The Act requires owners and operators of critical infrastructure to report cyber incidents to CISA within 72 hours and ransomware demands within 24 hours.⁷¹ The new cyber reporting law takes effect when

CISA promulgates rules to define the entities within the critical infrastructure sectors that will be impacted by [the] law and the types of substantial cyber incidents it covers. The [law] requires CISA to issue a notice of proposed rulemaking on these definitions within 24 months from the date of the bill's enactment and issue a final rule within 18 months of issuing the proposed rule.⁷²

In addition to developing a shared understanding of CISA and other federal cyber authorities, the Joint Force and federal and state governments should capitalize on the capabilities of the National Guard and Reserve cyber forces. According to Lieutenant General Jon Jensen, Director of the Army National Guard, forces gain mission-relevant experience as they rotate through USCYBERCOM in a Title 10 status.⁷³ USCYBERCOM also benefits from these rotations since most National Guard and Reserve members perform cybersecurity in their civilian jobs and bring great perspectives and knowledge. Their operational experience should be leveraged to build and strengthen ties between their home stations and local governments and public and private sector entities where they live and work, thereby building strategic depth, one of General Nakasone's objectives.⁷⁴

Before, during, and after a complex catastrophe, the relationships built by National Guard and Reserve cyber personnel are foundational for improving coordination and cooperation. Guard and Reserve forces can function as primary liaisons between DoD and others concerned with cybersecurity, improving shared understanding and building trust. National Guard cyber protection teams would conduct initial cyber incident response operations in a State Active Duty status under the direction of a state governor.⁷⁵ Regardless of status, USNORTHCOM should routinely seek opportunities to leverage Title 10 cyber authorities with Title 32 authorities to activate National Guard and Reserve members during complex catastrophe cyber mission rehearsal exercises.

Protecting U.S. critical infrastructure from cyber-attacks primarily rests with CISA, but DoD has limited cyber authorities within the public and private sectors. However, General Nakasone's new role as the National Manager puts NSA on equal footing for providing recommendations to the Secretary of Defense, the Director of National Intelligence, and the Committee on National Security Systems to improve the detection of cyber incidents affecting these systems.⁷⁶ Combined NSA and CISA authorities, capabilities, insights, and partnerships enhance USNORTHCOM DSCIR and DoD cyber force operational readiness.

Orchestrating Authorities, Capabilities, and Equities

As the DoD continues building capability and capacity to detect, deter, and defeat cyberspace threats against the homeland, it should expect resistance from external federal government and public and private sector entities. The Services may also push back given their focus on modernization plans, budget prioritization, and operations abroad. Thus, a DoD “Complex Catastrophe Cyber Stakeholders, Communications, Authorities, and Narratives” (C3 SCAN) framework could assist USNORTHCOM and USCYBERCOM in effectively planning, prioritizing, and executing complex catastrophe DSCIR operations.⁷⁷

This framework could serve as an information and knowledge management tool, enabling the Office of the Secretary of Defense to facilitate DoD cyberspace communication and collaboration with CISA and other public and private sector stakeholders.⁷⁸ The DoD C3 SCAN accounts for the local contexts of each stakeholder that could be involved, including their cyber equities, authorities, primary communications channels, and stakes in DoD's mission-relevant terrain in cyberspace. It also accounts for stakeholders' and organizations' roles in USNORTHCOM DSCIR operations.⁷⁹ The C3 SCAN would capture the various information flows, means, and narratives that serve as tools for guiding DoD senior leaders' strategic communications and key leader engagements with stakeholders, including allies and partner nations. Former USNORTHCOM Deputy Commander and National Infrastructure Advisory Council (NIAC) member, retired Lieutenant General Reynold Hoover, emphasizes open communications, strategic messaging, and engagement with key critical infrastructure stakeholders for effective response operations in the homeland.⁸⁰

USNORTHCOM, its JTFs, and supporting cyber forces know the various cyber authorities necessary to work with and through its various partners in different situations. Section 6 of Executive Order 14028 directed DHS (i.e., CISA) to “develop a standard set of operational procedures (playbook) to be used in planning and conducting cybersecurity vulnerability and incident response activity respecting [Federal Civilian Executive Branch] Information Systems.”⁸¹ Through persistent engagement with mission partners, USNORTHCOM and supporting cyber forces could participate in stakeholders' meetings and working groups to review and update their respective National cybersecurity incident response playbooks, orders, and campaign plans. The primary aims of the C3 SCAN are to 1) identify DoD cyber advocates and opponents; 2) build trust and a shared understanding amongst stakeholders

regarding cyber authorities, capabilities, and equities; and 3) identify and register stakeholders' concerns and DSCIR requirements. Due to increasing cyber threats posed by malign actors, especially Russia and China, national and international networks' vulnerabilities and complex interrelationships demand immediate coordinated action at all levels.⁸² Collaboration and work should also center on discovering and capitalizing on shared equities and interests to build more resilient relationships for crisis management. For example, in 2018, the NIAC provided the National Security Council with whole-of-nation response recommendations for improving US ability to prepare for and recover from catastrophic power outages, as depicted in Figure 5.⁸³

Recommendations Overview



Figure 5. National Infrastructure Advisory Council Recommendations for Surviving a Catastrophic Power Outage, December 2018⁸⁴

Over time, USNORTHCOM and supporting cyber forces will improve their credibility with constituents and stakeholders. They should exercise and rehearse the communications mechanisms identified within the C3 SCAN during table-top and large-scale exercises such as CISA's

biennial Cyber Storm exercise and other whole-of-nation exercises.⁸⁵ After these events, USNORTHCOM should review and refine the C3 SCAN's communications means, capabilities, and authorities. Additionally, the Command should update all cyber-related orders and directives and continuously exchange liaison officers with USCYBERCOM, DHS/CISA, and DOJ/FBI. Finally, DoD key leader engagements should engender creative ideas and discussions, bolster buy-in, and create greater transparency between stakeholders. Organizing and conducting these liaison events ahead of time is one method of mitigating the effects of intractable crises, even if the scope and scale of a future complex catastrophe are unknown.⁸⁶

CONCLUSION

As revisionist powers seek to disrupt the international order and conduct operations below the level of armed conflict, including cyber-attacks, DoD must effectively position its cyber forces and capabilities to defend against cyber-attacks before they hit the homeland.⁸⁷ An attack against the U.S. power grid could result in multiple failures in life-sustaining infrastructure and significantly impact Joint Force power-projection capabilities.⁸⁸ Accordingly, USNORTHCOM must work closely with USCYBERCOM to collaborate with CISA and other federal and non-federal stakeholders' cyber authorities, capabilities, and equities to posture DoD cyber forces to respond with speed and agility. Current federal cyber laws, such as the Defense Production Act, Federal Power Act, and others, may hinder USNORTHCOM and supporting cyber forces' ability to conduct cyberspace operations in defense of the homeland. However, several titles in the U.S. Code (e.g., Title 10, 32, 50) and recent years' NDAs equip the USNORTHCOM Commander to effectively command and control cyber defensive operations and support USCYBERCOM's offensive operations (e.g., joint targeting) before, during, and after a complex catastrophe.⁸⁹ Still, close partnerships and education must continuously occur to deconflict or clarify conflicts or inconsistencies in the numerous laws and U.S. Code.

As the supported command during complex catastrophes within CONUS, USNORTHCOM must possess a shared understanding of command relationships, cyber authorities, and capabilities with USCYBERCOM before, during, and after a complex cyber-attack. Well-coordinated national cybersecurity response planning will enable USNORTHCOM to validate plans and orders, enumerate and prioritize mission-relevant terrain in cyberspace, and ensure DSCIR readiness.⁹⁰ Preparation should include USNORTHCOM routinely exchanging liaison officers with USCYBERCOM, CISA, and the FBI and leveraging Title 10 and 32 authorities to activate National Guard and Reserve forces to prepare DoD organizations and personnel for their roles in these crises. Overall, the combined authorities, capabilities, and insights of USCYBERCOM, NSA, and the National Manager are a force-multiplier in enabling USNORTHCOM, CISA, and DoD cyber forces to thwart complex cyber-attacks.

Finally, tools such as the DoD C3 SCAN could enable the USNORTHCOM and USCYBERCOM Commanders and cyber forces to orchestrate CISA, interagency, intelligence community, public, and private sector cyber authorities, capabilities, and equities in a complex

catastrophe to plan and prioritize DSCIR options. In 1942, innovative civil-military collaboration enabled the U.S. military to partner with the newly established Civil Air Patrol to protect America's sea lanes, defend against and deter future U-Boat attacks, and thwart Germany's Operation Drumbeat.⁹¹ Similarly, the combined authorities, capabilities, and partnerships of DoD, CISA, the FBI, and the public and private sector can enable cyber forces to thwart asymmetric attacks against the homeland.♥

NOTES

1. The President's National Infrastructure Advisory Council, *Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure*, August 2017, 3, <https://www.cisa.gov/sites/default/files/publications/niac-securing-cyber-assets-final-report-508.pdf>.
2. Ed O'Flley, "The Burning Shore: How Hitler's U-Boats Brought World War II to America," (Basic Books, New York, 2014), 103-131; and Deputy Secretary of Defense, *Definition of the Term Complex Catastrophe, Memorandum for Secretaries of the Military Departments*, Washington, D.C., February 19, 2013, <https://info.publicintelligence.net/DoD-ComplexCatastropheDefinition.pdf>.
3. *Ibid*, 127-133.
4. Michael Gannon, "Operation Drumbeat: The Dramatic True Story of Germany's First U-Boat Attacks Along the American Coast in World War II," (Harper & Row Publishers, New York, 1990), 343; and Richard Lentinello, *How Gas Rationing Worked During World War II*, December 30, 2019, <https://www.hemmings.com/stories/2019/12/30/how-gas-rationing-worked-during-world-war-ii>.
5. *Ibid*, 343.
6. Lennart Maschmeyer and Nadiya Kostyuk, *There is No Cyber 'Shock and Awe': Plausible Threats in the Ukrainian Conflict*, February 8, 2022, <https://warontherocks.com/2022/02/there-is-no-cyber-shock-and-awe-plausible-threats-in-the-ukrainian-conflict/>; and Michael Hull, *Operation Drumbeat's Devastating Toll on Allied Shipping*, December 12, 2018, <https://warfarehistorynetwork.com/2018/12/09/operation-drumbeats-devastating-toll-on-allied-shipping/>.
7. Nicole Sganga, "It's Coming": President Biden Warns of "Evolving" Russian Cyber Threat to U.S.," March 21, 2022, <https://www.cbsnews.com/news/russia-cyber-attack-threat-biden-warning/>; and Raphael Satter, Zeba Siddiqui, and James Pearson, "U.S. warns China could hack infrastructure, including pipelines, rail systems," May 26, 2023, <https://www.reuters.com/world/china/china-rejects-claim-it-is-spying-western-critical-infrastructure-2023-05-25/>.
8. Cybersecurity and Infrastructure Security Agency (CISA), *Shields Up*, <https://www.cisa.gov/shields-up>. Accessed February 11, 2022.
9. U.S. Cyberspace Solarium Commission, *Final Report*, v, <https://www.solarium.gov/home>, https://drive.google.com/file/d/1ryMCIL_dZ30QyFqFkkf10MxIXGT4yv/view. Accessed February 10, 2022.
10. General Paul Nakasone, *CYBERCOM and NSA Chief: Cybersecurity is a Team Sport*, December 6, 2021, <https://www.defensenews.com/outlook/2021/12/06/cybercom-and-nsa-chief-cybersecurity-is-a-team-sport/>.
11. Department of Homeland Security, *National Preparedness Goal*, <https://www.dhs.gov/national-preparedness-goal>. Accessed February 10, 2022. "The National Preparedness Goal defines what it means for the whole community to be prepared for all types of disasters and emergencies. The goal itself is succinct: 'A secure and resilient nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk.' These risks include events such as natural disasters, disease pandemics, chemical spills and other man-made hazards, terrorist attacks and cyber-attacks."
12. Kyle Rempfer, "The Homeland is No Longer a Sanctuary" Amid Rising Near-Peer Threats, *NORTHCOM commander says*, August 27, 2018, <https://www.militarytimes.com/news/your-air-force/2018/08/27/the-homeland-is-no-longer-a-sanctuary-amid-rising-near-peer-threats-northcom-commander-says/>.
13. Department of Defense, 2022 National Defense Strategy, 5, 8, <https://media.defense.gov/2022/Oct/27/2003103845/-1-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF>.
14. The White House, *Executive Order on Improving the Nation's Cybersecurity*, May 12, 2021, <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/> and *National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems*, July 28, 2021, <https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/>; U.S. Cyberspace Solarium Commission; and The CSC 2.0 Project, *Preserving the Legacy and Continuing the Work of the Cyberspace Solarium Commission*, <https://www.cybersolarium.org/>. Accessed February 10, 2022.
15. Senators Angus King and Tom Fannin, *To Combat Cyber-Attacks, the US Government and Businesses Must Work More Closely*, July 19, 2021, <https://www.cnn.com/2021/07/19/perspectives/cyber-attacks-security-us-government-businesses/index.html>. "The commission recommended more than 75 measures ... 25 of the commission's proposals passed into law;" U.S. Cyberspace Solarium Commission, see "Our Progress"; and Solarium Commission *2021 Annual Report on Implementation*, August 2021, <https://www.solarium.gov/public-communications/2021-annual-report-on-implementation>.

NOTES

16. The White House, *Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems*, January 19, 2022, <https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems>.
17. Tim Frank, *National Security Memorandum/NSM-8: A Call to Action on Defense Systems*, January 24, 2022, https://www.splunk.com/en_us/blog/industries/national-security-memorandum-nsm-8-a-call-to-action-on-defense-systems.html.
18. The White House, *National Cyber Strategy of the United States of America*, September 2018, specifically pillar #1: “protecting the American people, homeland, and way of life by safeguarding networks systems, functions and data,” <https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>; and Department of Defense, *Summary of the Department of Defense Cyber Strategy 2018*, specifically goal #2: “compete and deter in cyberspace” and #3: “strengthen alliances and attract new partnerships.”
19. U.S. Joint Chiefs of Staff, *Joint Operating Environment 2035: The Joint Force in a Contested and Disordered World*, July 14, 2016, 17, 24, 26, 35, https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joe_2035_july16.pdf?ver=2017-12-28-162059-917; General Glen VanHerck, *Statement of Commander, United States Northern Command and North American Aerospace Defense Command Before the House Armed Services Committee and Subcommittee on Strategic Forces*, March 8, 2023, 9, https://armedservices.house.gov/sites/republicans.armedservices.house.gov/files/NNC_FY23%20Posture%20Statement%20%20HASC%20SF%20FINAL.pdf; and insights from retired Army Lieutenant General and former USNORTHCOM Deputy Commander (2016-2018), Reynold Hoover, to the author, February 23, 2022.
20. Reynold Hoover; and Steve Lasky, *A Rise In Ransomware Threatens America’s Critical Infrastructure*, January 25, 2021, [https://www.securityinfowatch.com/cybersecurity/article/21228250/a-rise-in-ransomware-threatens-america-critical-infrastructure](https://www.securityinfowatch.com/cybersecurity/article/21228250/a-rise-in-ransomware-threatens-american-critical-infrastructure).
21. Ministry of Defence, *Global Strategic Trends: The Future Starts Today*, 6th ed. (United Kingdom: Ministry of Defence, Strategic Trends Programme: Development, Concepts and Doctrine Centre, October 2018), 134, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/771309/Global_Strategic_Trends_-_The_Future_Starts_Today.pdf; and as defined by the U.S. Joint Chiefs of Staff (JCS) in Joint Publication (JP) 3-12, *Joint Cyberspace Operations* (Washington DC: U.S. Joint Chiefs of Staff, December 19, 2022), “Cyberspace. A global domain within the information environment consisting of interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers;” https://jdeis.js.mil/jdeis/new_pubs/jp3_12.pdf.
22. Office of the Director of National Intelligence, *Annual Threat Assessment of the US Intelligence Community* (Washington, DC: Office of the Director of National Intelligence, February 6, 2023), 10, 15, <https://www.odni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf>; and VanHerck, *Statement of Commander ...9-10*.
23. Andy Greenberg, “How an Entire Nation Became Russia’s Test Lab for Cyberwar,” *Wired*, June 20, 2017, <https://www.wired.com/story/russian-hackers-attack-ukraine/>; Dragos, *Crashoverride: Analysis of the Threat to Electric Grid Operations* (Hanover, Md.: Dragos, 2017), 10, <https://dragos.com/blog/crashoverride/CrashOverride-01.pdf>; and Dustin Volz, *U.S. Government Concludes Cyber Attack Caused Ukraine Power Outage*, February 25, 2016, <https://www.reuters.com/article/us-ukraine-cybersecurity-idUSKCN0VY30K>.
24. Greenberg, “How an Entire Nation Became Russia’s Test Lab for Cyberwar;” and Serhiy Martynets, *U.S. Suspects Russia of Involvement in Cyber-attacks on Ukrainian Power Grids* (Ukrainian National News), January 7, 2016, <https://www.unn.com.ua/uk/news/1536191-ssha-pidozryuyut-rosiyu-u-prichetnosti-do-kiberatak-na-ukrayinski-elektromerezhi>.
25. Cybersecurity and Infrastructure Security Agency, Alert (AA21-200A) *Tactics, Techniques, and Procedures of Indicted APT40 Actors Associated with China’s MSS Hainan State Security Department*, July 19, 2021, <https://www.cisa.gov/uscert/ncas/alerts/aa21-200a>.
26. Federal Bureau of Investigation, *Four Russian Government Employees Charged in Two Separate Hacking Campaigns Targeting Worldwide Critical Infrastructure*, March 24, 2022, <https://www.fbi.gov/news/stories/russian-government-employees-charged-in-hacking-campaigns-032421>.
27. Office of the Director of National Intelligence, *Annual Threat Assessment ...*,10, 15; and Satter, “U.S. warns China could hack infrastructure, including pipelines, rail systems.”

NOTES

28. Office of Energy Efficiency and Renewable Energy (EERE), *East Meets West? Lab Study Focuses on Connecting Power Grid from Coast to Coast* (Washington, DC: EERE, May 31, 2017), <https://www.energy.gov/eere/articles/east-meets-west-lab-study-focuses-connecting-power-grid-coast-coast>; and U.S. Energy Information Administration, *U.S. Electric System is Made Up of Interconnections and Balancing Authorities*, July 20, 2016, <https://www.eia.gov/todayinenergy/detail.php?id=27152>; In Figure 1, “The Eastern Interconnection encompasses the area east of the Rocky Mountains and a portion of northern Texas. The Eastern Interconnection [EI] consists of thirty-six balancing authorities: thirty-one in the United States and five in Canada. The Western Interconnection [WI] encompasses the area from the Rockies west and consists of 37 balancing authorities: thirty-four in the United States, two in Canada, and one in Mexico. The Electric Reliability Council of Texas (ERCOT) covers most, but not all, of Texas and consists of a single balancing authority.”
29. Cybersecurity and Infrastructure Security Agency, *Energy Sector*, <https://www.cisa.gov/energy-sector> and <https://www.cisa.gov/critical-infrastructure-sectors>. Accessed March 16, 2022); and The White House, *Presidential Policy Directive - Critical Infrastructure Security and Resilience*, February 12, 2013, <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.
30. Loch Johnson, “On Drawing a Bright Line for Covert Operations,” *American Journal of International Law*, Vol. 86, No. 2 (April 1992), 286, 292, <https://doi.org/10.2307/2203235>. According to Lennart Maschmeyer, Johnson’s escalation ladder does not include critical infrastructure sabotage, but the scope of effects places it within the riskiest, “extreme options”; and Peter Aldhous, Stephanie M. Lee and Zarah Hirji, *The Texas Winter Storm and Power Outages Killed Hundreds More People Than the State Says*, May 26, 2021, <https://web.archive.org/web/20210718121413/https://www.buzzfeednews.com/article/peteraldhous/texas-winter-storm-power-outage-death-toll>.
31. U.S. Joint Chiefs of Staff, Joint Publication (JP) 3-27, *Homeland Defense* (Washington DC: U.S. Joint Chiefs of Staff, April 10, 2018), II-8, II-12, II-13, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_27.pdf. This paper primarily focuses on a potential complex catastrophe (i.e., a complex cyber-attack) occurring within the continental U.S.
32. *Ibid.*, vii – viii, II-6, 10-11.
33. Cheryl Pellerin, *NORTHCOM Prioritizes Homeland Defense, Cyber, Partners* (U.S. Strategic Command), March 14, 2012, <https://www.stratcom.mil/Media/News/News-Article-View/Article/983560/northcom-prioritizes-homeland-defense-cyber-partners/>.
34. U.S. Joint Chiefs of Staff, JP 3-28, *Defense Support of Civil Authorities* (Washington DC: U.S. Joint Chiefs of Staff, October 29, 2018), I-2, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_28.pdf; and JP 3-27, *Homeland Defense*, II-10.
35. Department of Defense, *Deputy Secretary of Defense Directive-Type Memorandum (DTM) 17-007 – “Interim Policy and Guidance for Defense Support to Cyber Incident Response*, June 21, 2017 (change 6, June 21, 2023), 2, <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dtm/DTM-17-007.pdf>.
36. Jonathan Ablett and Andrew Erdmann, “Strategy, Scenarios, and the Global Shift in Defense Power,” McKinsey & Company, April 2013, 1, http://www.mckinsey.com/insights/public_sector/strategy_scenarios_and_the_global_shift_in_defense_power; and Stephan Gundel, “Towards a New Typology of Crises,” *Journal of Contingencies and Crisis Management* 13, no. 3 (2005), 112.
37. U.S. Joint Chiefs of Staff, JP 3-27, *Homeland Defense*, I-3; Department of Defense, *Deputy Secretary of Defense Directive-Type Memorandum ...*, 9-11; and Eric Pederson, MAJ Don Palermo (USA), MAJ Stephen Fancy (USA), LCDR (Ret) Tim Blevins, *DOD Cyberspace: Establishing a Shared Understanding and How to Protect It*, January 1, 2022, <https://www.alsa.mil/News/Article/2891794/dod-cyberspace-establishing-a-shared-understanding-and-how-to-protect-it/>.
38. U.S. Joint Chiefs of Staff, JP 3-08, *Interorganizational Cooperation* (Washington DC: U.S. Joint Chiefs of Staff, October 12, 2016, validated October 18, 2017), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_08.pdf; JP 3-33, *Joint Task Force Headquarters* (Washington DC: U.S. Joint Chiefs of Staff, 31 January 2018).
39. Lasky, *A Rise in Ransomware*; and U.S. Joint Chiefs of Staff, JP 3-12, *Joint Cyberspace Operations*, IV-17.
40. Nakasone, *CYBERCOM and NSA Chief*; and Martin Matishak, “*Cyber Command to expand ‘canary in the coal mine’ unit working with private sector*,” June 28, 2023, <https://therecord.media/cyber-command-under-advisement-team-cyber-threat-collaboration>.
41. Ministry of Defence, *Global Strategic Trends*, 16, 81, 124.

NOTES

42. Dmitri Alperovitch, *How Russia Has Turned Ukraine Into a Cyber-Battlefield*, January 28, 2022, <https://www.foreignaffairs.com/articles/russia-fsu/2022-01-28/how-russia-has-turned-ukraine-cyber-battlefield>.
43. Mark Pomerleau, *Cyber Command Moving Toward an Integrated Information War Approach*, March 11, 2022, <https://www.fedscoop.com/cyber-command-moving-toward-an-integrated-information-warfare-approach/>.
44. Adapted from General Raymond Odierno Knowledge Management Workshop product, May 2011. Modifications to graphic and addition of USNORTHCOM logo created by the author.
45. General Paul Nakasone, *Statement of Commander, U.S. Cyber Command Before the 118th Congress Senate Committee on Armed Services*, March 7, 2023, 4, <https://www.armed-services.senate.gov/imo/media/doc/CDRUSCYBERCOM%20SASC%20Posture%20Statement%20FINAL%20.pdf>.
46. Department of State, *Recommendations to the President on Deterring Adversaries and Better Protecting the American People from Cyber Threats*, Officer of the Coordinator for Cyber Issues, May 31, 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>.
47. Major Sharon Rollins, *Defensive Cyber Warfare Lessons from Inside Ukraine*, U.S. Naval Institute Proceedings, Vol. 149/6/1,444, <https://www.usni.org/magazines/proceedings/2023/june/defensive-cyber-warfare-lessons-inside-ukraine>; Patrick O’Nell, *The US is Unmasking Russian Hackers Faster Than Ever: The White House Was Quick to Publicly Blame Russia For A Cyberattack Against Ukraine, The Latest Sign That Cyber Attribution is a Crucial Tool in the American Arsenal*, February 21, 2022, <https://www.technologyreview.com/2022/02/21/1046087/russian-hackers-ukraine/>; John Grady, *Intel Sharing Between U.S. and Ukraine ‘Revolutionary’ Says DIA Director*, March 18, 2022, <https://news.usni.org/2022/03/18/intel-sharing-between-u-s-and-ukraine-revolutionary-says-dia-director>; and General Paul Nakasone, *Statement of Commander, U.S. Cyber Command Before the 118th Congress Senate Committee on Armed Services*, March 7, 2023, 4, <https://www.armed-services.senate.gov/imo/media/doc/CDRUSCYBERCOM%20SASC%20Posture%20Statement%20FINAL%20.pdf>.
48. U.S. Cyberspace Solarium Commission ..., v.
49. Paul M. Nakasone, “A Cyber Force for Persistent Operations,” *Joint Force Quarterly*, 92 (2019), 12-13, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92_10-14_Nakasone.pdf.
50. U.S. Joint Chiefs of Staff, JP 3-27, *Homeland Defense*, III-16.
51. U.S. Joint Chiefs of Staff, JP 3-12, *Joint Cyberspace Operations*, III-I-2.
52. Cohen, *CYBERCOM and NSA Chief*; and U.S. Joint Chiefs of Staff, JP 3-12, *Joint Cyberspace Operations*, II-8.
53. Cohen, *CYBERCOM and NSA Chief*.
54. U.S. Army War College, *Strategic Cyberspace Operations Guide*, Center for Strategic Leadership, August 1, 2021, 60, https://csl.armywarcollege.edu/USACSL/Publications/Strategic_Cyberspace_Operations_Guide.pdf.
55. Julian Barnes, *U.S. Military Has Acted Against Ransomware Groups, General Acknowledges*, December 5, 2021, <https://www.nytimes.com/2021/12/05/us/politics/us-military-ransomware-cyber-command.html>.
56. U.S. Joint Chiefs of Staff, JP 3-12, *Joint Cyberspace Operations*, IV-8-11.
57. *Ibid*, IV-2, IV-23.
58. FindLaw, *United States Code – Unannotated*, January 1, 2018, <https://codes.findlaw.com/us/>; U.S. Joint Chiefs of Staff, JP 3-27, *Homeland Defense* ..., III-3. *United States Code*; and Cornell Law School, 6 *U.S. Code § 466 - Sense of Congress Reaffirming the Continued Importance and Applicability of the Posse Comitatus Act*, <https://www.law.cornell.edu/uscode/text/6/466>.
59. Figure created by the author; derived from U.S. Joint Chiefs of Staff, JP 3-12, *Joint Cyberspace Operations* ..., III-3 (“Key Titles of United States Code Related to Cyberspace Operations”); FindLaw, *United States Code – Unannotated*, January 1, 2018, <https://codes.findlaw.com/us/>; Cornell Law School, 6 *U.S. Code § 466*; and Congressional Research Service, *National Guard Civil Support in the District of Columbia*, February 23, 2021, <https://crsreports.congress.gov/product/pdf/IF/IF11768>.
60. U.S. Code, §251. *Federal Aid for State Governments*, <https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title10-section251-1&num=0&edition=prelim>. Accessed March 3, 2022.
61. Peter Pascucci and Kurt Sanger, *Revisiting a Framework on Military Takedowns Against Cybercriminals*, July 2, 2021, <https://www.lawfareblog.com/revisiting-framework-military-takedowns-against-cybercriminals>.
62. U.S. Joint Chiefs of Staff, JP 3-27, *Homeland Defense*, I-6; and Department of Defense, *Deputy Secretary of Defense Directive-Type Memorandum*, 3.

NOTES

63. U.S. Army War College, *Strategic Cyberspace Operations Guide, 106-111*; U.S. Department of Justice, *9-48.000-Computer Fraud and Abuse Act*, <https://www.justice.gov/jm/jm-9-48000-computer-fraud>. Accessed March 3, 2022); Cornell Law School, 6 U.S. Code § 466; and the Honorable Paul Ney, Jr., *DOD General Counsel Remarks at U.S. Cyber Command Legal Conference*, March 2, 2020, <https://www.defense.gov/News/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/>.
64. The CSC 2.0 Project, *2021 Annual Report on Implementation, 23-24*, https://drive.google.com/file/d/19V7Yfc5fvEE6dG-IoU_7bidLRf5OvV2_/view.
65. U.S. Cyberspace Solarium Commission, ..., 63, 69; Department of Homeland Security, *Defense Production Act*, <https://www.fema.gov/disaster/defense-production-act>. Accessed February 10, 2022); and Congressional Research Service, *The Legal Framework of the Federal Power Act*, January 22, 2020, <https://crsreports.congress.gov/product/pdf/IF/IF11411>.
66. Neil Jenkins, *Testimony Before the US-China Economic and Security Review Commission on U.S. Private Industry Responses to the China Cyber Challenge*, February 17, 2022, https://www.uscc.gov/sites/default/files/2022-02/Neil_Jenkins_Testimony.pdf.
67. King and Fannin, *To Combat Cyber-Attacks*.
68. Cybersecurity and Infrastructure Security Agency, *Shields Up*; and Joint Cyber Defense Collaborative, <https://www.cisa.gov/jcdc>. Accessed February 18, 2022.
69. Jenkins, *Testimony Before the US-China Economic and Security Review Commission*.
70. Cybersecurity and Infrastructure Security Agency, *Statement From CISA Director Easterly on the Passage of Cyber Incident Reporting Legislation*, March 11, 2022, <https://www.cisa.gov/news/2022/03/11/statement-cisa-director-easterly-passage-cyber-incident-reporting-legislation>; and Jen Easterly @CISAJen Twitter update, March 11, 2022, <https://twitter.com/CISAJen/status/1502254277301002244>.
71. Shardul Desai, et al, *Cyber Incident Reporting Requirements for Critical Infrastructure Sectors Signed into Law*, March 16, 2022, <https://www.hklaw.com/en/insights/publications/2022/03/cyber-incident-reporting-requirements-for-critical-infrast-structure>.
72. Desai, *Cyber Incident Reporting Requirements for Critical Infrastructure Sectors*.
73. Army War College, *Military Strategy and Campaigning (Lesson II) Homeland Defense/DSCA Moderated Panel*, January 3, 2022.
74. Nakasone, *Statement of Commander*, 5-6; and Cohen, *CYBERCOM and NSA Chief*; and Army Cyber Command @ARCYBER, tweet regarding Army Reserve and National Guard openings in cyber, signal, legal, intelligence, logistics, IT and security, March 2, 2022, <https://twitter.com/ARCYBER/status/1499074555180109834>.
75. Reynold Hoover; and New York State Division of Military and Naval Affairs, *New York National Guard Job Zone, Cyber Protection Team (CPT) Temporary Duty (M-Day)*, <https://dmna.ny.gov/jobs/?id=cpt#:~:text=The%20Cyber%20Protection%20Team%20is%20a%20joint%20partnership,basis%2C%20in%20support%20of%20state%20and%20federal%20missions>. Accessed March 3, 2022.
76. The White House, *Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems*.
77. The author developed the DoD “C3 SCAN” framework which can be accessed here: https://warroom.armywarcollege.edu/wp-content/uploads/22-039-DoD_C3_SCAN_Framework.png.
78. Department of Defense, *Deputy Secretary of Defense Directive-Type Memorandum, 7-9*.
79. Department of Defense, *Deputy Secretary of Defense Directive-Type Memorandum, 13-14*.
80. Reynold Hoover, *Lecture: Military Operations in CONUS* (Part of the Strategic Landpower Integrated Research Project), Army War College, February 16, 2022.
81. Cybersecurity and Infrastructure Security Agency, *New Federal Government Cybersecurity Incident and Vulnerability Response Playbooks*, November 2021, https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf.
82. U.S. Joint Chiefs of Staff, JP 3-27, *Homeland Defense, II-3*.
83. The President’s National Infrastructure Advisory Council, *Surviving a Catastrophic Power Outage: How to Strengthen the Capabilities of the Nation* (Arlington, Virginia: CISA NIAC, December 2018), 2, https://www.cisa.gov/sites/default/files/publications/NIAC%20Catastrophic%20Power%20Outage%20Study_FINAL.pdf.

NOTES

85. The President's National Infrastructure Advisory Council, *Surviving a Catastrophic Power Outage*, 3.
85. Cybersecurity and Infrastructure Security Agency, *CISA Hosts Eighth Cyber Storm Exercise With More Than 200 Organizations*, March 14, 2022, <https://www.cisa.gov/news/2022/03/14/cisa-hosts-eighth-cyber-storm-exercise-more-200-organizations>; <https://www.cisa.gov/cyber-storm-viii-national-cyber-exercise>; and The President's National Infrastructure Advisory Council, *Surviving a Catastrophic Power Outage*, 3.
86. Gundel, "Towards a New Typology of Crises," 112.
87. Jim Garamone, *Global Integration Seeks to Buy Leaders Decision Time, Increase 'Speed of Relevance'*, July 2, 2018, <https://www.defense.gov/News/News-Stories/Article/Article/1565240/global-integration-seeks-to-buy-leaders-decision-time-increase-speed-of-relevan/>.
88. VanHerck, *Statement of Commander*, 9.
89. U.S. Joint Chiefs of Staff, JP 3-27, *Homeland Defense*, II-13.
90. VanHerck, *Statement of Commander*, 5,9.
91. Offley, "The Burning Shore," 157-158; Gannon, "Operation Drumbeat," 343; and Hap Harris, "Civil Air Patrol," *Aerospace Historian*, Vol. 13, No. 4 (Winter 1966), 186, <https://www.jstor.org/stable/44524484>. Accessed January 15, 2022.

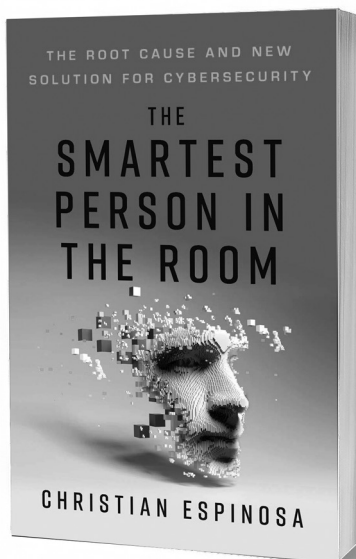
THE CYBER DEFENSE REVIEW

◆ BOOK REVIEW ◆

The Smartest Person in the Room: The Root Cause and New Solution for Cybersecurity

By Christian Espinosa

Reviewed by
Cadet Aaron Calhoun



EXECUTIVE SUMMARY

Christian Espinosa's *The Smartest Person in the Room* provides a creative approach to understanding and improving company culture. While the book emphasizes improving highly technical employees' communication and interpersonal skills, it ensures broad applicability through simplistic language and relatable personal anecdotes. The "Secure Methodology" lists in-detail human-centric goals for technical employees who experience challenges communicating with co-workers. Tailoring a technically-oriented methodology to advance social development makes Espinosa's book a useful, thought-provoking read.

REVIEW

Christian Espinosa, CEO and founder of Alpine Security, now part of CISO Global, brings 30 years of cyber security expertise service derived as an Air Force communications-computer systems officer and private sector executive. His book *The Smartest Person in the Room: The Root Cause and New Solution for Cybersecurity* draws upon his experiences, and explains why his team-building approach, the "Secure Methodology," works.

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



Aaron Calhoun, a 4th year cadet at the United States Military Academy, is a nuclear engineering major and has focused research on computational simulations of fission and inertial fusion reactors. Following his freshman year, he created a database of nuclear reactor parameters and a respective Python analysis program for Sandia National Laboratories. Through Stamps Scholarship Foundation he continued his research at Cambridge University, where he built the first full-scale nuclear reactor in the experimental code SCONE.

Eleven chapters cover two central topics: (1) why current methodologies of cyber defense are failing to overcome cyber criminals, and (2) why his “Secure Methodology” will overcome this failure. The “Secure Methodology” focuses on cyber security industry issues, but it is readily applicable to any technical or leadership environment. Espinoza’s seven steps, in order, are awareness, mindset, acknowledgment, communication monotasking, empathy, and *kaizen* (Japanese for “improvement”). To explain his steps, Espinoza provides a framework of team-level exercises and personal anecdotes that enhance reader comprehension and application.

These seven steps were formulated around Espinoza’s belief that the root cause of modern cyber security infirmities is weak interpersonal skills – often from highly-technical employees. Espinoza explains that these employees are the very heart of any successful cybersecurity company, and the effective hiring and training of this workforce is mission essential to the company at large. Technical proficiency must always remain a defining factor in a company’s hiring process, but Espinoza explains why social skills and the ability to self-reflect must also be a top priority – particularly for long-term positions. This means finding individuals resolved to overcome insecurities, defensive instincts, and any desire to be “the smartest person in the room.” Technical teams will never realize their full potential unless their members prioritize technical understanding and interpersonal communication over individual egos.

Awareness: Espinoza’s first step is developing awareness, specifically the need for meaningfully practicing self-reflection. In this chapter, Espinoza notes that common “blind spots” which limit self-awareness stem from entrenched mental patterns – these neurological “ruts” often are difficult to identify and eliminate as they are commonly subconscious actions and outlooks formulated over

many years. Thus, one's level of self-awareness often is best analyzed with the help of other people; knowing how one's actions impact others requires communication. Clear, simplistic "coaching" sessions can effectively enable employee self-reflection and awareness.

Mindset: Mindset, likewise, is an extension of awareness. It is "how you view the objective or the problem." Espinoza asserts that the most successful are those who maintain a constantly growing, "I can learn/overcome this" outlook. The growth mindset operates optimally when the driving rationale is an innate interest in their field of expertise - not a bigger salary. Espinoza's conclusion - hiring processes must account for the recruit's "why" factor. A passion for financial success alone will not motivate cyber security teams to outpace criminals.

Acknowledgment: Espinoza defines "acknowledgment" as the expression of genuine appreciation for the work of others, which requires the leader to stop and meaningfully reflect on the progression of a project or individual, rather than yet uncompleted tasks. Espinoza views this acknowledgment-based approach as far more effective in building teams that are motivated by positive affirmation and respect rather than by fear and anxiety. For cyber security executives, this also entails keen awareness and acknowledging the differences between areas of expertise. "Technical employees" are not a monolith of expertise. As a result, company leadership needs to acknowledge and understand their employees' boundaries. Lastly, he discusses how lack of acknowledgment from leadership "trickles down" and leads to a systemic culture of resentment and unappreciation. Open acknowledgment lies at the very foundation of a positive company culture.

Communication: The desire to be "the smartest person in the room," often further exacerbated by what is industry-wide reliance on inscrutable technical abbreviations, impairs effective communications in the cyber security team. In short, cyber security is often unnecessarily complicated. Espinoza urges language simplification and punctuality of body language. The author explains that body language and tone are more important even than word choice in effective communication. Both technical and executive positions need to be capable of adapting comprehensible language conducive to a shared understanding. Espinoza describes various techniques, like mirroring body language and adapting linguistic patterns, to help build a common, collegial form of communication. Unless overcome, insecurities regarding personal intelligence can seriously impair inter-disciplinary cooperation.

Monotasking: Monotasking is Espinoza's primary tool for improving focus. He explains that instant communication tools, like email, have created an environment where employees easily conflate the completion of many inconsequential tasks with productivity. Projects that require intensive focus commonly take a back seat to the implicit need for constant connection. He later observes that a culture of instant communication can cause anxiety, where every message is viewed as urgent, thereby enslaving employees "to other people's

time.” Espinoza explains that multitasking focuses on one task within a given time “block.” He also explains why people develop communication-oriented anxiety from a psychological perspective and how multitasking utilizing the “block” methodology allows for productive periods of uninterrupted work.

Empathy: Espinoza’s chapter on empathy explains why interpersonal skills are essential for all members of a cyber security team, particularly the leaders. In line with his “acknowledgement of difference”, as discussed before, Espinoza notes that the failure of employees to empathize and appreciate the talents of others limits their ability to effectively solve problems. He notes this is especially true for highly technical employees with limited understanding or appreciation for the work of non-technical employees. An overweening desire to be the smartest person in the room will further exacerbate a lack of understanding and empathy. Communications driven by a desire to maintain intellectual superiority are seldom accompanied by offers or requests for help, making technical problems harder to solve, and team members otherwise impeded by a culture of unproductive intellectual insecurity. Espinoza concludes this chapter discussing two primary forms of empathy (affective and cognitive) and how, at an individual level, they can be introduced into company culture.

Kaizen: As Espinoza states, Kaizen is the seventh and final step in the “Secure Methodology” and “gives you permission to start and then continuously improve.” The importance of Kaizen stems from the assumption that “the only thing certain is uncertainty.” Enabling an organization to set goals without black-and-white expectations creates an environment of adaptability and resiliency. Focusing on the problem(s) at hand rather than remaining upset at changes in circumstance optimizes the overall team effort in any given project. While Espinoza’s summary of Kaizen philosophy is limited, he uses much of the chapter to discuss root-cause analysis, the tool he offers to better understand fundamental causation, and how to embrace uncertainty. His discussion of Kaizen is a broader debate of how to frame fears surrounding failure and uncertainty, not an in-depth discussion of Kaizen itself. Improvement and reflection of the other six steps require Kaizen.

CONCLUSION

The Smartest Person in the Room: The Root Cause and New Solution for Cybersecurity is written with a cyber security focus, yet Espinoza’s “Secure Methodology” should apply to myriad fields and is understandable to a general audience. Despite the initial self-help guru feel of the book, Espinoza’s “Secure Methodology” provides a clear roadmap on improving the cohesion of highly technical teams. The future of cyber security, for Espinoza, can be greatly improved if companies from the outset prioritize inter-personal skills in their hiring and training practices; moreover, the adoption of the “Secure Methodology” provides specific human-centric goals for highly technical employees who are challenged in interpersonal settings. This review broadly summarizes each step of Espinoza’s “Secure Methodology;” the

book provides specific examples, exercises, and considerable detail as to how his suggestions can be implemented. In summary, Espinoza's "Secure Methodology" provides an excellent, easy to read, overview of skills that are essential to any highly technical team, particularly cybersecurity, where the technology is evolving at warp speed.📖

Full citation (as seen in this CDR Book Review):

Title: ***The Smartest Person in the Room:
The Root Cause and New Solution for Cybersecurity***

Author: Christian Espinoza

Publisher: Author's Republic (January 22, 2021)

Paperback: 280 Pages

Price: \$18.97 Paperback

 \$8.97 Kindle

THE CYBER DEFENSE REVIEW

CONTINUE THE CONVERSATION ONLINE

 CyberDefenseReview.Army.mil

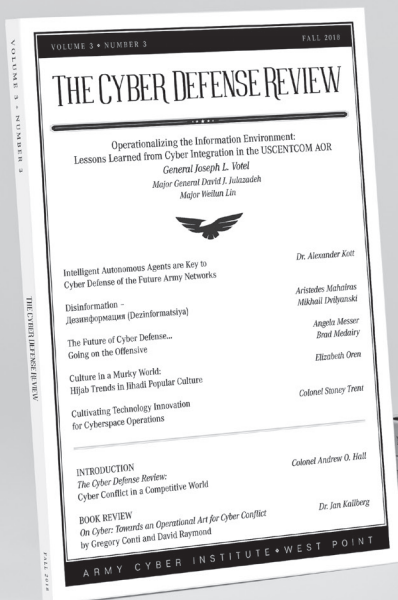
 westpointpress.com

AND THROUGH SOCIAL MEDIA

 Instagram [@WestPointPress](https://www.instagram.com/WestPointPress)

 LinkedIn [@West-point-press](https://www.linkedin.com/company/West-point-press)
[@LinkedInGroup](https://www.linkedin.com/company/LinkedInGroup)

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





WEST POINT PRESS



THE CYBER DEFENSE REVIEW IS A NATIONAL RESOURCE THAT CONTRIBUTES
TO THE CYBER DOMAIN, ADVANCES THE BODY OF KNOWLEDGE,
AND CAPTURES A UNIQUE SPACE THAT COMBINES MILITARY THOUGHT
AND PERSPECTIVE FROM OTHER DISCIPLINES.