

# THE CYBER DEFENSE REVIEW

\*\*\*

## Coalition Strategic Cyber Campaigns: Functional Engagement as Cyber Doctrine for Middle Power Statecraft

*Joseph Szeman and Christian Leuprecht*



## Weaponizing Words: Using Technology to Proliferate Information Warfare

*Dr. Craig Douglas Albert, Samantha Mullaney, Lt. Col. Joseph Huitt,  
Dr. Lance Y. Hunter, Lydia Snider*

## The Ukrainian Information and Cyber War

*Dr. Chris Bronk, Gabriel Collins (J.D.), Prof. Dan Wallace*

## U.S. Allies Offensive Cyber: Entrapment Risk or Entanglement Nuisance

*Maj. Mikkel Storm Jensen, Ph.D.*

## Risks to Zero Trust in a Federated Mission Partner Environment

*Keith Strandell and Dr. Sudip Mittal*

## Competitive Advantage in the Russo-Ukraine War: Technological Potential Against a Kremlin Goliath

*Capt. Melissa Vargas*

## Beyond “Bigger, Faster, Better:” Assessing Thinking About Artificial Intelligence and Cyber Conflict

*Dr. Christopher Whyte*

---

### INTRODUCTION

Cyber: If you want to go fast, go alone,  
if you want to go far, go together

*Col. Stephen Hamilton*

### BOOK REVIEW

*Cyber Persistence Theory: Redefining  
National Security in Cyberspace*  
by Michael P. Fischerkeller, Emily O. Goldman,  
and Richard Harknett

*Dr. Mark Grzegorzewski*



# THE CYBER DEFENSE REVIEW

◆ FALL 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

Prof. Tim Watson  
Loughborough University, UK

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

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

Prof. Samuel White  
Army War College

Dr. Martin Libicki  
U.S. Naval Academy

Dr. Hy S. Rothstein  
Naval Postgraduate School

**CREATIVE DIRECTORS**

[Sergio Ananco](#) | Gina Daschbach

**LEGAL REVIEW**

Courtney Gordon-Tennant, Esq.

**KEY CONTRIBUTORS**

Sheri Beyea

Tim Boss

Col. (Ret.) John Giordano

Charles Leonard

Thomas Morel

Clare Blackmon

Kate Brown

Lt. Col. Douglas Healy

Evonne Mobley

Alfred Pacenza

**CONTACT**

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

**SUBMISSIONS**

*The Cyber Defense Review*  
welcomes submissions at  
[TheCyberDefenseReview@westpoint.edu](mailto:TheCyberDefenseReview@westpoint.edu)

**WEBSITE**

[cyberdefensereview.army.mil](http://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. Stephen Hamilton	9	Cyber: If you want to go fast, go alone, if you want to go far, go together
-----------------------	---	--------------------------------------------------------------------------------

RESEARCH ARTICLES

Dr. Craig Douglas Albert Samantha Mullaney Lt. Col. Joseph Huitt Dr. Lance Y. Hunter Lydia Snider	15	Weaponizing Words: Using Technology to Proliferate Information Warfare
Dr. Chris Bronk Gabriel Collins (J.D.) Prof. Dan Wallach	33	The Ukrainian Information and Cyber War
Dr. Mark Grzegorzewski Maj. Margaret Smith Dr. Barnett Koven	51	Civil Cyber Defense – A New Model for Cyber Civic Engagement
Maj. Mikkel Storm Jensen, Ph.D.	67	U.S. Allies Offensive Cyber: Entrapment Risk or Entanglement Nuisance
Keith Strandell Dr. Sudip Mittal	89	Risks to Zero Trust in a Federated Mission Partner Environment

---

---

## RESEARCH ARTICLES

**Joseph Szeman  
Christian Leuprecht**

99

Coalition Strategic Cyber Campaigns:  
Functional Engagement as Cyber  
Doctrine for Middle Power Statecraft

**Capt. Melissa Vargas**

121

Competitive Advantage in the  
Russo-Ukraine War: Technological  
Potential Against a Kremlin Goliath

**Dr. Christopher Whyte**

135

Beyond “Bigger, Faster, Better:”  
Assessing Thinking About Artificial  
Intelligence and Cyber Conflict

---

## PROFESSIONAL COMMENTARY

**Lt. Col. John Childress**

153

CISA – The Future of Cyber  
Weather Forecasting

---

## BOOK REVIEW

**Dr. Mark Grzegorzewski**

161

*Cyber Persistence Theory:  
Redefining National Security  
in Cyberspace*  
By Michael P. Fischerkeller,  
Emily O. Goldman,  
and Richard Harknett





# THE CYBER DEFENSE REVIEW

◆ INTRODUCTION ◆



# Cyber: If you want to go fast, go alone, if you want to go far, go together

Colonel Stephen Hamilton, Ph.D.



As I write this, Israel has declared itself in a state of war against Hamas. Ukraine pushes steadily for the recovery of its territory from the Russian invasion, and uncertainty around the globe continues to increase. When I reflect on the changes over the last decade in the cyber domain, there appears to be a common theme: collaboration and interdisciplinary teamwork. Technology continues to evolve rapidly. However, our ability to employ technology and defend cyberspace successfully has increasingly required collaboration and teamwork; hence, we cannot do it all alone. Just as in the post-WWII era other manufacturing economies stood up and began to compete with American dominance, so too has American dominance in the cyber domain begun to erode as other nations with different skills and technology emerge as global leaders.

The U.S. Army does nothing alone. Through the doctrine of Unified Action, the different services come together to mass effects, divide responsibilities, and share intelligence and other resources – all with the objective of fighting and winning the nation’s wars in land, maritime, air, space, and cyberspace. As a computer scientist and Signal officer, I focused the first part of my career in the physical dimension of computer hardware, software, and networking. Once I transitioned to the Cyber branch, I realized that the

*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 Stephen Hamilton** is the Director of the Army Cyber Institute at the United States Military Academy (USMA) located at West Point, New York. In his position as Director, COL Hamilton leads a multi-disciplinary team of military and civilian scholars who provide advisement and research for the U.S. Army. He has a B.S. in Computer Science from USMA, an M.S. in Software Engineering from Auburn University, and a Ph.D. in Computer Science from the Johns Hopkins University. COL Hamilton additionally teaches Cloud Computing in the Department of Electrical Engineering and Computer Science. He began his career as a signal officer and deployed in support of Operation Iraqi Freedom in 2004 where he commanded Alpha Company 57th Signal Battalion. Following a tour at USCYBERCOM, he transferred to the Cyber Corps. He holds an extra class amateur radio license, and his research interests include software-defined radios, cloud computing, and data visualization.

cyberspace domain cuts across all three dimensions: physical, human, and information. This is what makes the cyber domain difficult to comprehend and operate in: the academic disciplines that the domain crosses span across electrical engineering, computer science, data science, and social science. It is not enough to be an expert only in computer science—true expertise requires leveraging expertise in all these fields. That is why this trend of collaboration and interdisciplinary teamwork has emerged—the only way to have the expertise in all the fields is to build a team of experts. It is not sufficient merely to be an expert on databases or networking—modern threats are crossing multiple areas of expertise and moving rapidly as the law and the military work to keep pace. As an example, advances in large language models require knowledge not only of advanced math but also of how the very messy real world is encapsulated into data.

In this edition of the CDR, the reader will find several articles that present this theme. Beginning with our research articles, we see the theme of teams of interdisciplinary experts coming together to tackle hard problems. In the article “Civil Cyber Defense,” Dr. Mark Grzegorzewski, MAJ Margaret Smith, and Dr. Barnett Koven discuss the concept of a civil cyber defense force like the Air Force’s Civil Air Patrol and argue for a whole-of-society approach to cybersecurity. The authors base this recommendation on Estonia’s Cyber Defense League (CDL) organization. It not only demonstrates the need for collaboration and teamwork in our society but also shows that our partners in Estonia can potentially help us learn how to do this. There is another article “Risks to Zero Trust in a Federated Mission Partner Environment,” by Keith Strandell and Sudip Mittal, which discusses how to share data effectively and securely through federated mission partner networks in a zero-trust environment. In “Coalition Strategic Cyber Campaigns: Functional Engagement as Cyber Doctrine for Middle Power Statecraft” Prof.

Christian Leuprecht and Joseph Szeman provide functional engagement as a strategy for middle power states to operate with a voice in cyberspace since they do not have the capacity for persistent engagement. Yet again, this idea shows the teamwork nature of cyber.

To survive in cyberspace, we must also ensure the various agencies and military units within the Department of Defense work together as a team. The article “Weaponizing Words: Using Technology to Proliferate Information Warfare” presents the risks the US is facing in the information advantage environment. One of the policy recommendations is for the US to unify its approach to data, intelligence, and information warfare. This requires an interdisciplinary and teamwork approach for the US to gain an advantage in information warfare.

We feature two research articles that examine the Russia-Ukraine conflict, “The Ukrainian Information and Cyber War,” by Chris Bronk, Gabriel Collins, and Dan Wallach, and “Competitive Advantage in the Russo-Ukraine War: Technological Potential Against a Kremlin Goliath,” by CPT Melissa Vargas. CPT Vargas’s work describes how collective efforts outside Ukraine (international teamwork) gave the nation an otherwise unanticipated competitive advantage by rallying the world to its cause and ensuring support in actions and weapons, and not just words. In “The Ukrainian Information and Cyber War,” the authors discuss the advantages Ukraine had due to cyber threat intelligence from Microsoft and Google, along with the Starlink network to provide connectivity when the Viasat modems were cyber-attacked. This collaboration shows promise but also the risks of efforts between US private companies and the government of Ukraine. These last two articles are real-world examples of how future wars will be fought—it is not just by the Army, but an international teamwork event across the five domains in three dimensions: physical, informational, and human.

Finally, the professional commentary “CISA – The Future of Cyber Weather Forecasting,” LTC John Childress describes CISA’s Joint Cyber Defense Collaborative (JCDC), which aims to partner with private cybersecurity companies to help disseminate and enhance cybersecurity data to provide a “forecast” for everyone in the cyber ecosystem. He then compares it to the National Weather Service (NWS), which provides forecasts using weather data. The analogy of weather and cyber events was conceived as early as 2000 when the SANS Institute stood up the Internet Storm Center. However, the idea of looking at how the NWS operates to help define how the JCDC will work brings up the theme of collaboration and teamwork. The NWS relies not just on distributed sensors, but also on people to working together to help build an accurate forecast.

I hope the main takeaway from this edition of the CDR is how robust cyber expertise sits at the intersection of other disciplines, and to truly excel in this space, it requires teams of experts working together, sharing knowledge, and leveraging information to fight and win the nation’s wars. The future of success in both cyber activities and war resides in collaboration and teamwork as new technologies rapidly emerge and become a part of our new way of operating.♥



# THE CYBER DEFENSE REVIEW

◆ RESEARCH ARTICLES ◆





# Weaponizing Words: Using Technology to Proliferate Information Warfare

---

Craig Douglas Albert, Ph.D.  
Samantha Mullaney  
Lieutenant Colonel Joseph Huitt

Lance Y. Hunter, Ph.D.  
Lydia Snider

## ABSTRACT

*The United States risks losing its information advantage over its near-peer competitors, specifically China. One reason behind this possibility is that the U.S. lacks a coherent doctrine of information warfare, which has put the U.S. at a disadvantage. Considering the Russian interference in elections of several North Atlantic Treaty Organization (NATO) states and allies, including Ukraine, Germany, and, the United States, most stunningly in the 2016 presidential election, this article addresses the question: What is to be done? Before delving into possible solutions, the exact nature of the complex problem must be explored. The purpose of this article is to investigate the ways the U.S. could improve in information warfare, specifically against one of its top near-peer competitors, China. First, this article summarizes how China compares with the United States concerning information warfare and influence operations. Second, it delves into some of the definitional chaos in which the U.S. is mired. Thirdly, the article illustrates the doctrinal and data policies of the U.S. Department of Defense. Finally, it concludes with policy recommendations.*

## INTRODUCTION

This article asserts that the United States (U.S.) could perform better in the realm of information advantage against its near-peer competitors. Specifically, we examine China's IW (Information Warfare) as it is an increasingly DoD-recognized threat and its growing technological development in the realm of artificial intelligence poses unique threats to the U.S.<sup>1</sup> We demonstrate that the key reason for the current

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



**Craig Douglas Albert, Ph.D.**, is Professor of Political Science and the Graduate Director of the Master of Arts in Intelligence and Security Studies at Augusta University. His areas of concentration include international relations and security studies, ethnic conflict, cyberterrorism, cyberwar, information operations, and epidemic intelligence. He is widely published, including articles in the *Defense and Security Analysis*; *Iran and the Caucasus*; *Politics*; *East European Politics*; *Chicago-Kent Law Review*; *Politics and Religion Journal*; *Politics & the Life Sciences*; *Cyber Defense Review*; *Journal of Cyber Policy*; *Global Society*; and *Intelligence and National Security*. Dr. Albert has testified before a U.S. Congress' joint sub-committee of the House Foreign Affairs Committee. You can follow him on Facebook/Instagram/Twitter @DrCraigDALbert.

predicament is that the U.S. lacks a coherent doctrine of IW, which puts the U.S. at a disadvantage. China's current advantage is due not to its superior capability, but to the U.S.' lack of clear definition of terms, lack of unified approach, and lack of effective use of data. Thus, the U.S. has the capacity and capability to improve and to regain strategic superiority in this realm. We acknowledge that "information warfare" is not a term currently endorsed and widely used by the U.S. government. In fact, As Ross denotes, the U.S. Army is moving toward a new terminology, contained within the Information Advantage (IA) and Decision Dominance (DD) doctrinal framework.<sup>2</sup> Information Warfare is one of the tasks associated with the IA & DD framework, but we chose to focus on IW to examine an adversary's point of view, and the Chinese Communist party (CCP) is waging information warfare against the U.S.. Also, it is a term commonly used outside the U.S. government and within academia, but we also seek to acknowledge the future of IA & DD in DoD.

As recently as 2018, Seth Jones noted that the U.S. abandoned most of its information capabilities, choosing to focus on lethal rather than political or information operations.<sup>3</sup> Historically, the U.S. has been surprised by its strategic adversaries' sophistication and offensive capability, including non-state actors such as the Islamic State of Iraq and the Levant (ISIS). The Institute for the Study of War acknowledged this in 2016, stating that tactics such as ISIS's virtual caliphate, posed a distinct threat to the U.S. as long as they did not have a clear, government-wide IW strategy.<sup>4</sup> Today, the CCP wields specific information warfare tactics and poses a similar threat.

The U.S.'s IW deficit stems from a lack of a common definition. At times, different units within the U.S. military work against each other, rather than with each other, producing a "silo effect" of data, information, and ultimately intelligence collection and analysis. There is considerable movement within the service branches



**Samantha Mullaney** is a graduate of Augusta University's Master in Intelligence and Security Studies Program in Augusta, Georgia. The focus of her research is on information warfare forms, tactics, and implications. Her capstone included completing an information warfare internship at the Georgia Cyber Center, where she researched Russian information warfare forms and tactics in Ukraine and the US between 2014 and 2020. Samantha has a BA in History from Fairfield University, an MA in Elementary Education from Boston University, and spent nearly a decade teaching children in Djibouti, Yemen, Jordan, and the UAE. She also speaks intermediate Arabic and basic German. She has been published in *The Cyber Defense Review*.

to adopt and update the language from information warfare and information operations in favor of the term “information advantage.” However, many branches are still suffering from a historical lack of common parlance. For instance, when President Clinton established the Broadcasting Board of Governors (BBG), it did not synchronize other elements of public diplomacy or strategic communications, and thus the Departments of State and Defense disseminated different public messaging.<sup>5</sup> Some of this may stem from the fact the Department of State-led Global Engagement Center (which has a vital role supporting information operations) seems to be understaffed, undersourced, and plagued by internal problems that have affected proper messaging in this realm.<sup>6</sup> In fact, Kiesler notes, “There is no recognized leadership to task, direct, resource, or guide policy in the highly complex, disparate field of information operations.”<sup>7</sup> LTG Stephen Fogarty and COL (Ret.) Bryan Sparling recently wrote, “The stunning social media-powered rise of ISIS in 2015, Iran's increasing digital belligerence, and China's disinformation surrounding the COVID-19 pandemic” are all examples of information warfare challenges that have begun “a conversation across the defense establishment regarding appropriate roles for the uniformed armed services in this environment of unprecedented information warfare.”<sup>8</sup> The above instances of information warfare and information operations (IWIO), as well as Russian interference in several NATO states and allies since at least 2018, begs the question: What is to be done?<sup>9</sup>

Of course, before delving into possible solutions, the exact nature of the complex problem must be explored. The purpose of this article is to investigate how the U.S. is fairing in information warfare, specifically against one of its top near-peer competitors, China. It also seeks to deliver recommendations on how it could do better concluding with specific policies meant to create discussion within the community and mitigate the problems. Before proceeding, however, it is important



**LTC Joseph Huitt** is a Cyber Warfare Operations Officer, currently serving as Cyber Warfare Deputy Director, Talent Management U.S. Army Cyber Command and also as a senior fellow at West Point's Center for Junior Officers. He is a graduate of the College of Naval Command and Staff, U.S. Naval War College, and a Distinguished Military Graduate of Augusta University. LTC Huitt holds master's degrees in Defense and Strategic Studies, and Intelligence Studies. LTC Huitt has served in leadership positions from the tactical to strategic levels, over his 23-plus years of service. He has gained invaluable experience serving with Special Operations Command in West Africa, USAFRICOM in England, NATO-ISAF in Afghanistan, 66th Military Intelligence Brigade in Germany, USARCENT in Saudi Arabia, 2nd Infantry Division in South Korea, and various stateside units.

to provide some conceptualization of terms that are used throughout this article.

Information warfare (IW) refers to the deliberate use of any element of information to influence the decision making of the adversary and achieve a strategic goal.<sup>10</sup> IW takes place within the information environment, which refers to the physical, informational, and cognitive dimensions that interact with information.<sup>11</sup> Information operations (IO) refer to the specific tactical undertakings in the pursuit of information warfare. The goal of IW is to act in a manner that aids in manipulating the adversary "to win strategic victories and bend the wills of their adversaries without ever engaging in physical combat."<sup>12</sup> It is important to note that IW is used at all stages of warfare, including in kinetic operations. We now turn to a brief illustration of how China dominates the narrative and achieves an advantage across the information environment.

### LEFT BEHIND AND OUTMANEUVERED

Malicious actors have benefited from access to modern technology, such as social media platforms, AdTech, and vast troves of stolen data, enabling IW to become one of the cheapest, easiest, and least restrictive types of warfare.<sup>13</sup> The quest to disrupt the decision-making process by using and misusing information is incredibly destabilizing to open societies since IOs target the cognitive domain of individuals and the citizenry as a whole.<sup>14</sup> IW seeks to sow confusion and polarization, thereby destroying the bonds that provide for stability within a society.<sup>15</sup> The U.S.'s historical emphasis on tactical and kinetic activities has placed it at a distinct disadvantage during the current period of conflict between major competing powers, specifically with China.<sup>16</sup> Competing nation-states seek to undermine the U.S.'s democratic norms and stability by utilizing information operations.<sup>17</sup>



**Lance Y. Hunter, Ph.D.**, is Professor of International Relations in the Department of Social Sciences at Augusta University. Dr. Hunter's expertise is in security studies and democratization. His research focuses on the causes and effects of terrorism and the relationship between evolving technology and conflict. His work has appeared in *Journal of Peace Research*; *Terrorism and Political Violence*; *Party Politics*; *Studies in Conflict and Terrorism*; *Armed Forces and Society*; *Conflict, Security and Development*; *European Political Science*; *Global Policy*; *Cyber Defense Review*; and *World Affairs*.

### *China's Strategic Advantage*

China possesses a comprehensive doctrine and advanced physical IW assets.<sup>18</sup> This is possibly due in large part to the nature of the totalitarian state, which has more comprehensive control over the information infrastructure than the U.S. and therefore greater strategic advantage.<sup>19</sup> Limited in scope, but strategically long-term, IW measures are consistently implemented, creating a cumulative effect. Chinese IW emphasizes "limited objectives in a limited theatre of operations, conducted away from its borders, higher in tempo, shorter in duration, but highly decisive in nature."<sup>20</sup> By combining the thinking of Sun Tzu and Mao Zedong, Chinese IW is heavily focused on psychology and is used as a weapon in and of itself rather than as a support tool.<sup>21</sup> Most Western scholars define Chinese IW as encompassing China's "three warfares," which include legal, psychological, and media operations. These "warfares" attempt to demoralize the adversary, influence public opinion, and manipulate international law.<sup>22</sup> Most noticeable is China's willingness to use highly integrated IW preemptively, illustrated by its IO campaign against Taiwan.<sup>23</sup> Wortzel explains that China combines electronic warfare, precision strikes, cyber warfare, and attacks on space systems to paralyze an adversary's information capabilities.<sup>24</sup>

Strategically, China adheres to Mao's concept of the "People's War" when waging cyber-enhanced IW. This means utilizing a high volume of cyberattacks or dissemination of disinformation through cyber means. Watts explains the content across platforms is uniform.<sup>25</sup> Furthermore, as a totalitarian state, the CCP can coerce numerous Chinese citizens to do their part and espouse a narrative on behalf of the state, as illustrated by the "50 Cent Party."<sup>26</sup> One advantage is the sheer number of people the CCP has working in this arena. They have the ability to direct vast numbers of actual users to execute bot-like operations. Unlike actual bots, however, these are immune to platform bot





**Lydia Snider** works for the U.S. Department of the Army as a specialist in foreign malign influence.

violation rules, because behind the accounts are real people. While thousands may be posting at the behest of the CCP, even copying and pasting the same response, when the platform AI studies the event, it sees numerous real accounts, not a bot network. IW is at the forefront of China's revolution in military affairs and is viewed as the critical weapon rather than a support for other military endeavors.<sup>27</sup> China recognizes that it cannot compete with U.S. defense spending and instead, starting in the 1950s, has institutionalized IW which has developed into a Strategic Support Force (SSF), the current central element of China's IW capabilities.<sup>28</sup>

China has created entire institutions to develop IW capabilities, including the Academy of Military Sciences Military Strategy Research Centre, the PLA Academy of Electronic Technologies, and the Xian Politics Academy that trains psychological warfare officers.<sup>29</sup> Additionally, the PLA has utilized simulation training for IW for more than a decade.<sup>30</sup> Psychological warfare units are dispersed throughout the PLA following initial training, providing a common language and doctrine across departments. Additionally, Elsa Kania and John Costello, as well as Larry Wortzel note that China's view of IW subsumes cyber warfare.<sup>31</sup> Given the totalitarian control the CCP needs over the domestic population, this sort of integration of cyber and information capabilities in the international arena would not be out of character. In fact, the control over information and therefore ideology, whether through cyber-mediated elements or not, "may allow for better planning, acquisition, and operations while enabling the creation of a more flexible cadre of personnel tailored toward new paradigms of information operations."<sup>32</sup> China's global network of influencers illustrates this strategy.<sup>33</sup> In this strategy, videos of mostly young Chinese women speaking in the language of the target audience speak of their respect for the target country and its culture and of China as a good friend. These videos appear in over a hundred different languages with almost the same script.<sup>34</sup> Each

of these academies and centers gives China a probable advantage over the U.S. in that they are steadily increasing their understanding of TTPs in the realm of information warfare and have wide dispersion capabilities as well. The resulting strategy allows for more flexibility and fluidity in its offensive operations.

The last two decades have seen China attempt to move from confrontational IW to the appearance of cooperation.<sup>35</sup> However, the facade has grown very thin in recent years with the development of the “wolf warrior diplomacy” strategy, which vigorously targets the U.S. and other Western nations and institutions.<sup>36</sup> China builds the facade through a proliferation of Confucius Institutes, hosting new journalists from Africa in training workshops, and promoting tourism and events for foreign elites.<sup>37</sup> The Belt and Road Initiative is presented as economic cooperation for the betterment of developing states, but large-scale Chinese investment in Africa has led to negative consequences. The CCP’s infrastructure investment, a core element of the Belt and Road Initiative, is directly linked to undercutting local construction companies, operating on a profit margin of less than 10 percent, and is often tied to selection and use of Chinese contractors.<sup>38</sup> In addition, these single-source projects often are launched without feasibility studies or may include a clause to allow for a loan’s cancellation and immediate repayment.<sup>39</sup> Although the Initiative is presented as a cooperative endeavor, one is reminded that it is indeed another form of Chinese propaganda, aimed at promoting the overall aims of the CCP.

The Chinese strategy focuses on weakening the institutions that stabilize American society by co-opting human networks inside these institutions. Other CCP-backed groups include the Chinese Students and Scholars Association and the China Association for International Friendly Contact. The former is a network across universities that receives funding from the CCP and distributes propaganda targeted at universities where there may be negative narratives about China.<sup>40</sup> The latter organization specifically targets business people and veterans and seeks to shape messaging through invitations to tour China.<sup>41</sup> When China faces an inability to create a façade of cooperation, it relies on different elements of the three warfares to coerce or manipulate adversaries. This is most adeptly seen in China’s activity in the South China Sea.<sup>42</sup> China’s aptitude in IW is clear. Its fleet of spy ships, SIGINT stations located as far afield as Cuba, its own dedicated SIGINT/EW aircraft, and dispersed human asset network allow it to carry out IW simultaneously along multiple fronts.<sup>43</sup> In terms of media warfare, China has adroitly co-opted media outlets around the world through its front organization, Xinhua News. In Africa especially, this co-option of local journalists has weakened any concerted critique of China’s Belt and Road Initiative and extractive policies, helping China wage a psychological war and also enabling the manipulation of Africa’s legal structures.

There is little distinction between foreign and domestic media control by the Chinese Communist Party. For example, the Central Propaganda Department controls China National Radio, China Radio International, and CCTV. Consolidating media control is a deliberate attempt to unify domestic and international propaganda narratives.<sup>44</sup> The United Front, Confucius Institutes, and wealthy Chinese working on behalf of the CCP have co-opted universities,

professors, think tanks, multinational corporations, and researchers to convey to the public crafted messages on behalf of the CCP, funnel research to China, and censor scientific or academic research that would negatively affect China's reputation.<sup>45</sup> This use of messaging encourages Americans to trust the espoused narrative because it comes from traditionally venerated U.S. institutions, such as universities and think tanks. This creates a unified front within China, where the domestic and international narrative focuses on Chinese supremacy, posing a threat in itself to the effectiveness and longevity of democratic states worldwide. The more people "believe" in China's regime, the more a threat is posed to democratic institutions worldwide, in the long run. This is yet another angle China uses in its information war against the U.S.

Chinese IW is also present on social media platforms. Scott Harold, Nathan Beauchamp-Mustafaga, and Jeffrey Hornung posit that China's use of social media helps it destroy an adversary's command authority through the demonization of a leader and the demoralization of the public.<sup>46</sup> Like Russia's, Chinese IW sees chaos and division as a product of successful psychological warfare, whether waged on social media platforms or through strategically placed individuals parroting a Chinese narrative. Given the totalitarian nature of the CCP, any and every business or actor inside of or connected to China can and may be used for the benefit of the state. One advantage the CCP maintains over the U.S. is its willingness to exert state control over social media platforms, through its censorship of internal conversation and with state control over the now internationally used platform, TikTok. With TikTok, the CCP has a platform that both collects data on users and over which it has complete control of what content is delivered to users.

Currently, China's use of cyber for IW is coupled with a powerful and far-reaching network of human agents cultivated through organizations such as the United Front that help execute highly complex and integrated influence operations.<sup>47</sup> This vast network of human assets in multiple arenas enables China to alter public perception and portray messages favorable to the CCP. Specifically, China targets personnel and institutions with financial incentives to dampen negative publicity.<sup>48</sup> The CCP's response to the COVID pandemic is illustrative of its IW capabilities and its strong coordination between overt and covert IW.<sup>49</sup> Now that a brief case analysis of China's use of IW and IO has been illustrated, it is necessary to understand how and in what ways the U.S. lags behind China in the IW/IO competition. Ultimately, the U.S. cannot replicate the CCP's power over the PLA and utilize its IW forms and tactics without demolishing national and international war standards. That does not mean the U.S. cannot find a way to counter these tactics and maintain democratic norms.

## **DEFINITIONAL CHAOS**

The U.S.'s competitors and near-peer competitors have institutions devoted to the successful utilization of information operations and achievement of strategic advantage in this domain. They also have broad, but useful, definitions of IW. Largely, the U.S.' adversaries define IW as conflict in the information space that forces a specific decision by undermining political, information, social, or economic systems, often using mass psychological tactics to destabilize



society by targeting a population.<sup>50</sup> The goal of modern IW against the U.S. is to erode trust in authority and institutions, thereby undermining shared values.<sup>51</sup>

The U.S. government does not have a consistent definition of what IWIOs are, and lacks a dedicated institution or agency with which to wage IWIOs effectively for strategic advantage.<sup>52</sup> IW is divided across multiple agencies in the U.S., such as the Department of State's Global Engagement Center, the CIA, U.S. Cyber Command (USCYBERCOM), and other elements of the military.<sup>53</sup> Essentially, the U.S. uses the "same terms differently in different contexts," which creates confusion and a lack of strategic capability.<sup>54</sup> Scholars such as Whyte define IW as the use or abuse of information to influence the decision-making options and processes of the adversary to achieve military or strategic gains.<sup>55</sup> This is a broad definition that encompasses many tactics within the military and non-military realms. The Army's definition is somewhat similar, noting that IW is a simultaneous effort directed at creating a specific effect in the information environment and is a battle "*of* information," rather than just a battle *for* information.<sup>56</sup> However, a 2012 joint publication from the Joint Chiefs of Staff confined IOs to military operations.<sup>57</sup> In fact, Alicia Wanless and James Pammet note that the U.S. interprets IW/IO in largely military terms and tries to delineate between acceptable and unacceptable actions within these parameters.<sup>58</sup> There is no such distinction for foreign adversaries given their different governing structures.

It is understandable that the military focuses on command and control and how IW targets critical military elements necessary to gain a military strategic advantage. However, the IW waged against the U.S. is far broader than this focused definition. IOs target the cognitive domain of individuals and the citizenry as a whole.<sup>59</sup> China utilizes persistent narratives that cause members of the target society to question themselves, and China seeks to disrupt the decision-making process of a state by using and misusing information. The U.S. government requires a common definition of IW which can be disseminated to national security agencies, the military, and public relations elements. These terms should be clearly defined and the parameters demarcated. The U.S. cannot wage an effective defensive information war without a consistent definition of IW.<sup>60</sup> This article now proceeds to a discussion regarding how the DoD understands and effectuates IW. After detailing this, this article proceeds to set-forth policy recommendations that seek to bolster the U.S.'s IW/IO.

## DATA AND THE DEPARTMENT OF DEFENSE

To better understand the impact of information warfare and the U.S. Government's (USG) approach to counter adversary actions, it is imperative to review the existing doctrine and policy that guide it. This article highlights the current guidance from the DoD and some of the challenges of wading through the vast data, directives, and policies which reference decades-old policy, include conflicting guidance, and lack of a common lexicon. To set some common ground, the authors first discuss what DoD defines as data and how this is used to generate information and intelligence. Armed with the understanding that U.S. adversaries and competitors are waging IW, this section outlines the basics of how DoD processes data.

DoD highlights in its Data Strategy that “data is a high-interest commodity and must be leveraged in a way that brings both immediate and lasting military advantage.”<sup>61</sup> Joint Publication (JP) 2-0 highlights that raw data must be collected and by itself may not be relevant or useful. As JP 2-0 further illustrates that information consumed solely by itself may be utilized by a commander, but is not of much use for decision dominance. When related to the operating environment and considered in the light of past experience, however, it gives rise to a new understanding of the information, which may be termed *intelligence*.<sup>62</sup> The intelligence directorate enriches information by collecting national tactical means to answer a commander’s requirements, enabling decision dominance. DoD made information the seventh joint function in 2017 based on 2016 guidance first established in Joint Publication 1, “Operations in the Information Environment (IE).”<sup>63</sup>

Publicly available information (PAI) is information available on the open Internet and it plays an important role in IW/IO. DoD Directive 3115.18, “DoD Access to and Use of PAI,” issued in 2019, outlines the lawful and appropriate access to “obtain, and use PAI to plan, inform, enable, execute, and support the full spectrum of DoD missions.”<sup>64</sup> While new directives are important, old directives have not always been updated, causing confusion and gaps in strategy implementation. The U.S. Intelligence Community (IC) is flush with data; however, it is generally just white noise. Because of the definitional chaos of IO,<sup>65</sup> and the silo effect of data, different U.S. agencies approach IWIO differently and are often at odds with one another. Different units across all branches of the military often look at the same data for different issues and do not share the information across the DoD. In many instances, different military organizations are buying the same data from companies under different contracts for each organization. In other words, there is such a disunity of approach in data collection because DoD has not created a data governance entity to manage data acquisition from private industry and make it available across the force. DoD has put the onus on components to develop and implement their own data acquisition plans.<sup>66</sup> Furthermore, if DoD had a data lake that housed curated, publicly and commercially available information, which was available to its components, it would drastically reduce redundant data as a service contracts. This situation is one of the reasons the U.S. is behind the curve relative to China concerning the information domain and battlespace. This strategic adversary has clear conceptual approaches to influence operations, and has a more centralized or unified approach to information warfare and intelligence collection than does the U.S..<sup>67</sup> Thus, a more unified approach will help connect the dots with the U.S.’ collected data. It should be noted that the IC has the data at hand but does not always efficiently utilize the data to achieve its ends. As the U.S. plans for future data acquisition it needs to follow its adversaries’ lead in tracking narratives in the languages in which they are communicating and bringing on language and cultural experts who understand the nuances of those narratives.

## LACK OF A UNIFIED APPROACH

DoD understands the challenges of IW and has developed numerous policies to attempt to address them with the end state of achieving information advantage.<sup>68</sup> However, these new

policies failed to provide guidance that would benefit DoD organizations and military branches in the twenty-first century. Despite the existing elements of known national power, diplomacy, information, military, and the economy (DIME), and the aforementioned new policies for DoD, the military branches have developed their own approaches that are not synchronized. The term “IW” is also a point of contention—DoD prefers the term (IO), which encompasses a host of information-related capabilities (IRCs).

DoD has published Joint Publication (JP) 3-13, “Information Operations,” in 2012 and updated it again in 2014. The definition of IO outlined in JP 3-13 is “the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own.”<sup>69</sup> JP 3-13 further discusses that, after analyzing a target audience, desired effects can be accomplished through various means, including DIME actions. Here, the lack of a unified approach becomes apparent as these IRCs are managed separately at the joint level and across all military branches. For context, IRC capabilities can include but are not limited to personnel from the electronic warfare (EW), cyberspace operations (CO), military information support operations (MISO), civil-military operations (CMO), military deception (MILDEC), intelligence, and public affairs (PA) communities.<sup>70</sup>

All the communities mentioned above have developed their own guidance over time, executed it with various authorities, and achieved varying degrees of success. Some of these capabilities are nascent (i.e., cyber), and others have a long tradition (i.e., MILDEC). Historically, it is challenging for DoD to synchronize all these capabilities beyond incorporating them for a specific operation. However, the U.S. Congress has noticed that the environment has changed and identified gaps in its understanding of combating the *shaping operations* U.S. adversaries are conducting within the information environment.

To summarize, the U.S. is behind its strategic near-peer competitors, specifically China, due to the lack of a clearly implemented and unified approach, definitional chaos within the information environment, and inefficient utilization of evolving data and information into intelligence. With the understanding of Chinese influence operations and an illustration of the precise reasons the U.S. is behind its strategic adversaries based on DoD doctrine and implementation, what is to be done?

## POLICY RECOMMENDATIONS AND DISCUSSION

The first and most obvious policy recommendation is that the U.S. needs to form a centralized, unified approach dedicated to data, intelligence, and IW. This has already been achieved by the CCP. Although there are some in the U.S. who may oppose the creation of such a plan, this article demonstrates why it is a strategic necessity. The U.S. is losing because of its inability to turn data into operational intelligence and its lack of human capital allocation regarding IW. This gives its adversaries the strategic advantage. What is not necessarily needed is a

centralized entity to develop a unified approach. Rather, it is a unified approach based on policy across departments and within a unified command structure.

Existing institutions may provide the backbone from which to consolidate and then disseminate a unified approach to IW. Sue Gordon and Eric Rosenbach argue in *Foreign Affairs* that the Cybersecurity and Infrastructure Security Agency should become the center of gravity for domestic cybersecurity operations.<sup>71</sup> Additionally, they argue that USCYBERCOM ought to be realigned and re-envisioned into something approaching the U.S. Special Operations Command (USSOCOM). In a similar vein, Lieutenant General Timothy D. Haugh, Lieutenant Colonel Nicholas J. Hall, and Major Eugene H. Fan argue that this new information environment requires “tight partnerships among all elements of the DoD, the interagency, and our coalition partners, driving a shift in the weight of effort from preparing for conflict to competing now.” They continue, “We do not need a new approach to command and control, but a new framework that both materially creates the awareness among, and organizes the horizontal coordination of, organizations across the continuum of cooperation, competition, and conflict.”<sup>72</sup> Regardless of whether a unified approach creates a new entity or reenergizes current entities with new authorizations to handle all aspects of IWIO, this is the first step to help the U.S. counter IWIO by adversaries. It is currently unclear if the upcoming redefinition of terms by the Army, and its switch to using information advantage rather than information operations, as recently noted by Ross, will help or hinder the operational chaos produced by the terminology.<sup>73</sup>

Secondly, once a unified approach is defined, the U.S. needs to develop clear operationalizations and definitions for its information operations and strategic approaches. These concepts need to be clearly codified and implemented across the board, intra- and interagency. Once this is done, it may be necessary to go on the IW offensive. The U.S. needs to set the narrative in several key areas in an assertive way, using digital and social media in a fashion similar to how Radio Free Europe was used in the Cold War to communicate pro-democratic and anti-communist messages to thousands of individuals living behind the Iron Curtain.<sup>74</sup> The advantages and strengths of democracy, democratic participation, and respect for human rights need to lead the agenda-setting program of the U.S..

Currently, the U.S. is playing defense concerning the democratic narrative and, in fact, is generally reactive in response to disinformation and propaganda. There is almost no chance of winning the influence war within the Chinese space if the U.S. does not utilize successful tactics. Justin Sherman explains in a prior article for CDR that the Chinese have built out “variously undemocratic practices, such as online censorship, using digital technologies.”<sup>75</sup> However, he also notes that digital authoritarianism affects the international arena, and U.S. national security directly, by allowing authoritarian regimes to consolidate power, encouraging the global diffusion of digital surveillance and propagating the idea of Internet sovereignty, thereby potentially avoiding U.S. deterrence strategies.<sup>76</sup> Thus, authoritarian spaces control the information environment and, conversely, the information environment helps proffer authoritarianism.<sup>77</sup> Playing constant defense is a poor strategy and has been largely unsuccessful for

the U.S. Our near-peer competitors' sophistication demands the return to strategic offense in the information environment.

Furthermore, the U.S. must strengthen its defenses. For instance, U.S. policy typically does not allow for individuals within the IC or IWIO domains to engage with fake accounts, bots, or organized campaigns aimed at the U.S. citizenry. In fact, according to Major Jessica Dawson, "The result of this is that there is no agency within the Army charged with understanding the ways in which U.S. adversaries can manipulate the domestic information warfare space... [T]he U.S. Army is unable to assess or respond to threats in the social media space."<sup>78</sup> Although it may draw more attention to these accounts and issues, which the U.S. typically discourages, counter-attacking or taking the offensive may surprise Chinese information operatives. If done in a sophisticated manner, U.S. intervention into these spaces may quickly throw its adversaries into an emotive state, which could derail their policy. The action would also signal a policy and strategic culture shift in the U.S., which could help reassert U.S. dominance in this information space, forcing adversaries to play its game, rather than vice versa.

Additionally, U.S. near-peer competitors use popular influencers to their strategic and cultural advantage.<sup>79</sup> China pushes out influencers targeting its own population, and it hires Western influencers to target the West. In fact, China targets its own population through data-driven analytics to exert domestic control.<sup>80</sup> The U.S. could use a similar methodology against China and foreign adversaries as well, without violating U.S. law, military norms, or democratic codes of conduct. Instead of shutting down DoD military influencers, the U.S. could help them expand to combat Chinese IW/IO. Military members not on TikTok could be used to counter CCP efforts stateside by explaining why they are not on the platform. Active social media influence by exceptionally talented individuals could act as an IWIO deterrence. As Morin states, domestic IIOs would be targeted toward adversarial IIOs and seek to reduce "the viewing of an adversary's IIO content."<sup>81</sup>

As the digital age progresses and the information environment becomes a clearinghouse for great power conflict, the U.S. needs to engage this domain strategically and tactically. It can do so by setting its own agenda in this space, while also remaining dedicated to liberal democracy.<sup>82</sup> As noted earlier, Chinese IWIO strategies focus on active offense at all times; there is no difference in their peacetime versus conflict strategies. To compete within this space, the U.S. needs to choose wisely which elements of IW should be used offensively. David Morin explains that incorporating Information Influence Operations (IIOs) into USCYBERCOM tactics "would allow [the U.S.] to effectively guide perception and even shape the targeted population's perception of reality, if effectively conducted."<sup>83</sup>

The U.S. should also consider its strategic use of the Internet in multiple areas. In terms of web presence on the domestic front, all government sites should be technologically savvy and well-integrated with social media platforms to help bolster government legitimacy among generations that are increasingly technologically-oriented. Additionally, the government should

consider policies and procedures that would enable the exclusion of bad foreign actors, companies, and advertisement funding.<sup>84</sup> If the U.S. were to disrupt and deny foreign actors' abilities to disseminate influence operations actively through U.S. companies and Internet platforms, it would begin the process of active defense.

Due to China's regime structure, the U.S. and China are playing two separate games with separate rule books. China is directly targeting U.S. civilian interests, has deep pockets to spread its message, and has control of its own media. It can even pay U.S. companies for advertising space, whereas the U.S. denotes limited funds to IW/IO and does not focus on the same targets. The U.S. should utilize the Internet in a manner that aggressively goes on the offensive on behalf of American citizens. This will likely encourage China to complain that the U.S. has caused offense on the international stage. However, it is long past time for the U.S. to demonstrate clearly its IWIO capabilities and impose costs on its adversaries in their attempts to disrupt American society.

For this to be effective, the U.S. must engage in IWIO through a whole-of-society approach, but one that plays out much differently than the centrally directed, coercive manner of authoritarian regimes. Although this article argues that DoD needs a centralized division and strategy for IW/IO to compete with China, it also needs a decentralized environment which allows for all sectors of U.S. society to engage in the game by their own initiative. This would include defense, entertainment, schools, and the citizenry, as imagined by researchers Cristina-Elena Ivan, Irena Chiru, and Rubén Arcos.<sup>85</sup> The U.S. needs an overarching message to disseminate and, to be effective, it has to come from multiple segments of society. As a part of this whole-of-society approach, U.S. companies will need to play an active role. As Dawson notes, technology companies such as Facebook and Google are ungoverned, unrestricted spaces; as such, they pose a significant security risk for the United States, especially concerning data and intelligence for IOs.<sup>86</sup>

The focus of technology platforms should be to prevent U.S. adversaries from co-opting the platform to wage a disinformation campaign against the U.S. citizenry. Most especially, as Major Dawson insists, "The U.S. must recognize the current advertising economy as enabling and profiting from information warfare being waged on its citizens and address the threat."<sup>87</sup> While we must address the fight the adversaries put in front of us, we win, not by trying to play their game, but by playing ours effectively.🛡️

## **DISCLAIMER**

The views presented are those of the author(s) and do not necessarily represent the views of DoD or its components.



## NOTES

1. Lily Hay Newman, “It’s Time to Get Real About TikTok’s Risks,” *Wired Magazine* (September 6, 2022), <https://www.wired.com/story/tiktok-national-security-threat-why/>.
2. Lieutenant Colonel Robert J. Ross, PhD, “Information Advantage Activities: A Concept for the Application of Capabilities and Operational Art during Multi-Domain Operations,” *The Cyber Defense Review* (Fall 2021): 63.
3. Seth G. Jones, “Going on the Offensive: A U.S. Strategy to Combat Russian Information Warfare,” CSIS (October 1, 2018) <https://www.csis.org/analysis/going-offensive-us-strategy-combat-russian-information-warfare>.
4. Harleen Gambhir, “The Virtual Caliphate: ISIS’s Information Warfare,” *Institute for the Study of War* (December 2016), <https://understandingwar.org/sites/default/files/ISW%20The%20Virtual%20Caliphate%20Gambhir%202016.pdf>
5. Lieutenant Colonel Gregory M. Tomlin, PhD, “The Case for an Information Warfighting Function,” *Military Review* (September–October 2021): 91, <https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/SO-21/tomlin-info/tomlin.pdf>.
6. P Jack Kiesler, “A Next Generation National Information Operations Strategy and Architecture,” Paper, Belfer Center for Science and International Affairs, Harvard Kennedy School (September 13, 2021), <https://www.belfercenter.org/publication/next-generation-national-information-operations-strategy-and-architecture>.
7. Kiesler, A Next Generation, 8/36.
8. Lieutenant General Stephen G. Fogarty and Colonel (Ret.) Bryan N. Sparling, “Enabling the Army in an Era of Information Warfare,” *The Cyber Defense Review* (Summer 2020): 18.
9. Connor Cunningham, “A Russian Federation Information Warfare Primer,” The Henry M. Jackson School of International Studies, University of Washington (November 12, 2020), <https://jsis.washington.edu/news/a-russian-federation-information-warfare-primer/>.
10. Christopher Whyte, A. Trevor Thrall, and Brian M. Mazanec, “Introduction” in *Information Warfare in the Age of Cyber Conflict*, edited by Christopher Whyte, A. Trevor Thrall, and Brian M. Mazanec, 1–11.
11. See DOD *Dictionary of Military and Associated Terms*, (as of January 2021), and DOD Directive 3600.01, *Information Operations (IO)*, (May 2, 2013, incorporating Change 1, May 4, 2017), and GAO, *Information Operations: DOD Should Improve Leadership and Integration Efforts*, GAO-20-51SU (Washington, D.C., October 18, 2019), and Congressional Research Service, *Information Warfare: Issues for Congress*, R45142 (updated March 5, 2018).
12. Scott D. McDonald, Brock Jones, and Jason M. Frazee, “PHASE ZERO: How China Exploits It, Why the United States Does Not,” *U.S. Naval War College Review* 65, 3 (Summer 2012) <https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1471&context=nwc-review>.
13. Justin Sherman, “Digital Authoritarianism and Implications for US National Security,” *The Cyber Defense Review* (Winter 2021): 108–109.
14. Christopher Whyte, A. Trevor Thrall, and Brian M. Mazanec, eds., *Information Warfare in the Age of Cyber Conflict* (New York: Routledge, 2021), 237.
15. Catherine A. Theohary, “Information Warfare: Issues for Congress,” *Congressional Research Service Report* (2018): 1.
16. Mark Pomerleau, “Why is the United States losing the information war?” *C4ISRNet* (October 2020): 5, <https://www.c4isrnet.com/information-warfare/2020/10/05/why-is-the-united-states-losing-the-information-war/>.
17. Pomerleau, “Why is the United States?”
18. Manuel Cereijo, “China and Cuba and Information Warfare (IW): Signals Intelligence (SIGINT), Electronic Warfare (EW) and Cyberwarfare,” [www.lanuevacuba.com/archivo/manuel-cereijo-123.htm](http://www.lanuevacuba.com/archivo/manuel-cereijo-123.htm).
19. Theohary, *Information Warfare*.
20. J. Yin and P.M. Taylor, “Information Operations from an Asian Perspective: A Comparative Analysis,” *Journal of Information Warfare* 7, no. 1 (2008), 3.
21. Yin and Taylor, “Information Operations, 3.
22. Larry M. Wortzel, “The Chinese People’s Liberation Army and Information Warfare,” *US Army War College, Monographs, Books, and Publications* (2014): 30, <https://press.armywarcollege.edu/monographs/506>.
23. J. You, “China’s Emerging National Defence Strategy,” *China Brief* 4, no. 23 (2004): 5–7, [http://jamestown.org/china\\_brief/article.php?issue\\_id=3152](http://jamestown.org/china_brief/article.php?issue_id=3152).
24. Wortzel, “The Chinese People’s,” 13–15.
25. Watts, “China’s Propaganda.” <https://www.wired.com/2016/12/obama-russia-hacking-sanctions-diplomats/>.

## NOTES

26. Renee Diresta et al., “Telling China’s Story: The Chinese Community Party’s Campaign to Shape Global Narratives,” Stanford Cyber Policy Center, Stanford Internet Observatory (2020): 14.
27. Yin and Taylor, “Information Operations,” 3-4.
28. Elsa B. Kania and John K. Costello, “The Strategic Support Force and the Future of Chinese Information Operations,” *The Cyber Defense Review* 3, no. 1 (2018): 106; Kania and Costello, “The Strategic Support Force,” 116.
29. Yin and Taylor, “Information Operations,” 4.
30. Timothy Thomas, “The Chinese Way of War: How Has it Changed?” The MITRE Corporation, sponsored by U.S. Army Futures and Concepts Center (2020): 47.
31. Kania and Costello, “The Strategic Support Force,” 111; Wortzel, “The Chinese People’s,” 16.
32. Kania and Costello, “The Strategic Support Force,” 112.
33. Lili Turner and Nirit Hinkis, “Chinese State Media’s Global Influencer Operation,” Miburo (now part of the Digital Threat Analysis Center), (January 31, 2022) <https://miburo.substack.com/p/csm-influencer-ops-1>
34. Turner and Hinkis, “Chinese State Media’s.”
35. Yin and Taylor, “Information Operations,” 5.
36. Ben Smith, “Meet Zhao Lijian, The Chinese Diplomat Who Got Promoted for Trolling the US on Twitter,” BuzzFeed News (December 2, 2019), <https://www.buzzfeednews.com/article/bensmith/zhao-lijian-china-twitter>.
37. Maddalena Procopio, “The Effectiveness of Confucius Institutes as a Tool of China’s Soft Power in South Africa,” *African East-Asian Affairs* (2015): 1-2.
38. Reuben L. Lifuka, “Corruption in the Zambian Construction Sector: The China Factor,” The Hoover Institution, *China’s Sharp Power in Africa* (2021): 6, [https://www.hoover.org/sites/default/files/research/docs/lifuka\\_webreadypdf.pdf](https://www.hoover.org/sites/default/files/research/docs/lifuka_webreadypdf.pdf).
39. Lifuka, “Corruption,” 8.
40. Watts, “China’s Propaganda.”
41. Wortzel, “The Chinese People’s,” 33.
42. Doug Livermore, “China’s ‘Three Warfares’ in Theory and Practice in the South China Sea,” *Georgetown Security Studies Review*, March 25, 2018, <https://georgetownsecuritystudiesreview.org/2018/03/25/chinas-three-warfares-in-theory-and-practice-in-the-south-china-sea/>.
43. Yin and Taylor, “Information Operations,” 7.
44. DiResta et al., “Telling China’s Story,” 9; Wortzel, “The Chinese People’s,” 32.
45. Alex Joske, “The Party Speaks for You: Foreign Interference and the Chinese Communist Party’s United Front System,” Australian Strategic Policy Institute (June 9, 2020), <https://www.aspi.org.au/report/party-speaks-you>; Wortzel, “The Chinese People’s,” 32.
46. Scott W. Harold, Nathan Beauchamp-Mustafaga, and Jeffrey W. Hornung, “Chinese Disinformation Efforts on Social Media,” RAND Corporation (2021): 21.
47. DiResta et al., “Telling China’s Story,” 3, 7.
48. Theohary, *Information Warfare*, 12.
49. DiResta et al., “Telling China’s Story,” 39.
50. Ivan, Chiru, and Arcos, “A Whole of Society,” 498; Lin, “On the Organization,” 167.
51. Ivan, Chiru, and Arcos, “A Whole of Society,” 495; See also Chris Dougherty, “Confronting Chaos: A New Concept for Information Advantage,” *War on the Rocks*, September 9, 2021, <https://warontherocks.com/2021/09/confronting-chaos-a-new-concept-for-information-advantage/>.
52. Herbert Lin, “Doctrinal Confusion and Cultural Dysfunction in DoD,” *The Cyber Defense Review* 5, no. 2 (2020), 90.
53. Theohary *Information Warfare*, 7.
54. Lin, “Doctrinal Confusion,” 100.
55. Whyte et al., *Information Warfare*, 2.
56. FM 3-13: *Information Operations*, Department of the Army, Headquarters (December 2016), 2-1, <http://www.apd.army.mil>; Zac Rogers, “The Promise of Strategic Gain in the Digital Information Age: What Happened?” *Cyber Defense Review* 6, no.1, (Winter 2021): 87.



## NOTES

57. *Information Operations*, Joint Chiefs of Staff, Joint Publication 3-13 (November 27, 2012): vii.
58. A. Wanless and J. Pammet, "How Do You Define a Problem Like Influence?" *Journal of Information Warfare* 18, no. 3 (Winter 2019): 7.
59. Whyte et al., *Information Warfare*, 237.
60. Wanless and Pammet, "How Do You Define a Problem Like Influence?" 9.
61. DOD, *Executive Summary*.
62. Joint Chiefs of Staff, *Joint Publication 2-0: Joint Intelligence* (October 22, 2013).
63. Joint Chiefs of Staff, *Joint Publication 1: Doctrine for the Armed Forces of the United States* (March 25, 2013), [https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jpl\\_ch1.pdf](https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jpl_ch1.pdf).
64. DOD, *DOD Access to*.
65. Wanless, A. and J. Pammet, "How Do You Define a Problem Like Influence?" *Journal of Information Warfare* 18, no. 3 (Winter 2019): 2.
66. DOD, *Executive Summary*.
67. See Tashev Blagovest, Lieutenant Colonel Michael Purcell, and Major Brian McLaughlin, "Russia's Information Warfare: Exploring the Cognitive Dimension," *MCU Journal* 10, no. 2 (2019): 133.
68. See GAO, "Information Operations: DOD Should Improve Leadership and Integration Efforts," GAO-20-51SU (October 2019) for a complete breakdown of terms the DOD uses.
69. Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations* (2014).
70. *Ibid*.
71. Sue Gordon and Eric Rosenback, "America's Cyber-Reckoning: How to Fix a Failing Strategy," *Foreign Affairs* 101, no.1 (2022): 10-20.
72. Lieutenant General Timothy D. Haugh, Lieutenant Colonel Nicholas J. Hall, and Major Eugene H. Fan, "16th Air Force and Convergence for the Information War," *The Cyber Defense Review* 5, no.1(2020): 41.
73. Robert J. Ross, "Information Advantage Activities: A Concept for the Application of Capabilities and Operational Art during Multi-Domain Operations," *The Cyber Defense Review*, 6 no. 4 (Fall 2021): 63-73.
74. McCauley, Russian Influence Campaigns, 475; See also, Fletcher Schoen and Christopher J. Lamb, *Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Difference*, Institute for National Strategic Studies Strategic Perspectives, no. 11 (Washington, DC: National Defense University Press, 2012): 12-97.
75. Sherman, "Digital Authoritarianism," 107.
76. *Ibid*.
77. *Ibid*.
78. Jessica Dawson, "Microtargeting as Information Warfare," *The Cyber Defense Review* 6, no. 1 (2021): 63-79.
79. David Morin, "Information Influence Operations: The Future of Information Dominance," *The Cyber Defense Review* 6, no. 1 (2021): 136.
80. Dawson, "Microtargeting as Information Warfare," 68.
81. Morin, "Information Influence Operations," 137.
82. Laura Rosenberger and Lindsay Gorman, "How Democracies Can Win the Information Contest," *The Washington Quarterly* 43 no. 2 (2020): 75-96.
83. Morin, "Information Influence Operations," 136.
84. Dawson, "Microtargeting as Information Warfare."
85. Ivan, Chiru, and Arcos, "A Whole of Society."
86. Dawson, "Microtargeting as Information Warfare," 64.
87. *Ibid*.



# The Ukrainian Information and Cyber War

---

Chris Bronk  
Gabriel Collins  
Dan S. Wallach

## ABSTRACT

*Information and cyber action have been important but ancillary components of the Ukraine war since its outbreak on February 24, 2022. We offer a set of observations:*

- ◆ *A form of cyber conflict has emerged in which Russia often attempts to aggressively deny service or purloin information, while Ukraine and its allies often blunt the attacks;*
- ◆ *Communications security for Russian forces from the tactical- to theater-level has frequently failed, often with disastrous consequences, as signals intelligence information has been employed to target military command echelons;*
- ◆ *Unmanned aircraft have come to occupy a critical intelligence and air support function for Ukraine, although Russia is increasingly able to employ drones as well;*
- ◆ *Intelligence support from the West to Ukraine appears highly significant and useful, possibly substantially shaping Ukrainian strategy and tactics;*
- ◆ *The infrastructure and technical expertise of large tech firms such as Google, Microsoft, and SpaceX also helped Ukraine stay abreast of the Russian cyber threats; and*
- ◆ *Propaganda operations by Ukraine have had tremendous reach in Europe and continue to elicit support, while those of Russia have been largely inward-facing and designed to shore up support for the war among the Russian public.*

*We also consider what cyber tools and effects might be employed as the war continues.*

© 2023 Chris Bronk, Gabriel Collins, Dan S. Wallach



**Chris Bronk** is an associate professor with tenure, in the Hobby School of Public Affairs at the University of Houston. An academic-practitioner with manifold interests, he directed UH's graduate cybersecurity program and was faculty in the College of Technology. Bronk publishes interdisciplinary research at the intersection of technology and policy, frequently in collaboration with undergraduate and graduate students. He published a book, *Cyber Threat: The Rise of Information Geopolitics in U.S. National Security* and has engaged in scholarship on Internet censorship, online surveillance, border security, public diplomacy, organization information technology, and critical infrastructure protection. His academic work has been sponsored by the National Science Foundation, Department of Energy, Department of Defense, Department of Homeland Security, Deloitte, Microsoft, and AT&T. He has served as both a Foreign Service Officer and Senior Advisor at the U.S. Department of State, managing the deployment of its enterprise wiki, Diplopedia, which remains in use today.

## INTRODUCTION

In a matter of months the Ukraine war will enter its third year.<sup>1</sup> At the outset of hostilities, many figured that Moscow's bold gamble to storm Ukraine by force and seize the country's capital would succeed as similar operations did in Hungary (1956), Czechoslovakia (1968), and Afghanistan (1979). Before this invasion commenced, no one knew how effectively Ukraine's military would fight. Once the shooting started, we learned that Ukraine's military was indeed motivated and fought well. With the war now marked by several major shifts on the battlefield, we believe it is wise to consider less tangible forms of action that have occurred, and how they may shape future fighting. There have been some real surprises in this war including in cyber and information operations. An accounting of both is provided here, as well as how information and cyber action may influence the outcome of this war, whether it ends in a negotiated settlement, capitulation, or collapse.

The unexpected turns of the Ukraine war have yielded observations that cover communications, logistics, operational art, and a variety of other topics, including information and computation. From propaganda to air defense, this war is one in which the proliferation of computation and information technologies has produced a battlefield environment vastly different from earlier conventional engagements of the post-Cold War period. We will cover a range of issues, some more briefly than others, and we obviously are unaware of the classified operations undertaken by the belligerents and their supporters. Early on, we saw publicly reported snippets alluding to US information sharing,<sup>2</sup> and of Chinese cyber operations supporting Russia,<sup>3</sup> and other reports over time that suggest that the information battle is often as surprising as the kinetic conflict.



**Gabriel Collins** is the Baker Botts Fellow in Energy and Environmental Regulatory Affairs at Rice University's Baker Institute for Public Policy's Center for Energy Studies and a Senior Visiting Research Fellow at the Oxford Institute for Energy Studies. At Baker, he co-heads the Program on Energy & Geopolitics in Eurasia. Gabe's research portfolio covers a range of energy, water, and national security issues. Collins received his B.A. from Princeton University and a J.D. from the University of Michigan Law School. He was a member of the China Maritime Studies Institute team, is still teased by his family for joining a commodity hedge fund in 2008, has practiced law, and is now thrilled to be at the premier global energy & resource think-tank. Gabe is a Permian Basin native, reads Mandarin and Russian well enough to use them in his research, speaks each just well enough to get himself in trouble, and is licensed to practice law in Texas.

## THE CYBERS

Many observers were surprised when hostilities commenced at the absence of a crippling cyberattack on the Ukrainian telecommunications infrastructure. In the earliest hours of fighting, the world watched as armored columns streamed by Ukrainian border checkpoint cameras that passed their images over the internet unimpeded. Ukraine stayed online as Russia invaded. Both Russian and US military doctrine now include the use of cyber effects alongside traditional “kinetic” warfare. We know the Russians tried to cause cyber effects, including Russian attacks on ViaSat’s modems,<sup>4</sup> which were mitigated by new connectivity via SpaceX’s StarLink orbital information network. Subsequent Russian attacks on StarLink were unsuccessful.<sup>5</sup> Efforts notwithstanding, as of the date of this article, Russia has failed to close off Ukraine from cyberspace.

The failure of Russia’s early-on cyber operations clearly played in Ukraine’s favor, with Ukraine maintaining both internal communications and the wherewithal to disseminate to the world, whether through traditional news channels or through YouTube, TikTok, and other online forms of media. Also, while we would not know until later, the US had established secure communications from Ukraine to the US military’s European Command.<sup>6</sup>

A related surprise was the absence of effects from massive cyberattacks aimed at Ukraine’s critical infrastructure. In 2015 and again in 2016, Russia conducted against Ukraine some of the cleverest hacks of electricity infrastructure seen anywhere heretofore.<sup>7</sup> A year later, Russia launched Petya/NotPetya, a massively destructive set of false ransomware attacks against Ukrainian government and commercial targets. Petya had a far-reaching impact on firms beyond Ukraine as well, which was severely destructive of international cargo carrier Maersk.<sup>8</sup> We have yet to see this magnitude of destructive cyberattack against Ukraine, possibly because such attacks were thwarted, or because of rapid repair.



**Dan S. Wallach** is a Professor in the Departments of Computer Science and Electrical and Computer Engineering and a Rice Scholar at the Baker Institute for Public Policy at Rice University in Houston, Texas. His research considers a variety of computer security topics, including electronic voting, Internet censorship, and security issues in web browsers, servers, and smartphone applications. Wallach served on the Air Force Science Advisory Board (2011-2015) and as a member of the U.S. Election Assistance Commission's Technical Guidelines Development Committee (2019+). He will soon be on leave from Rice to serve as a DARPA program manager.

Before the war, there was an assumption that cyber action would be at the center of any Russian kinetic campaign.<sup>9</sup> This was the case when Russia attacked Georgia in 2008. But now we proffer a new hypothesis: that Russia went for broke with cyber action in its earlier campaigns in Ukraine (2012) and in Syria (2015). Lessons learned (by Ukraine and others) have been applied in Ukraine in 2022, blunting the impact of more recent cyberattacks. For example, IBM's Security X-Force group has documented "at least six" Russian campaigns targeting Ukraine and has published a list of security indicators to help thwart them. Of course, there have been many other documented cyberattacks, both before and after the invasion began.<sup>10</sup> This suggests that cyber's role in Russian military planning is a form of "icing on the cake." It is nice to have, but hardly a prerequisite for launching a kinetic attack.

In addition, there is ample evidence that the global IT industry in general, and Ukraine's IT community in particular, has been better prepared for destructive Russian cyberattacks than before. Nonetheless, Microsoft asserts with a great degree of confidence that during this war Russia has launched "destructive cyberattacks within Ukraine, network penetration and espionage outside Ukraine, and cyber influence operations targeting people around the world."<sup>11</sup> While some experts feel Microsoft's claims are overblown,<sup>12</sup> the pattern of cyberattacks against Ukraine being discovered and mitigated seems clear. The Defense Department's U.S. Cyber Command (USCYBERCOM) made contributions by releasing cyber indicators of compromise valuable to the Ukrainians and available by Pastebin to all.<sup>13</sup>

At the one-year mark in fighting, summaries on the cyber conflict by two of the United States's largest IT companies, Microsoft, and Google (through its Mandiant subsidiary) showed a more nuanced picture. Both firms actively support cyber defense actions to protect Ukrainian information resources as well as those of nations actively supporting the Ukrainians. These com-

panies generate a massive amount of data regarding malicious activity in cyberspace. Google's visibility into cybersecurity matters was greatly augmented when it acquired Mandiant, a dominant commercial response and intelligence entity. Microsoft, with its massive global software install base also enjoys unique visibility in the Ukraine war's cyber conflict. Their assessments both deserve attention.

Google collected and confirmed a 250 percent increase in "phishing" email activity designed to compromise Ukraine's computer systems and a 300 percent increase in NATO member states.<sup>14</sup> Destructive cyber activity by Russian GRU (military intelligence) operatives have largely been confined to "wiper" attacks designed to delete data as well as cryptographic ransomware ones that deny data access. Interestingly, there has not been a major spillover of destructive malware outside of Ukraine as occurred with GRU's 2017 *NotPetya* campaign.<sup>15</sup>

Microsoft's report at the one-year mark similarly assesses Russia's cyber operations, pointing the finger at Russia for a "ransomware operation against the transportation sector in Poland, a NATO member and key logistical hub for Ukraine-bound supplies." In addition to destructive cyber activity, Microsoft states that the GRU, "potentially compromised a separate Polish transportation sector firm, and later increased reconnaissance against NATO-affiliated organizations, suggesting an intent to conduct future intrusions against this target set." The most frequently hacked organizations in Ukraine are in its government, communications, and energy sectors.<sup>16</sup> That Microsoft has granular data which it has shared about Poland's spillover position sends an important message to NATO. While the attacks, thus far, against Poland have not been egregiously startling, that they occurred at all reinforces a norm that cyberattack is not the same as the kinetic variety. One preliminary hypothesis is that Moscow might in fact believe that cyber actions which cause serious economic, and potentially, physical damage, might not trigger the Article 5 collective defense threshold, or that Russia's cyberattacks at most would trigger a "proportionate response."

We doubt the explanation is effective Russian or Ukrainian battlefield cyber action, which in any event is not making the news. The Fancy Bear/APT28 Russian cyber group, "believed by US intelligence officials to work primarily on behalf of the GRU," has been a significant presence in cyber operations against Ukraine since 2014.<sup>17</sup> Known for its résumé of destructive cyber-attacks, the GRU's cyber forces have attempted to attack Ukrainian infrastructure, but at least one operation against an industrial control system in the country was identified before significant damage occurred.<sup>18</sup> Among combat information systems, Russia has had little visible success in hacking Ukraine's Integrated Air Defense System similar to what Israel achieved with its strike on Syria's nuclear facility in 2007. This does not mean cyberspace-collected intelligence hasn't been effective. Targeting of a Ukrainian precision-guided strike on the Russian barracks at Makiivka on January 1, 2023, likely was enabled by concentrated mobile phone use by the Russian soldiers housed there.<sup>19</sup>

Other academics have produced a considerable volume of writing on the Ukraine war's cy-



ber component. Kenneth Geers draws upon his experience as a cybersecurity researcher in Ukraine in his overview of Russian cyberattacks against Ukraine, both before and during the invasion.<sup>20</sup> Kristen Eichensehr notes the limited role taken of cyber operations in the Ukraine war and considers the ramifications for this on international law.<sup>21</sup> Nadiya Kostyuk and Erike Gartzke present a statistical analysis of 11 years of recent military campaigns and find that “cyber operations are rarely used as either complements to or substitutes for conventional military operations.”<sup>22</sup> Joshua Rovner’s observations track ours, including the seeming importance of cyberattacks as part of a military campaign and the corresponding absence of Russian effectiveness.<sup>23</sup> Cyberattacks *should* be particularly effective for *sabotage*, damaging or degrading both cyber and physical assets, without the risks normally associated with human saboteurs, who might be captured or killed. From what we see, their primary use in Ukraine is for *espionage* (e.g., exfiltrating secrets/signals intelligence). Lastly, Gavin Wilde examines how NATO and Russian military theorists view the role of cyberattacks as part of larger military campaigns, discussing a number of cyber failures in prior campaigns. He states:

The issue is less that Western observers might have overestimated Russia’s cyber potential in its war on Ukraine, more that they almost certainly underestimate the complexities and frictions which separate intent from execution, intensity from effect. Particularly in the still murky arena of information warfare, the chasm between theory and practice remains wide.<sup>24</sup>

Perhaps the most important takeaway on cyber activity in Ukraine’s nearly two-year-old war with Russia is that cyberattacks may only be a small part of the conflict. That said, we can see important developments in adjacent areas, including in computational information or propaganda operations as well as the collection of intelligence. Cyber is neither boon nor bust, but rather a piece of military capability that remains difficult for its users to calibrate and hardly an alternative to all other modes of force. It may hold true that, “cyber operations offer a novel instrument of power below the threshold of war, creating a new strategic space of competition,” in areas of non-military or hybrid conflict.<sup>25</sup> In major conflict, cyber operations are part of a larger mix of activity designed to produce military outcomes or alter opinion.

## **COMMUNICATION BREAKDOWN**

We expected Russia to do much to confuse and confound the Ukrainians with cyber action and with strategic and battlefield communications at the top of their target list. We did not anticipate a manifold breakdown in Russian communications among units moving into Ukraine and attempting to coordinate complex operational maneuvers in multiple thrusts across hundreds of kilometers of frontage.<sup>26</sup> We saw ample evidence of Russia not having secure communications at the tactical and operational level. Russian encrypted communications were an abysmal failure.<sup>27</sup> This was clear when a staff officer in the field had to report the death of his commander, Maj. Gen. Vitaly Gerasimov, to their headquarters in Tula, Russia. His request



for a secure line was rebuffed, as his commander stated that the encrypted telephones did not work. The message was intercepted and then shared with the world.<sup>28</sup>

Faced with nonsecure and dysfunctional battlefield communications, Russian commanders shifted to what did work—chiefly cellular telephones,<sup>29</sup> often operating on the Ukrainian phone network.<sup>30</sup> This allowed Ukraine access to these calls, some of which they have published, and of course, to geolocate those phones. In at least one instance, the tactic was used to target and kill a Russian general.<sup>31</sup> Conversely, we might have expected Russia to hack the Ukrainian cellular networks, giving them the same advantages—particularly when we have known for years that among other Russian electronic warfare capabilities,<sup>32</sup> Russian unmanned aerial vehicles (UAVs) are capable of acting as deceptive cellular base stations.<sup>33</sup> US cyber assistance may have helped blunt or defeat Russian cyberattacks in this arena,<sup>34</sup> and/or Ukrainian troop phone use may have grown more disciplined; for example, Ukrainian troops are instructed to walk 400 to 500 meters away from their position before using a phone.<sup>35</sup>

Some suggest that Russia has an advantage in keeping the Ukrainian cellular network operational, both for its own communications and to hack Ukrainian targets.<sup>36</sup> Certainly, quiet surveillance over Ukrainian communications could be advantageous to Russia's military. Cellular communications are still an important piece of tactical intelligence, not least for their importance to reconnaissance and attack by drone. Russia's narrower strategy now focusing only on Ukraine's East may make it easier to deploy Russia's electronic warfare systems,<sup>37</sup> and thereby degrade Ukraine's air defense radar and other communications with heavy and adaptive jamming in the radio frequency spectrum. This includes the remote operation of unmanned aerial vehicles (UAVs).

## DRONE HELL

In his study of military innovation, Max Boot reminds us that new weapons can remake the conduct of war.<sup>38</sup> Of import in the Ukraine war, perhaps more than any other, is unmanned aircraft. A lesson from the most recent Armenia-Azerbaijan conflict is that the side that masters the employment of drones (a.k.a. unmanned aerial vehicles) may hold a critical advantage.<sup>39</sup> Before fighting broke out, drones were identified as an important equalizer for Ukraine,<sup>40</sup> and this has proven accurate. Two forms of drones, the cheap quadcopter and the heavier medium-endurance UAV, have transformed the information picture that is battlefield situational awareness. Each deserves some attention.

Cheap quadcopters have made an incredible impact in tactical reconnaissance in the region surrounding the forward line of troops. For example, the widely available DJI Phantom 4 Pro offers tremendous observation capability with a 20 megapixel camera producing 4K video recorded or 1080p video live streamed, while operating at a distance of 10 kilometers, with an endurance of 30 minutes.<sup>41</sup> Fully equipped, the Phantom 4 Pro costs about \$2,000, or one-fortieth the cost of a Javelin fire-and-forget anti-tank missile. Given the prominent role of artillery

in the war, these cheap drones have radically improved battlefield situational awareness, targeting, and damage assessment. We have also seen videos from drones, either locally improvised in Ukraine by hobbyists or produced by the Ukrainian military's Aerorozvidka reconnaissance organization,<sup>42</sup> being used to drop grenades on tanks and other armored targets,<sup>43</sup> all deliverables that also carry propaganda value.

Also involved in strikes against Russian forces and infrastructure targets are Turkish-supplied Bayraktar TB2 UAVs. While the TB2 appears clunky next to US military UAVs, Ukraine has used them to great effect, both for surveillance and to launch missiles. The shift from manned aircraft to unmanned UAVs in reconnaissance and close air support already proved effective in Iraq and Afghanistan, but analysts were concerned about whether they would be as effective in areas with more sophisticated air search radars and electronic warfare. The answer appears to be that effectiveness is situational in nature. In essence, when the opponent has gaps in sensor and air-defense coverage—as Russian forces did during their sham-bolic early assault on Ukraine in 2022—larger strike and observation drones like the TB2 can operate more aggressively. But once the opponent elevates the quality of electronic warfare operations and brings kinetic air defenses (i.e. surface to air missiles or fighter aircraft) fully into play, the environment becomes far less permissible for a TB2-type UAV.<sup>44</sup> At the lower rungs of the UAV ecosystem (loitering munitions and smaller observation and strike drones), Russian and Ukrainian forces are engaged in a rapid Darwinian contest pitting Russian jammers against Ukrainian observers and attackers.<sup>45</sup>

Ukraine's drone warfare activities evolving substantially. Kyiv's forces have been availing themselves of improvements to range and quantity. Then-Ukrainian Defense Minister Oleksii Reznikov told Reuters in March 2023 that Ukraine is working with over 80 indigenous drone makers.<sup>46</sup> As it taps this diverse technical ecosystem, defense officials appear to show particular interest in long-ranged strike drones, including tests announced in December 2022 that allegedly involved a 1,000-km range strike drone. If production can be scaled up and especially, if Ukrainian manufacturers can obtain sufficient NATO support for a high-capability "drone parts bin," Kyiv could deploy a symmetrical answer to the Shahed drones Russia has been launching at targets across Ukraine for months.<sup>47</sup> Multiple drone attacks on Moscow during the summer of 2023 foreshadow what could evolve into a broader, higher intensity campaign more akin to the Houthi drone war against Saudi Arabia and the UAE in recent years.<sup>48</sup>

Coming months may also see qualitative increases in Ukrainian drone capability, potentially including the first combat use of networked drone swarms. Of particular note, the 24 February 2023 US military aid package to Ukraine included Anduril's Altius-600, launchable from many platforms, with a range exceeding 250 miles, and is capable of operating in a networked swarm.<sup>49</sup> Observers should also expect additional strikes on Russian energy and critical infrastructure in response to Moscow's targeting of Ukraine's power grid.<sup>50</sup> As the Ukrainian Air Force acquires F-16s, it may also (as Israel has) seek persistent anti-radiation

loitering munitions for air defense suppression and destruction missions. It is also likely that more intense and widespread drone-on-drone aerial combat will take place in Ukraine and that the country's east and south will effectively be a global laboratory for such activity.<sup>51</sup> The bottom line is that as the war heads into 2024, the drone space will combine creativity and innovation, while calling for greater industrial mass on the basis that while drones are game changing, they exert their most profound effects when deployed in large quantities.

## INTELLIGENCE AND THE INFORMATION WAR

Russia's supposedly pervasive penetration of Ukrainian political and economic structures failed at the most basic level to yield accurate intelligence about Kyiv's willingness to fight. Had the Russians received or accepted better information and been able to premise their assumptions on something closer to reality, they might have structured an entirely different attack plan and been more successful in meeting less ambitious goals than taking down Kyiv and much of the country in a matter of days. Putin reminds us that intelligence is fed to political leaders who often ignore or dismiss it due to their own cognitive blinders or ambitions.<sup>52</sup>

In the West, intelligence regarding the war has been abundant, accurate, and publicly disseminated. For example, the U.K.'s Ministry of Defense has been publishing daily summaries on its Facebook page. In the days prior to Russia entering Ukraine, American and British public statements accurately predicted Russian actions before they happened.<sup>53</sup> Demonstrably, Russia was unable to protect the confidentiality of its planning and deliberation process, with US intelligence operations having thoroughly penetrated Russia's political leadership, spying apparatus, and military.<sup>54</sup> Russian denials at the time proved false, damaging Russian credibility as to other statements they have made since, thereby bolstering the legitimacy of NATO information releases. While the US and its allies predictably have yet to disclose their sources or methods, the scope and breadth of their disclosures were certainly a surprise. "It doesn't have to be solid intelligence," one US official said. "It's more important to get out ahead of [the Russians], Putin specifically, before they do something."<sup>55</sup> This rapid dissemination represents a paradigm change in how intelligence is processed, leading to a variety of benefits—including reports that Russia delayed its own invasion timetable, which allowed NATO allies more time to coordinate response.

Relatively little has been written about cyber intelligence operations against Russia by Ukraine and its allies, although there have been suggestions that NATO forces have contributed targeting data for high-value targets such as munitions depots and command centers. Employment of HIMARS, an artillery rocket launcher, and its long-range (~90 km) guided rocket GLMRS,<sup>56</sup> have yielded spectacular results in destroying ammunition depots and command targets.<sup>57</sup> Such targeting information undoubtedly was cyber-enhanced, for example, by hacking and tracking cellular telephones or even by hacking into Russian military command networks; or more traditional signals intelligence operations (e.g., triangulating the

locations of radars and radios); or by satellite reconnaissance; and/or from observers and drones on the frontlines.

There was a reported leak of US military classified information, where photographs of printed documents appeared on various Internet chat rooms and social media.<sup>58</sup> News reports appear to confirm two important facts. First, they confirm that the US and its allies have extensively compromised Russian government sources. They also reveal a US security vulnerability, or perhaps a compromised insider, leaking sensitive US intelligence. Some of the leaked documents reportedly appear to have been modified to make it appear that Russian casualties were lower and Ukrainian casualties were higher, suggesting that the leak at least in part was calculated propaganda, a subject covered in the next section.

It is also entirely possible that cyber operations have degraded Russian military capabilities. In another context, for example, Israel allegedly hacked a Syrian radar system<sup>59</sup> prior to bombing the Al Kubar nuclear facility in 2007.<sup>60</sup> We note that the same Russian S-300 radars used by Syria in 2007 are fielded by Russia in Ukraine today, so it is conceivable that some Ukrainian military operations have tried something similar. The Russians may also be attempting to glean cyber intelligence. They have done so before. One curious episode, unearthed in 2016, concerned a Ukrainian homegrown cell phone app for artillery targeting, which Russia's military was able to compromise, giving it real-time geolocations of Ukrainian artillery units.<sup>61</sup> This is exactly the kind of cyber intelligence activity that we would have expected to happen in the current war. If it is happening, it is not making the news.

What we do know about is the relevance of open-source intelligence (OSINT). At least at the beginning of the war, any Ukrainian with a camera who filmed an attack on a Russian armored vehicle seemed to post it on the internet. Those images, in aggregate, plus videos posted by the Ukrainian and Russian militaries, often from UAVs, provide a surprisingly comprehensive view of the war. They are also increasingly studied by large, distributed amateur and scholarly communities. King's College Ph.D. student and former US Marine officer Rob Lee,<sup>62</sup> among others, strung together a collage of online media to create a compelling analytic narrative of the war. Non-governmental groups like Bellingcat have collected data and developed guides and tools for others to use (e.g., for Telegram and TikTok).<sup>63</sup> No doubt machine learning techniques and increasingly sophisticated geo-indexed imagery sources can paint vivid battlefield pictures.<sup>64</sup> There is even an OSINT component to understanding the cyber war, evinced by raw reporting from security researchers and government/civil society and aggregated in a CSIS report.<sup>65</sup>

## **PROPAGANDA, MISINFORMATION, AND DISINFORMATION**

Many assumed that Russia was powerfully strong in enhancing and exploiting influence operations using cyberspace.<sup>66</sup> Russia's combination of computer hacking and targeted

propaganda in both the U.K. Brexit referendum and US national elections in 2016 revealed highly sophisticated skill in undermining NATO democratic institutions. We have come to expect online active measures that confound NATO democracies,<sup>67</sup> yet Ukraine has dominated the information war for public support. In information operations, Ukraine has been able to transform leaked, unsecure Russian communications into a video of anti-armor ambushes<sup>68</sup> and a narrative of triumph over a hapless opponent. Ukraine has waged a media war that effectively portrays itself as a victim it is, and that effectively reveals the terrible price Russia has paid thus far for its invasion. The retreat of Russian forces from the outskirts of Kyiv scored additional propaganda points.

Ukraine's need from the West for more modern weaponry has been an incessant and ongoing information campaign by the country that has been highly successful.<sup>69</sup> From the first day of combat, Ukraine's leaders have made the case repeatedly for modern armaments able to give it a qualitative edge on the battlefield. Videos uploaded to Telegram, Twitter, YouTube, and other social media platforms weaved a narrative of plucky Ukrainian light infantry repeatedly visiting chaos and calamity on Russian mechanized units. This success begat requests for more arms, accompanied by videos of precision-guided destruction once fielded. Kyiv's public efforts to influence Western countries to fill its dire need for replacement tanks and armored vehicles peaked with President Zelenskyy's late 2022 visit to the US, which was presaged with a video in which Bob Seeger's "Like a rock" riff once found in Chevrolet truck commercials became the soundtrack for a mash-up of American-built heavy armor.<sup>70</sup>

Russian propaganda, internally targeted, has bolstered support at home, although Russia has also aggressively cracked down on and jailed its internal activists.<sup>71</sup> How successful they are ultimately remains to be seen, but Russia has invested heavily in efforts to hobble its domestic news media and limit access to the broader internet.<sup>72</sup> For the Ukrainian territories occupied by Russian forces, Russia has rerouted internet traffic through its own ISPs censorship regime.<sup>73</sup>

Outside of its own borders, Russia has been ineffective at countering Ukraine's narrative. From the outset, Russia repeatedly has claimed that Ukraine is filled with "Nazis,"<sup>74</sup> and they continue to traffic this palpably false claim, both internally and externally. Russian propaganda efforts regarding Ukraine appear borne of an unreality hard for almost anyone to accept as true, but those efforts continue nonetheless.<sup>75</sup> To add to this incompetence, Russian propaganda has led to successful, deadly targeting of Russian forces. Ukraine undoubtedly was fully aware of Russian news reports of maritime logistical operations in the port of Berdyansk when it prepared its standoff missile attacks against Black Sea Fleet amphibious ships.<sup>76</sup> And despite being under Russian control, video from Berdyansk of a sinking Russian ship and the strikes against two others leaked online.<sup>77</sup> Russian-controlled footage also emerged online of the severely damaged Black Sea Fleet flagship, *Moskva*, before it sank.

## WHAT'S COMING NEXT?

Wisdom is shown again and again with the aphorism, “it’s difficult to make predictions, especially about the future.” We will not try to predict the future of kinetic warfare in Ukraine, which depends on a variety of unknowns, including what weapons Ukraine is able to adopt and how effective it will be at blunting Russia’s attacks. Likewise, we cannot predict whether NATO sanctions against Russia and its oligarchs will yield sufficient domestic political pressure for Russia to either convince Putin to withdraw or to convince others to overthrow him. What we can predict is that both sides will increasingly look to cyber tactics to support kinetic warfare as well as support propaganda and information operations.

For kinetic warfare, we are already seeing a variety of NATO armaments being delivered to Ukraine, many of which include precise GPS targeting capabilities. This suggests Russia might counter with GPS jamming/spoofing. It also suggests that broader packages of the latest electronic warfare equipment might be necessary for Ukraine to continue to fight.<sup>78</sup> Clark, an expert on Russia’s portfolio of electronic warfare systems, including jammers, attack tools, counterattack tools, and surveillance equipment, explains how ineffective they have been for most of the war, becoming relevant only once the battle lines became relatively static in Eastern Ukraine.<sup>79</sup>

Propaganda operations undoubtedly will grow more sophisticated on both sides. Today’s propaganda largely entails the release of news and videos to broad audiences. Even though TikTok’s short videos might be a novel delivery mechanism, the idea of using videos for propaganda purposes is nothing new. What we expect to see going forward is *microtargeted propaganda*. Much as Russian operatives used Facebook’s advertisement targeting features to identify and manipulate US voters in the lead-up to the 2016 election,<sup>80</sup> we can and should expect similar microtargeting to on the Ukraine war, to include Russia attempting to manipulate US or other NATO elections and the election of less Ukraine-sympathetic leadership. It is also likely that Russian propaganda and cyber-hacking efforts will target other countries that have emerged as key Ukraine allies. For example, Albania, which has offered public support to Ukraine and has taken in a huge number of Ukrainian refugees, experienced a cyberattack forcing it to take down a number of government services.<sup>81</sup> This activity is now playing out on the information systems of multiple NATO countries, principally located near Russia and Ukraine.

Closer to the battlefield, attempts to manipulate soldier morale are as old as warfare itself. We know Russia has sent messages to Ukrainian phones (both soldiers and their families) and volunteers are sending pro-Ukrainian messages to random Russian phone numbers and posting them to Russian restaurant review sites.<sup>82</sup> Going forward, imagine individual soldiers receiving tailored text messages should come as no surprise: “Here’s a photo of you at this location today. We’ll kill you there tomorrow if you don’t lay down your arms and leave.” On top of that, Ukraine could leverage its war crimes accountability and documentation efforts<sup>83</sup> with tailored messages, e.g., “We know you were ordered to do X, which would make you personally liable



as a war criminal. Don't do it." Such messages could even be created as group texts with the soldiers' families, perhaps inferred from text message interception, in an attempt to leverage family ties to break soldier morale. Moreover, as word spreads at home, this would dissuade other civilians from enlisting for voluntary military service, and/or further encourage their exodus from Russia.<sup>84</sup> It is also completely reasonable to imagine Ukraine sending informative text messages to recently arriving Russian soldiers, e.g., "Welcome to Luhansk. Here's a link to your instruction on the Geneva Convention and war crimes."

One curious aspect of cyber effects in warfare is that they arguably raise less risk of escalation, with cyberattacks on nuclear command and control being a notable exception.<sup>85</sup> NATO's caution against Russian escalation has clearly limited the weapon flow to Ukraine. For example, the US has long supplied Ukraine with HIMARS artillery rocket systems, but delayed supplying the longer-range ATACMS. This contrasts with cyber operations, which the US can conduct itself without providing any technology directly to Ukraine, much less putting any American operator in harm's way.<sup>86</sup> While the details of US cyber operational support for Ukraine are not publicly disclosed, it is widely reported that US and other allied cyber operations are working closely to support Ukraine, and this very likely will continue.<sup>87</sup>

## CONCLUSION

This article considers many ways in which revolutionary technologies have impacted the Ukraine war.<sup>88</sup> We expected Russians to successfully mount sophisticated cyberattacks, both in terms of espionage and sabotage, against the Ukrainians, but this did not happen in any fashion that would have been decisive to the war. If anything, Ukraine has outperformed Russia, both in its cyber defense and its counterattacks (often with key aid from its NATO supporters).

We could easily conclude that Russia's cyber corps failed, or that cyber-effects are a minor component of Russia's overall military strategy. Perhaps a more nuanced view might be to conclude that this is but one of myriad aspects of Russia's military that so far has failed, to include its command and control, logistics, air forces, and navy. Pointing to anything going particularly well for Russia in this war is a challenge, which implicates failure at the highest echelons of Russia's military and civilian leadership.

Perhaps the question we ask, instead is why Russia has done so poorly with its cyber and information forces and why Ukraine has been so successful. It appears that a vigilant and prepared defender can stand up to the information and cyber punishment that may be dealt out by the Kremlin. Important lessons can be derived both from the ongoing war and for future contingencies.♥

## NOTES

1. While Russia calls it a “special military operation,” we refer to it in this essay as the “Ukraine War.” We also use “NATO” and “NATO allies” to include countries assisting Ukraine, including those not NATO members.
2. Harris, Shane, and Dan Lamothe. 2022. “U.S. rules for sharing intelligence with Ukraine.” *The Washington Post*, May 11, 2022, <https://www.washingtonpost.com/national-security/2022/05/11/ukraine-us-intelligence-sharing-war/>.
3. Milmo, Dan. 2022. “China accused of cyber-attacks on Ukraine before Russian invasion.” *The Guardian*, April 1, 2022. <https://www.theguardian.com/technology/2022/apr/01/china-accused-of-launching-cyber-attacks-on-ukraine-before-russian-invasion>.
4. O’Neill, Patrick. 2022. Russia hacked an American satellite company one hour before the Ukraine invasion. MIT Technology Review, May 10, 2022.
5. Kan, Michael. 2022. “Pentagon Impressed by Starlink’s Fast Signal-Jamming Workaround in Ukraine.” PCMag, April 21, 2022. <https://www.pcmag.com/news/pentagon-impressed-by-starlinks-fast-signal-jamming-workaround-in-ukraine>.
6. Harris, Shane, Karen DeYoung, Isabelle Khurshudyan, Ashley Parker, and Liz Sly. 2022. “As Russia prepared to invade Ukraine, U.S. struggled to convince Zelensky, allies of threat.” *The Washington Post*, August 16, 2022. <https://www.washingtonpost.com/national-security/interactive/2022/ukraine-road-to-war/>.
7. Assante, Michael. 2016. “SANS Industrial Control Systems Security Blog | Confirmation of a Coordinated Attack on the Ukrainian Power Grid.” SANS Institute, <https://www.sans.org/blog/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid/>.
8. Greenberg, Andy. 2018. “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/>.
9. Hofmann, Frank. 2022. “Russia’s hybrid war against Ukraine | Europe | News and current affairs from around the continent.” *DW*, February 18, 2022. <https://www.dw.com/en/russias-hybrid-war-against-ukraine/a-60829873>.
10. Harding, Emily. 2022. “The Hidden War in Ukraine | Center for Strategic and International Studies.” Center for Strategic and International Studies, <https://www.csis.org/analysis/hidden-war-ukraine>.
11. Smith, Brad. 2022. “Defending Ukraine: Early Lessons from the Cyber War - Microsoft On the Issues.” The Official Microsoft Blog, <https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/>.
12. Smalley, Suzanne. 2022. “Cybersecurity experts question Microsoft’s Ukraine report.” *CyberScoop*, July 1, 2022, <https://www.cyberscoop.com/cybersecurity-experts-question-microsofts-ukraine-report/>.
13. “Ukraine Network IOCs.” 2022. PasteBin, <https://pastebin.com/PCK97yjc>.
14. Google. 2023. *Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape*.
15. Willett, Marcus. “The Cyber Dimension of the Russia–Ukraine War.” In *Survival: October–November 2022*, pp. 7–26. Routledge, 2022.
16. Microsoft. 2023. A year of Russian hybrid warfare in Ukraine, March 15, 2023.
17. Volz, Dustin. 2016. “Russian hackers tracked Ukrainian artillery units using Android implant: report.” Reuters, December 21, 2016, <https://www.reuters.com/article/us-cyber-ukraine/russian-hackers-tracked-ukrainian-artillery-units-us-ing-android-implant-report-idUSKBN14B0CU>.
18. Lehto, M. “Cyber Warfare and War in Ukraine.” *Journal of Information Warfare* 22, no. 1 (2023).
19. Beale, Jonathan. 2023. “Makiivka attack: Could mobile phones have revealed Russian location?” BBC, <https://www.bbc.com/news/world-europe-64164921>.
20. Geers, Kenneth. 2022. “Computer Hacks in the Russia-Ukraine War.” DEFCON 30, <https://media.defcon.org/DEF%20CON%2030/DEF%20CON%2030%20presentations/Kenneth%20Geers%20-%20Computer%20Hacks%20in%20the%20Russia-Ukraine%20War%20-%20paper.pdf>.
21. Eichensehr, Kristen. 2022. “Ukraine, Cyberattacks, and the Lessons for International Law.” *AJIL Unbound* 116:145–149, <https://doi.org/10.1017/aju.2022.20>.
22. Kostyuk, Nadiya, and Erik Gartzke. 2022. “Why Cyber Dogs Have Yet to Bark Loudly in Russia’s Invasion of Ukraine.” *Texas National Security Review* 5, no. 3 (Summer): 113–126, <http://dx.doi.org/10.26153/tsw/42073>.
23. Rovner, Joshua. 2022. “Sabotage and War in Cyberspace.” *War on the Rocks*, <https://warontherocks.com/2022/07/sabotage-and-war-in-cyberspace/>.
24. Wilde, Gavin. 2022. “Assess Russia’s Cyber Performance Without Repeating Its Past Mistakes.” *War on the Rocks*, <https://warontherocks.com/2022/07/assess-russias-cyber-performance-without-repeating-its-past-mistakes/>.



## NOTES

25. Maschmeyer, Lennart. "Subversion, cyber operations, and reverse structural power in world politics." *European Journal of International Relations* 29, no. 1 (2023): 79-103.
26. Cranny-Evans, Sam, and Thomas Withington. 2022. "Russian Comms in Ukraine: A World of Hertz." RUSI, <https://rusi.org/explore-our-research/publications/commentary/russian-comms-ukraine-world-hertz>.
27. Myre, Greg. 2022. "How does Ukraine keep intercepting Russian military communications?" NPR, <https://www.npr.org/2022/04/26/1094656395/how-does-ukraine-keep-intercepting-russian-military-communications>.
28. Borger, Julian. 2022. "Vitaly Gerasimov: second Russian general killed, Ukraine defence ministry claims." *The Guardian*, March 9, 2022, <https://www.theguardian.com/world/2022/mar/08/vitaly-gerasimov-second-russian-general-killed-ukraine-defence-ministry-claims>.
29. Schogol, Jeff. 2022. "US military learning from Russian troops using cell phones in Ukraine." *Task & Purpose*, May 13, 2022, <https://taskandpurpose.com/news/russia-ukraine-cell-phones-track-combat/>.
30. Horton, Alex, and Shane Harris. 2022. "Russian troops' tendency to talk on unsecured lines is proving costly." *The Washington Post*, March 27, 2022, <https://www.washingtonpost.com/national-security/2022/03/27/russian-military-unsecured-communications/>.
31. Schmitt, Eric. 2022. "As Russian Troop Deaths Climb, Morale Becomes an Issue, Officials Say." *The New York Times*, March 16, 2022, <https://www.nytimes.com/2022/03/16/us/politics/russia-troop-deaths.html>.
32. Kadam, Tanmay. 2022. "Russia's Electronic Warfare Capability 'Exposed' In Ukraine War; Is Putin's Techno-Savvy Army Losing The EW Battle?" *EurAsian Times*, April 18, 2022, <https://eurasiatimes.com/russias-electronic-warfare-capability-exposed-in-ukraine-war/>.
33. Peck, Michael. 2017. "The Crazy Way Russia Could Hijack Your iPhone." *The National Interest*, April 2, 2017, <https://nationalinterest.org/blog/the-buzz/the-crazy-way-russia-could-hijack-your-iphone-19976>.
34. Srivastava, Mehul, Madhumita Murgia, and Hannah Murphy. 2022. "The secret US mission to bolster Ukraine's cyber defences ahead of Russia's invasion." *Financial Times*, March 8, 2022, <https://www.ft.com/content/1fb2f592-4806-42fd-a6d5-735578651471>.
35. Devine, Kieran. 2022. "Ukraine war: Mobile networks being weaponised to target troops on both sides of conflict." Sky News, April 1, 2022, <https://news.sky.com/story/ukraine-war-mobile-networks-being-weaponised-to-target-troops-on-both-sides-of-conflict-12577595>.
36. Sabin, Sam, and Laurens Cerulus. 2022. "3 reasons Moscow isn't taking down Ukraine's cell networks." Politico, March 7, 2022, <https://www.politico.com/news/2022/03/07/ukraine-phones-internet-still-work-00014487>.
37. Clark, Bryan. 2022. "The Fall and Rise of Russian Electronic Warfare." *IEEE Spectrum*, July 30, 2022. <https://spectrum.ieee.org/the-fall-and-rise-of-russian-electronic-warfare>.
38. Boot, M., 2006. *War made new: technology, warfare, and the course of history, 1500 to today*, Penguin.
39. Dixon, Robyn. 2020. "Azerbaijan's drones owned the battlefield in Nagorno-Karabakh — and showed future of warfare." *The Washington Post*, November 11, 2020, [https://www.washingtonpost.com/world%2FEurope%2FNagorno-karabakh-drones-azerbaijan-aremenia%2F2020%2F11%2F441bcbd2-193d-11eb-8bda-814ca56e138b\\_story.html](https://www.washingtonpost.com/world%2FEurope%2FNagorno-karabakh-drones-azerbaijan-aremenia%2F2020%2F11%2F441bcbd2-193d-11eb-8bda-814ca56e138b_story.html).
40. Bronk, Chris, and Gabriel Collins. 2021. "Bear, Meet Porcupine: Unconventional Deterrence for Ukraine." *Defense One*, <https://www.defenseone.com/ideas/2021/12/bear-meet-porcupine-unconventional-deterrence-ukraine/360195/>.
41. "Phantom 4 Pro V2.0." n.d. DJI. Accessed August 23, 2022, <https://www.dji.com/phantom-4-pro-v2>.
42. "Aerorozvidka." n.d. Wikipedia. Accessed August 23, 2022. <https://en.wikipedia.org/wiki/Aerorozvidka>.
43. Hambling, David. 2022. "Ukrainian Drone Drops Bomb Through Open Hatch To Score First Kill On Russia's Oldest Tank." *Forbes*, July 7, 2022, <https://www.forbes.com/sites/davidhambling/2022/07/07/ukrainian-drop-drone-bomb-through-open-hatch-to-score-first-kill-on-russias-oldest-tank/?sh=63cf770f36c6>.
44. See, for instance: Agnes Helou, "With Turkish drones in the headlines, what happened to Ukraine's Bayraktar TB2s?," *Breaking Defense*, 6 October 2023, <https://breakingdefense.com/2023/10/with-turkish-drones-in-the-headlines-what-happened-to-ukraines-bayraktar-tb2s/>
45. Hambling, David. 2023. "How Have Ukrainian Drones Beaten Russian Jammers — And Will It Last?" *Forbes*, 9 August 2023, <https://www.forbes.com/sites/davidhambling/2023/08/09/how-did-ukraine-beat-russias-drone-jammers/?sh=lc0afac97caa>
46. Hunder, Max. 2023. "Inside Ukraine's scramble for 'game-changer' drone fleet." *Reuters*. March 24, 2023, <https://www.reuters.com/world/europe/inside-ukraines-scramble-game-changer-drone-fleet-2023-03-24/>

## NOTES

47. Collins, Liam. 2018. "Russia Gives Lessons in Electronic Warfare | AUSA." Association of the United States Army, July 26, 2018. <https://www.ousa.org/articles/russia-gives-lessons-electronic-warfare>.
48. "More drones coming, Ukraine tells Russia after skyscraper hit," BBC, 1 August 2023, <https://www.bbc.co.uk/news/live/world-66367658>. See also: Collins, Gabriel. 2023. "Ukraine Needs Long-Range Firepower for Victory." Foreign Policy. January 4, 2023. <https://foreignpolicy.com/2023/01/04/ukraine-long-range-firepower-victory/> and Bronk, Christopher and Gabriel Collins. "Ukraine Needs a Whole Lot of Deadly Drones." Foreign Policy. April 13, 2022. <https://foreignpolicy.com/2022/04/13/ukraine-drone-warfare-armaments-russia/>
49. Newdick, Thomas. 2023. "Putin Admits Moscow's Air Defenses "Need Work" After Multi-Drone Attack." May 30, 2023. The Drive, <https://www.thedrive.com/the-war-zone/putin-admits-moscows-air-defenses-need-work-after-multi-drone-attack>.
50. "SBU drones hit power substation feeding military facilities in Russia's Belgorod region." 2023. Ukrinform. October 15, 2023, <https://www.ukrinform.net/rubric-ato/3774242-sbu-drones-hit-power-substation-feeding-military-facilities-in-russias-belgorod-region.html>
51. "How drones dogfight above Ukraine." 2023. The Economist. February 7, 2023. <https://www.economist.com/the-economist-explains/2023/02/07/how-drones-dogfight-above-ukraine>
52. Fingar, Thomas. 2011. *Reducing uncertainty: Intelligence analysis and national security*, Stanford University Press.
53. Sabbagh, Dan. 2022. "Drone footage shows Ukrainian ambush on Russian tanks." *The Guardian*, March 11, 2022, <https://www.theguardian.com/world/2022/mar/10/drone-footage-russia-tanks-ambushed-ukraine-forces-kyiv-war>.
54. Harris, Shane, Karen DeYoung, Isabelle Khurshudyan, Ashley Parker, and Liz Sly. 2022. "As Russia prepared to invade Ukraine, U.S. struggled to convince Zelensky, allies of threat." *The Washington Post*, August 16, 2022, <https://www.washingtonpost.com/national-security/interactive/2022/ukraine-road-to-war/>.
55. Dilanian, Ken, Courtney Kube, Carol Lee, and Dan De Luce. 2022. "Bold, effective and risky: The new strategy the U.S. is using in the info war against Russia." *NBC News*, <https://www.nbcnews.com/politics/national-security/us-using-declassified-intel-fight-info-war-russia-even-intel-isnt-rock-rcna23014>.
56. "M142 HIMARS." n.d. Wikipedia. Accessed August 23, 2022, [https://en.wikipedia.org/wiki/M142\\_HIMARS](https://en.wikipedia.org/wiki/M142_HIMARS).
57. Hunder, Max, Tom Balmforth, and Timothy Heritage. 2022. "Ukrainian military strikes with Western arms disrupt Russian supply lines - general." Reuters, July 14, 2022, <https://www.reuters.com/world/europe/ukrainian-military-strikes-with-western-arms-disrupt-russian-supply-lines-2022-07-14/>.
58. Barnes, Julian E., Helene Cooper, Thomas Gibbons-Neff, Michael Schwartz, and Eric Schmitt, "Leaked Documents Reveal Depth of U.S. Spy Efforts and Russia's Military Struggles," *The New York Times*, April 8, 2023, <https://www.nytimes.com/2023/04/08/us/politics/leaked-documents-russia-ukraine-war.html>.
59. Gasparre, Richard. 2008. "The Israeli 'E-tack' on Syria – Part II." *Airforce Technology*, <https://www.airforce-technology.com/analysis/feature1669/>.
60. Farrell, Stephen. 2018. "Israel admits bombing suspected Syrian nuclear reactor in 2007, warns Iran." Reuters, March 20, 2018, <https://www.reuters.com/article/us-israel-syria-nuclear/israel-admits-bombing-suspected-syrian-nuclear-reactor-in-2007-warns-iran-idUSKBNIGX09K>.
61. Martin, David. 2016. "Russian hacking proves lethal after Ukrainian military app hijacked." CBS News, <https://www.cbsnews.com/news/russian-hacking-proves-lethal-after-ukrainian-military-app-compromised/>.
62. Lee, Rob. 2022. "Rob Lee (@RALee85)." Twitter, <https://twitter.com/RALee85>.
63. 2022. Bellingcat - the home of online investigations, <https://www.bellingcat.com>.
64. Tearline. 2022. "Ukraine." Tearline.mil, <https://www.tearline.mil/category/ukraine/>.
65. Harding, Emily. 2022. "The Hidden War in Ukraine | Center for Strategic and International Studies," <https://www.csis.org/analysis/hidden-war-ukraine>.
66. Cordey, Sean. 2019. "Cyber Influence Operations: An Overview and Comparative Analysis," ETHZ Research Collection, <https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/382358/1/Cyber-Reports-2019-10-CyberInfluence.pdf>.
67. Rid, Thomas. 2020. *Active Measures: The Secret History of Disinformation and Political Warfare*. N.p.: Farrar, Straus and Giroux.
68. Sabbagh, Dan. 2022. "Drone footage shows Ukrainian ambush on Russian tanks." *The Guardian*, March 11, 2022, <https://www.theguardian.com/world/2022/mar/10/drone-footage-russia-tanks-ambushed-ukraine-forces-kyiv-war>.
69. Dyczok, Marta, and Yerin Chung. "Zelens kyiv uses his communication skills as a weapon of war." *Canadian Slavonic Papers* 64, no. 2-3 (2022): 146-161.

## NOTES

70. Even two of the authors added their voices to the chorus on sending Ukraine modern, Western tanks. Collins, Gabriel and Chris Bronk. 2023. "The M1 Abrams is the Right Tank for the Job in Ukraine." *Foreign Policy*, January 24, 2023.
71. Dixon, Robyn. 2022. "In Putin's Russia, antiwar protesters face prison and abuse." *The Washington Post*, June 26, 2022, <https://www.washingtonpost.com/world/2022/06/26/russia-protests-dissent-activists-skochilenko/>.
72. McMahon, Robert, and Emily Lieberman. 2022. "Russia Is Censoring News on the War in Ukraine. Foreign Media Are Trying to Get Around That." Council on Foreign Relations, <https://www.cfr.org/in-brief/russia-censoring-news-war-ukraine-foreign-media-are-trying-get-around>.
73. Satariano, Adam, and Lindsey Balbierz. 2022. "How Russia Took Over Ukraine's Internet in Occupied Territories." *The New York Times*, August 9, 2022, <https://www.nytimes.com/interactive/2022/08/09/technology/ukraine-internet-russia-censorship.html>.
74. Srullevitch, Andrew. 2022. "Why is Putin Calling the Ukrainian Government a Bunch of Nazis?" ADL. <https://www.adl.org/blog/why-is-putin-calling-the-ukrainian-government-a-bunch-of-nazis>. Also see: Cloud, David S., James Marson, Evan Gershkovich, and Laurence Norman. 2022. "Russia Ramps Up Accusations of Neo-Nazism in Ukraine." *The Wall Street Journal*, May 3, 2022, <https://www.wsj.com/articles/russia-reiterates-accusations-of-neo-nazism-in-ukraine-11651579622>.
75. Rossoliński-Liebe, Grzegorz, and Bastiaan Willems. "Putin's Abuse of History: Ukrainian 'Nazis', 'Genocide', and a Fake Threat Scenario." *The Journal of Slavic Military Studies* 35, no. 1 (2022): 1-10.
76. BBC. 2022. "Russian warship destroyed in occupied port of Berdyansk, says Ukraine," March 24, 2022, <https://www.bbc.com/news/world-europe-60859337>.
77. Sutton, H. I. 2022. "Satellite Images Confirm Russian Navy Landing Ship Was Sunk at Berdyansk - USNI News." USNI News, March 25, 2022, <https://news.usni.org/2022/03/25/satellite-images-confirm-russian-navy-landing-ship-was-sunk-at-berdyansk>.
78. LaPorta, James. 2018. "Lockheed's 'Dragon Shield' for Finland achieves operational capability." UPI, February 12, 2018, <https://www.upi.com/Defense-News/2018/02/12/Lockheeds-Dragon-Shield-for-Finland-achieves-operational-capability/2281518445772/>.
79. Clark, Bryan. 2022. "The Fall and Rise of Russian Electronic Warfare." *IEEE Spectrum*, July 30, 2022, <https://spectrum.ieee.org/the-fall-and-rise-of-russian-electronic-warfare>.
80. Mayer, Jane. 2018. "How Russia Helped Swing the Election for Trump." *The New Yorker*, September 24, 2018, <https://www.newyorker.com/magazine/2018/10/01/how-russia-helped-to-swing-the-election-for-trump>.
81. *Euronews Albania*. 2022. "'Sulm kibernetik nga jashtë Shqipërisë', AKSHI bllokoi shërbimet online." July 17, 2022, <https://euronews.al/vendi/aktualitet/2022/07/17/sulm-kibernetik-nga-jashte-shqiperise-akshi-blokon-shepbimet-online/>.
82. Cecil, Nicholas. 2022. "Putin's forces sending threats to phones of Ukraine's soldiers, say defence experts." *Evening Standard*, June 10, 2022. <https://www.standard.co.uk/news/world/vladimir-putin-war-ukraine-russia-psychological-warfare-institute-for-the-study-of-war-bl004992.html>. Also: Collins, Liam. 2018, "Russia Gives Lessons in Electronic Warfare | AUSA." Association of the United States Army, July 26, 2018. <https://www.ausea.org/articles/russia-gives-lessons-electronic-warfare>. Gronholt, Jacob. 2022. "Keyboard army using restaurant reviews to take on Russian state media." Reuters, March 3, 2022. <https://www.reuters.com/world/europe/keyboard-army-using-restaurant-reviews-take-russian-state-media-2022-03-02/>. Zitser, Joshua. 2022, "Ukraine: Meet the Volunteers Messaging Random Russians to Tell of Putin's War," *Business Insider*, March 19, 2022, <https://www.businessinsider.com/ukraine-meet-the-volunteers-messaging-random-russians-tell-putins-war-2022-3>.
83. *The New York Times*. 2022. "Documenting Atrocities in the War in Ukraine." May 22, 2022, <https://www.nytimes.com/interactive/2022/05/22/world/europe/ukraine-war-crimes.html>.
84. Ebel, Francesca and Mary Ilyushina, "Russians abandon wartime Russia in historic exodus", *The Washington Post*, February 13, 2023, <https://www.washingtonpost.com/world/2023/02/13/russia-diaspora-war-ukraine/>
85. Acton, James M. 2020. "Cyber Warfare & Inadvertent Escalation." *Daedalus* 149, no. 2 (Spring): 133-149, [https://doi.org/10.1162/daed\\_a\\_01794](https://doi.org/10.1162/daed_a_01794).
86. Libicki, Martin C. 2012. "Crisis and Escalation in Cyberspace | RAND." RAND Corporation, <https://www.rand.org/pubs/monographs/MG1215.html>.
87. Lin, Herbert. "Russian Cyber Operations in the Invasion of Ukraine." *The Cyber Defense Review* 7, no. 4 (2022): 31-46.
88. Robinson, Paul. "The Russia-Ukraine Conflict and the (Un) Changing Character of War." *Journal of Military and Strategic Studies* 22, no. 2 (2022).



# Civil Cyber Defense – A New Model for Cyber Civic Engagement

---

Dr. Mark Grzegorzewski  
Major Margaret Smith, Ph.D.  
Dr. Barnett Koven

## ABSTRACT

*In a world of ubiquitous connections, cybersecurity is everyone's responsibility. Gone are the days when the actions of others had little impact on a person's day-to-day activities. We are now completely digitally interdependent, meaning the actions of one individual can be the vulnerability that allows adversaries to target a soft spot in the United States' (U.S.) digital infrastructure. We argue a whole-of-society approach to cybersecurity is needed. The involvement of all members of society is required to defend against the scourge of cyber intrusions emanating from Russia, China, North Korea, and Iran. We do not promote individuals or corporations engaging in offensive cyber operations, but instead advocate that the U.S. already has a non-governmental model for citizen involvement in entities like the Civil Air Patrol (CAP), to adopt for cyberspace. We build on Estonia's Cyber Defense League (CDL) organizational model and the works of others, advocating for establishing a Civil Cyber Defense (CCD) in the U.S. We conclude with specific actions this new entity could take to increase the overall cybersecurity posture of the U.S. and identify potential issues with our CCD concept.*

## INTRODUCTION

**I**n cyberspace, we find ourselves in an era of ebbing United States (U.S.) dominance. Like actions in the physical space, America's adversaries are engaging in asymmetric tactics and strategies in cyberspace and the information environment to degrade the U.S. physical and cybersecurity posture and capabilities. At this moment, there

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



**Dr. Mark Grzegorzewski** is an assistant professor of cybersecurity at Embry-Riddle Aeronautical University in the Security Studies and International Affairs Department. He is also an Army Cyber Institute Fellow. His recent publications include: “911? We Have an Emergency: Cyberattacks on Emergency Response Systems,” “In Search of Security: Understanding the Motives Behind Iran’s Cyber-Enabled Influence Campaigns,” and “Why the United States Must Win the Artificial Intelligence (AI) Race.” Dr. Grzegorzewski worked for over 11 years in the Department of Defense, seven of those years for U.S. Special Operations Command. He holds a Ph.D., M.A., and B.A. in Political Science/Government from the University of South Florida and a graduate certificate in Globalization Studies.

is both an opportunity and a need for the U.S. to do something creative in addressing cybersecurity to better arm itself against asymmetric and irregular threats. Estonia, given its democratic government and proactive cyber defense posture, is an ideal case to examine. In 2007, Estonia was targeted by Russian cyber proxies, and in response, developed the Cyber Defense League (CDL), which relies on civilian talent to help fill security gaps and to augment its traditional government defense apparatus. To integrate the CDL, Estonia leveraged its hacking community’s social capital and national pride, providing everyday hackers and enthusiasts (who may or may not work professionally with computers) an opportunity to protect their country against foreign aggression in the cyber and information spaces.

At present, the U.S. is in a similar situation as Estonia in 2007: America is experiencing a constant barrage of cyber intrusions and foreign operations in the information environment. It is at great risk from the actions taken by its adversaries and their cyber proxies. To date, the U.S. has no plans to build a civilian program comparable to Estonia’s CDL or to leverage civilian knowledge in its cyber defense strategy. We argue that the U.S. should create an American Civil Cyber Defense (CCD) – civilians working to defend the nation from cyber threats – because civilians and civilian talent are necessary components of an effective and robust approach to cybersecurity and a whole-of-society response to cyber threats and cyberattacks. To be clear, our proposal does not include promoting civilian engagement in offensive cyber activities or espionage but is instead focused on building a framework for developing an all-volunteer force of civilian cyber defenders and leveraging civilian talents to augment the ongoing law enforcement, government, and military efforts to defend the nation and U.S. networks against cyber threats.

In this article, we make a case for the CCD by articulating what a “whole-of- society” approach to cyber-



**MAJ Maggie Smith, Ph.D.**, is an Army Cyber Officer currently serving as a Strategic Planner for HQDA. She is also a Senior Fellow at the Atlantic Council's Cyber Statecraft Initiative, Director of the Irregular Warfare Initiative's Cyber Project, and graduate faculty at the University of Maryland, College Park.

security should include, proposing how to implement and incorporate a CCD into America's national defense strategy, and providing an organizational structure for the CCD that is modeled on the Civil Air Patrol (CAP) concept. We also demonstrate the effectiveness of the CCD model by investigating the Estonian example. Finally, we address potential pitfalls and difficulties to employing citizens in a defensive-oriented CCD to augment our national cyber strategy and how to mitigate those risks.

### **THINK SMALL: STRENGTHENING THE NETWORK AT THE LOCAL LEVEL**

In cyberspace, one individual's vulnerability can quickly become the network's security compromise, and in terms of overall U.S. cybersecurity and interconnectedness, that means less secure organizations pose a direct risk to organizations that have hardened and resilient systems. In short, all networks are less secure due to interconnectivity and all networks are increasingly at risk as more and more devices and users become connected. Once an adversary gains a foothold into a network through an unsecured system, they can laterally move in and through that network to cause damage upstream or downstream. While many large organizations allocate extensive resources to cybersecurity, many more small businesses simply do not have the resources or expertise to protect their systems.

For example, in 2016, Cate Machine & Welding's "dusty old computer humming away in the back office" of the small Wisconsin business was taken over by Chinese hackers.<sup>1</sup> Even though the hackers were not interested in Cates' data, they used a jumbled maze of compromised computers as the launchpad for their attacks. "Mom and pop" businesses are equally important as any other node in the network and need greater security to make the broader cybersecurity ecosystem stronger.





**Dr. Barnett S. Koven** is a Manager at Deloitte working as a data scientist in the firm's federal sector strategy & analytics practice. Dr. Koven is a national security specialist and data scientist with over a decade of experience in counterterrorism, counterinsurgency and strategic competition. He has deep expertise in leading analytics teams applying quantitative and qualitative approaches to national security combining research design, inferential statistics, machine learning and applied AI, survey experimental research, and data visualization. He has received research funding from the U.S. Departments of Defense (DoD), Homeland Security (DHS), State, Justice, and Energy, as well as from the Horowitz Foundation for Social Policy, George Washington University (GWU) and University of Maryland (UMD). He received his Ph.D., M.Phil. and M.A. degrees in Political Science, as well as a B.A. degree in International Affairs and Latin American and Hemispheric Studies from GWU.

Just like the owners of Cate Machine & Welding “had no idea [their business computer] could be used as an infiltration unit for Chinese attacks,”<sup>2</sup> most small businesses do not view cybersecurity as a major priority or problem. Yet, 28 percent of data breaches occur at small businesses and of those 28 percent, “37 percent suffered a financial loss, 25 percent filed for bankruptcy, and 10 percent went out of business” in the year following the breach. Data also indicate that less than half of small businesses<sup>3</sup> believe they can quickly respond to a data breach.<sup>4</sup> Coupled with the fact that many small businesses cannot promptly respond to and remediate a cyber intrusion, 67 percent of small business owners deny they are even vulnerable to an cyberattack.<sup>5</sup> Additionally, ransomware attacks are increasing and 55 percent occur against businesses with less than 100 employees.<sup>6</sup> The result is a dangerous combination: small businesses do not think malicious actors will target them, and they are ill-equipped to handle a breach when one does occur.

Small businesses are not the only local or community concern – cybersecurity risks that state and local governments face are also alarming. Investors and insurance providers are increasingly worried about the spiking number of attacks against local government IT services and data. Specifically, the onslaught of ransomware attacks targeting the public sector at a time when most state and local governments are still trying to figure out how to deliver and sustain services online. A recent survey of “150 municipal bond credit analysts and specialists (excluding those at rating agencies) carried out by HillTop Securities shows digital risks are increasingly on investors’ minds – and practically none of those investors think state and local governments are prepared” for a cyberattack.<sup>7</sup> Additionally, only six percent of respondents thought state and local governments were “on their way to being prepared” for cyberattacks, and not a single survey respondent thought that small governments were “prepared,” or “very prepared,” to face a cybersecurity



incident.<sup>8</sup> The implications of an insecure public sector are vast and far-reaching and, with smaller budgets and smaller staffs, local government cybersecurity efforts are likely to remain underfunded and understaffed.

Of course, small businesses and local governments are not purposefully negligent or willfully ignorant. In many cases, small businesses and government entities do not have the proper conceptualization of cyber risk.<sup>9</sup> In other cases, small organizations do not have a sufficient budget allocated to cybersecurity or do not have the funding or technical resources to implement proper security measures.<sup>10</sup> While the proposed CCD model cannot address small business or local government resource allocation, the model can address owner and worker education to raise awareness and knowledge of cyber risks and advise on rudimentary remediation plans. A CCD and its cadre of volunteers could help small businesses and mayoral offices with cybersecurity tasks, like updating their systems and installing patches. Estonia provides a case study for how a CCD can make a difference in national defense by encouraging and enlisting the help of civilian talent.

### **IMITATION IS THE SINCEREST FORM OF FLATTERY: ESTONIA**

Estonia is one of the most digitally connected—and digitally dependent—countries in the world.<sup>11</sup> To make a decisive break with its Soviet past and chart its own future by embracing democracy and capitalism, Estonia incorporated technological solutions to leap past many other developing, former-Soviet states. But Estonia still struggles against the pull of Russia's influence—the northern Estonian border is just over 90 miles from Russia's second largest city, St. Petersburg.<sup>12</sup> Russia does not respect Estonia's sovereignty,<sup>13</sup> and to offset Russian influence in the country, Estonia actively pursued membership in the European Union and North Atlantic Treaty Organization.<sup>14</sup> Despite—or perhaps because of—these memberships, Estonia was the target of Russian cyber aggression in 2007 following the “Bronze Night” protests.<sup>15</sup> Adding to the Russian proximity problem is Russia's extant desire to reclaim its former great power status by expanding its sphere of influence.

In response to its 2007 cybersecurity failures, Estonia decided that it should scale its cyber capabilities by tapping into the civilian and private sectors to defend against hacks orchestrated by Russia (The IP addresses linked to the computers responsible for the 2007 attack on Estonia emanated from Russia, but the government denied direct involvement.). The Estonian cybersecurity community and the Ministry of Defense proposed the creation of a Cyber Defense League, modeled on the Estonian Defense League, which is a “voluntary national defense organization” under the Estonian Ministry of Defense.<sup>16</sup> The CDL was designed to augment the existing defense league and is tasked with a civilian cyber defense capability.<sup>17</sup>

Estonia divides its CDL forces into regional units composed of a diverse set of members whose skills are aligned with local concerns. Since the units are composed of volunteers, individuals cannot be compelled to always participate, and members maintain a commitment that works around their family and business obligations. The volunteer format has the

benefit of flexibility,<sup>18</sup> and since there is no permanent CDL staffing, a region could experience a lapse in support. Still, Estonian citizens broadly understand their precarious national security situation and that every Estonian has a role to play in homeland defense<sup>19</sup>—particularly in the cyber realm.

After gaining independence, Estonia made concerted efforts to become “E-stonia,” an internet-based society. The country was quickly wired after it became independent and began teaching programming to young schoolchildren (beginning at age 5). More importantly, it was a country whose population understood well the need to be free from the former Soviet Union, and its successor state, the Russian Federation, as Russia remained a tangible threat to the new country’s sovereignty. To be effective against Russian aggression, the Estonian CDL focuses citizen participation on improving critical information infrastructure security by pursuing three main efforts.<sup>20</sup>

- ♦ ***Developing a network of cooperation including for crisis response.*** This is accomplished by strengthening cooperation among qualified volunteer IT specialists, as well as through the creation of a network to combine the expertise of public and private sectors to act in a crisis.
- ♦ ***Improving the security of critical information infrastructure*** by regularly sharing threat awareness information and disseminating best practices to the public and private sectors, as well as enhancing preparedness for operating during a crisis.
- ♦ ***Promoting awareness, education, and training*** by providing continuous information security education and training to members as well as actively participating in cybersecurity training networks, including international ones.

In addition, the CDL can be reassigned to support the Estonian Computer Emergency Response Team (Estonian-CERT), a team that analyzes and disseminates cyber threats and vulnerabilities to coordinate responses during times of crisis involving critical information infrastructure and systems.<sup>21</sup>

Estonia’s comprehensive security approach recognizes that integrating the public into a whole-of-nation defense *after* the state is already at risk is too late. Taking a proactive security approach and engaging citizen defenders during a time of relative peace is critical to ensuring Estonia has a more robust defensive posture during conflict. Therefore, Estonia’s cyber defense strategy has created and fostered the connections among citizens, the commercial sector, and the government necessary to establish the networks for a collective defense *ahead* of a major crisis.<sup>22</sup> This also has the added benefit of promoting security, safety, and stability during peacetime.

## THE VOLUNTARY SERVICE MODEL

Derivatives of the three main efforts for the CDL described above include the voluntary service model as a cost-effective way to improve national defense.<sup>23</sup> In the case of Estonia,

CDL members are not paid unless they are mobilized.<sup>24</sup> Additionally, members provide their time and expertise without compensation and most participate out of a sense of patriotism. Of course, the opportunity to network among fellow professionals and gain workplace training is a non-financial benefit to all CDL volunteers, but it may not be sufficient to offset the opportunity cost of donating time. However, by drawing from, and depending on, its existing cyber-qualified workforce, Estonia saves on resources that would otherwise be allocated to training soldiers or government civilians on cybersecurity tradecraft. Regional cyber defense unit (CDU) members, in most cases, already maintain extensive cyberspace expertise and only need to learn organizational processes to be effective defenders. Furthermore, given the voluntary nature of the CDU, its members do not have to be housed on a full-time basis when compared to the costs of sheltering a traditional military member.

Another benefit of CDL's volunteer model is that it gives individuals that may not be qualified or capable of serving in the armed forces an opportunity to serve their country. That is to say, those who cannot serve in the armed forces are still able to work in the service of the state through the CDL. For instance, a cyber security expert with a physical disability may want to serve the country out of a sense of patriotic duty but traditional military qualification requirements would prevent them from serving. By opening CDL volunteer opportunities to traditionally excluded individuals allows many more volunteers to contribute to defense of the country. Given that the CDL is a voluntary organization, it also allows individuals to join who are not looking to commit to full-time military service.<sup>25</sup> The path to fulfilling patriotic service in cyberspace via the CDL allows for many more Estonians to contribute service in defense of their county at a very low cost to the government.

Another aspect of cost-saving is a shortened incident response time.<sup>26</sup> By not centralizing CDL volunteers, response times are shorter because mass mobilizations of personnel and equipment normally take time. Critically, quick response times and rapid remediation are key in any cyber incident.<sup>27</sup> When the decision to deploy CDL forces is made, the regionally aligned and trained CDUs are quick to respond. While larger strategically focused cyber forces are certainly important, having a local, quick reaction cyber force enables swift documentation and remediation of any cyber incident without having to expend the resources required to rapidly pull in strategic-level forces. CDL volunteers build upon the resilience of Estonia's cyber infrastructure by providing an on-demand service should the Estonian national cyber force be needed on a different mission set.<sup>28</sup>

## **CREATING A COLLECTIVE INTEREST: ESTONIAN SOCIAL CAPITAL AND NATIONAL PRIDE**

Any form of civilian cyber defense coordination requires trust among members and, by extension, the trust of their government. The trust between citizens and government is often referred to as a "psychological contract," wherein a person and organization both gain from

the partnership since their beliefs and principles largely overlap.<sup>29</sup> Moreover, in the psychological contract model, individuals understand the needs of the organization and how supporting the organization benefits them, which creates an obligation for the individual to protect their individual interests and the organizations' (the state) interests. Accordingly, any psychological contract is demonstrably at its strongest when there are high levels of public support between citizens and government. An example of a strong psychological contract between the state and citizens is the 78 percent of Estonian respondents who in 2018 agreed (with only 6 percent disagreeing) that the entire society was responsible for the defense of the nation.<sup>30</sup>

Critical to the notion of a psychological contract between individuals and the state, is the idea that corporations also have a role to play. Businesses can maximize outcomes by working in a stable environment in which actions in cyberspace are regularized and surprises minimized. By viewing themselves as part of a cybersecurity collective or ecosystem, in which private entities provide much of the information technology (IT), operations technology (OT), and skilled labor that underpin modern communications infrastructure for a state, IT and OT-related corporations increasingly see their interests as overlapping with the interests of the citizen and the state.<sup>31</sup> In the case of Estonia, the shared cybersecurity interests between the state, its citizens, and corporations has prompted private companies to view employee participation in the CDL as in their own best interest.<sup>32</sup>

Additionally, trust between individuals is just as important as trust between the citizen and the state. CDL members come together to provide expertise and education, they share information with each other and gain trust.<sup>33</sup> Trust and interoperability allows the CDL to resolve issues quickly and collectively. Trust also allows members to work outside of the traditional bureaucratic structures and thereby streamline responses.<sup>34</sup> Moreover, trusted connections exist outside the CDL. For example, CDL members can also call each other in their private or personal lives to resolve cyberspace issues. Regarding the Estonian collaborative model, Piret Pernik and Emmet Touhy write, "as people know each other personally, they tend to trust others more than in impersonal interactions, and greater flexibility enables them to share information swiftly as cyber incidents evolve very fast."<sup>35</sup>

Estonia has built resilience into their comprehensive security approach by emphasizing that every citizen has a role to play in national security.<sup>36</sup> Estonia's approach maintains the notion that all citizens may be called upon to contribute to a collective defense should Estonia's sovereignty or security be threatened. Additionally, given its small size, proximity to Russia, and its history of occupation, the government proactively looks for security gaps, anticipates emerging gaps, and identifies potential solutions should the traditional defense model for the state fail. Estonia's comprehensive security approach also recognizes that integrating the public into a whole-of-nation defense *after* the state is already at risk, is too late. Ultimately, taking a proactive security approach and engaging citizen defenders during a

time of relative peace is critical to ensuring Estonia has a more robust defensive posture in war or during an attack. Estonia's strategy has created and fostered the connections between citizens, the commercial sector, and the government necessary to establish the networks for a collective defense *ahead* of a major crisis and, has the added benefit of achieving security, safety, and stability goals during peace time.<sup>37</sup>

## **ALWAYS VIGILANT FOR AMERICA: CIVIL AIR PATROL**

The Civil Air Patrol (CAP) dates to 1941, when Gill Robb Wilson, a World War I aviator launched a program he had dedicated his post-war years to designing: the Civil Air Defense Services (CADS).<sup>38</sup> In the end, CADS was approved by the Commerce, Navy, and War Departments in November, and the newly dubbed CAP opened its national headquarters on December 1, 1941. As an organization, CAP provides a model for what an American civilian cyber defense program could look like. CAP offers its members a way to serve the nation without joining the military, and a CCD can do the same.

As an all-volunteer organization that educates young individuals and trains the next generation of aviation leaders, CAP is committed to service and development. Science, technology, engineering, and math (STEM) education is considered its capstone mission, and CAP has invested heavily in STEM initiatives since the organization's beginning.<sup>39</sup> Additionally, emergency preparedness and response are central to CAP's mission, as evidenced by its critical imagery collection of Ground Zero after 9/11.<sup>40</sup>

Organized like the U.S. Air Force (USAF), CAP provides a military leadership structure that promotes accountability and ensures that the CAP mission, values, and goals are supported by its affiliated chapters. The link to the military chain-of-command allows for a set of detailed and understandable consequences for any individual who breaks rules or regulations. It is especially critical to CAP's legitimacy that it remains accountable and transparent—as it receives federal funding for its programs and is a part of the USAF's operational mission. The oversight provided by a congressionally mandated program is important for at least two reasons. First, it guarantees that the CAP and all its local units are aligned with national priorities by synchronizing efforts across state lines. Second, congressional oversight helps ensure that citizens' groups act within the confines of the law.

The principles that shape CAP's relationship with the USAF—such as volunteerism and saving lives—provide a framework for nesting a CCD under the leadership of the newest branch of service, U.S. Space Force, which does not have a reserve or auxiliary component. While CAP already designates funding and efforts to STEM and cyber education, a dedicated CCD can take the CAP model and expand on its STEM mission to bring in a broader range of cybersecurity professionals, veterans, and businesses to help construct a dynamic cybersecurity ecosystem within the U.S. CCD's vision. Developing this infrastructure would help to bring cybersecurity awareness to the American public and promote responsible digital citizenship.

## A SPACE MAP: CREATING A CIVIL AIR PATROL FOR CYBERSPACE

The principles that shape CAP's relationship with the USAF provide a framework for nesting a CCD under the leadership of a military branch. To create regionally and community aligned volunteer units, the CCD should be the Space Force Auxiliary Force. Aligning the CCD under Space Force would give the organization clear funding lines and pre-existing oversight mechanisms and, since the successful CAP model already exists, policymakers should be optimistic about the CCD concept too. Further, while aligning a CCD to U.S. Cyber Command (USCYBERCOM) may seem more natural, Space Force recruited its current members from the highly technical branches of the pre-existing military services - all of which also comprise the jointly staffed USCYBERCOM. Furthermore, with the Triad concept,<sup>41</sup> Space Force has started working closer with USCYBERCOM and U.S. Special Operations Command (USSOCOM) to defend in and across domains. As such, situating the CCD within Space Force reserve's component would develop a network of cooperation that could cross domains and Services. Ultimately, placing the CCD under Space Force oversight would integrate it into a highly technical service with a streamlined, singular line of authority, avoiding the potential for a cumbersome and financially contentious bureaucratic structure.

Oversight is important for at least two reasons. First, it guarantees that the CCD, and all its local chapters, are aligned with national priorities by synchronizing efforts across state lines. Second, a military hierarchy allows for the establishment and enforcement of parameters couched within legal confines to prevent citizens' groups from turning into localized cyber militias. While we do not deny that the U.S. government (USG) will have to accept additional risk by adopting the CCD model, we also hold that embedding the CCD within the Space Force hierarchy will manage that risk. By operating within the military framework, there will be greater control over the activities of citizen groups, reducing the potential for them to evolve into localized cyber militias. When thinking through the risk calculus for a CCD program, policymakers must weigh the risk of *not doing anything* versus the risk of utilizing non-military citizens to aid in national defense.

Beyond providing oversight, tying the CCD to DoD, and specifically to Space Force, makes sense for at least three additional reasons. First, just as with the Estonian model, the CCD offers everyday citizens a chance to give back to their nation. Many seek out alternative service opportunities, like AmeriCorps or the Peace Corps, and the CCD will provide another service option for cyber-skilled individuals to use their talents for the benefit of national defense. For these individuals, tying the CCD to a military service will help replicate the unique *esprit de corps* found in the armed forces, and may provide a powerful incentive to join the CCD. Additionally, veterans of the armed forces with cyberspace experience will be an important asset for CCD regional teams. As skilled individuals cycle out of uniformed service, the CCD will provide them an opportunity to continue their work of defending the nation and to experience a camaraderie with like-minded volunteers.



Second, alternative agencies, such as the Cybersecurity and Infrastructure Security Agency (CISA), are already under-resourced. Not only is Space Force's proposed government fiscal year 2022 budget nearly an order of magnitude larger than CISA's,<sup>42</sup> Space Force also has more than five times the personnel.<sup>43</sup> To date, Space Force does not have a reserve or auxiliary component, something experts have argued is essential for future national security.<sup>44</sup> It is in the Space Force's interest to keep its highly skilled workforce, and particularly its officers leaving active duty, in a part-time status to retain their skills. USCYBERCOM and all cyber-trained military service members are likewise valuable assets that USG is trying to retain. A CCD could address the persistent issue of talent attrition and brain drain that cyber-focused military roles and government entities face, as outlined in the Cyberspace Solarium Commission's report.<sup>45</sup> A CCD is necessary to provide both a way for separating personnel to continue to serve and can provide the Space Force with critical civilian experience.

Third, DoD is uniquely positioned to provide a far larger amount of on-the-job professional training and education than any other USG department or agency.<sup>46</sup> This capability is essential given the large variation in backgrounds and skillsets a volunteer organization like a CCD will attract. Professional education and training can help ensure that all volunteers, despite diverse backgrounds and skillsets, possess a common knowledge base. It can also help further instantiate *esprit de corps* and help educate members on the importance of accountability and their obligations to the organization. Cybersecurity and IT-related certifications are expensive when not provided by employers and CCD will be an avenue for professionals to gain and maintain key certification credentials and help build a more cybersecurity-educated public. Finally, CAP trains, mentors, and provides its members and cadets with an opportunity to serve their community, state, and nation and, a CCD can do the same for technology professionals.

Using CAP as a model, a CCD will provide cyber-focused community education and emergency response efforts by recruiting a broad range of cybersecurity professionals, veterans, and businesses to help foster a more robust cybersecurity ecosystem within the U.S. The CCD's vision should be to bring cybersecurity awareness to the American public to ensure that every citizen is also a responsible digital citizen and every business, and local government, is a secure one. To achieve that vision, the CCD should capitalize on CAP's community-oriented approach to training, education, and security. Critically, the volunteer nature of the CCD does not mean the units will be staffed by amateurs – like CAP, with its skilled pilots and alternatively skilled, but equally essential, supporting positions, the CCD will be a group of volunteers dedicated to the collective cybersecurity of the U.S. and comprised of technical experts, cadets and students, and community members interested in supporting CCD's mission.

## **CYBERSECURITY IS A SHARED RESPONSIBILITY: CIVILIAN CYBER DEFENSE**

As a program modeled on CAP, the CCD will be a congressionally chartered, federally supported non-profit corporation that serves as the official civilian auxiliary of the U.S. Space Force and will be established as an organization by Title 10 of the United States Code with its duties, roles, and responsibilities detailed by legislation. A key tenet of the CCD is educating the public on cybersecurity and how to recognize and manage attacks and vulnerabilities. Importantly, CCD members will not require security clearances as they will not be using or accessing critical systems. Any abnormalities or vulnerabilities would be reported, potentially to CISA, to enhance the nation's overall cybersecurity posture by informing federal-level entities about cyber threats at the local level and by engaging in two-way sharing. The focus of the organization will be on resiliency, response, and rebuilding with a strict mandate to advise, educate, and remediate.

As a volunteer organization, a CCD will seek to influence cybersecurity awareness, beginning at the local levels – from the individual to the small businesses that make up American communities. And, due to its local focus, the CCD would have a natural affinity to other civic minded groups. These groups, in addition to their local concerns, are passionate about teaching people. The CCD can leverage those connections and provide seminars on improving cybersecurity and understanding cyberspace risk. Partnering with local chapters of organizations like the Neighborhood Watch, Rotary, Toastmasters, Chamber of Commerce, Veterans of Foreign Wars, and others, would enable a CCD to deliver education in STEM and cyber-related issues to increase awareness and digital literacy skills among professionals, seniors, and youth.

Emergency preparedness and response is another central tenet – a CCD could leverage its local resources and talent to aid in the rebuilding of systems and advise on defensive measures. Advising local businesses, assisting school and education systems wanting to establish or improve cybersecurity baselines, better protect student data, and working to deter attacks like ransomware, are all services an all-volunteer auxiliary service could provide. Should these proactive efforts not suffice, local individuals and organizations could also activate their local branch of the CCD to help them remediate and report cyberattacks. Like its CAP counterpart, the CCD will be a critical component of emergency response by helping to restore services and provide networks in the event of a natural or physical disaster.

As alluded to throughout this article, a CCD, like an Estonian CDL, would be a local organization. This has several benefits. First, it gains trust with the local community. In fact, ideally, members of the CCD would come from the communities they serve. Local participation is important as it allows the CCD to access users like a small business owner who may not welcome government assistance. Rather, by having someone from the community who may know the person experiencing a cybersecurity issue, there is a higher likelihood that the person requesting support will be open to CCD help or more likely to ask for help when needed, which could raise overall awareness of cybersecurity issues across all levels of government and provide



policymakers with a clearer picture of the threat landscape. Moreover, once the CCD member is accepted into the social space of the person requesting support, they can educate them further on their individual role in providing collective cyberspace security. As research has noted, individuals are more likely to trust information from people they know and trust already.<sup>47</sup>

## CONCLUSION

U.S. adversaries have mastered how to operate in the gray zone and are consistently conducting operations in and through cyberspace that fall below the threshold of armed conflict.<sup>48</sup> Despite the large number of cyberattacks that target private and small businesses, the USG remains risk-adverse to involving the public in defending the nation in cyberspace. Meanwhile, adversaries employ their own civilian actors within cyberspace and continue to impose cost.<sup>49</sup> The U.S. has been slow to respond to this evolving landscape because its traditional framework does not adequately account for this gray zone or persistent competition. However, by adapting and creating the CCD and incorporating it into the national defense strategy it will enhance domestic resilience in the face of cyber threats and bring the U.S. closer to developing a more effective cybersecurity ecosystem to address the challenges posed by constant competition in cyberspace.

This article does not advocate for allocating offensive capabilities or authorities to a civilian cyber force,<sup>50</sup> rather encourages policymakers to consider the benefits of a CCD to community cyber response efforts as part of a national defense.<sup>51</sup> The CCD's focus would include providing localized cybersecurity resilience and response resources, educating citizens on cyberspace risk and cyber hygiene, and other education and resilience focused programs designed to elevate cybersecurity awareness and knowledge. Because U.S. adversaries directly target private citizens, businesses, and local governments, we are engaged in an undeclared conflict in cyberspace and to effectively respond, the American public needs to be involved.

The CCD's actions collectively amount to a localized defensive effort to deny an adversary access to our systems and networks. CCD efforts also would be scalable and reactionary in times of national need. Moreover, since the CCD would be a civilian auxiliary force focused on building community resiliency, its work would be unclassified, allowing for a broader and more diverse membership. The U.S. should use citizen volunteers to defend (and report) in cyberspace to augment its broader strategic-level efforts and bridge the public-private divide. With CCD support at the local and community levels, the U.S. military and other national-level cyber assets can focus their concern on achieving strategic objectives.

Acknowledging that the American public needs to be involved in cybersecurity for national defense is a crucial first step toward developing a holistic cybersecurity ecosystem and resilient civilian network. A robust and layered cybersecurity strategy requires citizen engagement and participation. The U.S. must think unconventionally about who can, and should, defend the nation and get *everyone* involved in securing cyberspace. It is time for a Civil Cyber Defense.🛡️

## NOTES

1. Nicole Perlroth, “The Chinese Hackers in the Back Office,” *The New York Times*, June 11, 2016, <https://www.nytimes.com/2016/06/12/technology/the-chinese-hackers-in-the-back-office.html>.
2. Ibid.
3. Jeff Bell, “Small Business Cybersecurity 101: Simple Tips to Protect Your Data,” *Forbes*, June 14, 2021, <https://www.forbes.com/sites/forbestechcouncil/2021/06/14/small-business-cybersecurity-101-simple-tips-to-protect-your-data/>.
4. Ibid.
5. David Blisson, “The State of Small Business Cybersecurity in 2021,” *Security Intelligence*, May 20, 2021, <https://securityintelligence.com/articles/state-small-business-cybersecurity-2021/>.
6. Jason Johnson, “6 Security Challenges Facing SMEs Heading Into 2021,” *InformationSecurityBuzz*, December 11, 2020, <https://informationsecuritybuzz.com/6-security-challenges-facing-smes-heading-into-2021/>.
7. Andrew Peterson, “Why Wall Street is worried about state and local government cybersecurity,” *The Record*, <https://therecord.media/why-wall-street-is-worried-about-state-and-local-government-cybersecurity/>.
8. Andrew Peterson, “Why Wall Street is worried about state and local government cybersecurity,” *The Record*, <https://therecord.media/why-wall-street-is-worried-about-state-and-local-government-cybersecurity/>.
9. U.S. Small Business Administration. “Stay safe from cyber threats” 2021, <https://www.sba.gov/business-guide/manage-your-business/stay-safe-cybersecurity-threats>.
10. Paola Peralta, “Small businesses are leaving themselves vulnerable to cyber attacks,” May 3, 2022, *Employee Benefit News*, <https://www.benefitnews.com/news/small-businesses-arent-investing-in-cybersecurity>.
11. Peter High. “Lessons From The Most Digitally Advanced Country In The World.” *Forbes*, January 15, 2018.
12. Sharon Cardash, Frank Cilluffo, and Rain Ottis. “Estonia's cyber defence league: A model for the United States?” *Studies in Conflict & Terrorism* 36, no. 9 (2013): 777-787.
13. Samuel Stolten, “Estonian president calls for more NATO troops to defend against Russia threat,” January 13, 2022, *Politico*, <https://www.politico.eu/article/estonian-president-calls-for-more-nato-troops-to-defend-russian-threat/>.
14. Kevin Kohler, “Estonia's National Cybersecurity and Cyberdefense Posture.” *Center for Security Studies (CSS) at ETH Zurich*, September 7, 2020, <https://css.ethz.ch/en/services/digital-library/publications/publication.html/2d-d8caf3-6741-435b-8b4d-a4df92e67bcb>.
15. Kevin Kohler, “Estonia's National Cybersecurity and Cyberdefense Posture.” *Center for Security Studies (CSS) at ETH Zurich*, September 7, 2020, <https://css.ethz.ch/en/services/digital-library/publications/publication.html/2d-d8caf3-6741-435b-8b4d-a4df92e67bcb>.
16. Kaitseliit, “Estonian Defence League,” <https://www.kaitseliit.ee/en/edl>.
17. Nasser Abouzakhar, ed., “ECCWS2015-Proceedings of the 14th European Conference on Cyber Warfare and Security 2015: ECCWS 2015.” *Academic Conferences Limited*, 2015.
18. Sharon Cardash, Frank Cilluffo, and Rain Ottis. “Estonia's cyber defence league: A model for the United States?” *Studies in Conflict & Terrorism* 36, no. 9 (2013): 777-787.
19. Viljar Veebel, Illimar Ploom, Liia Vihmand, and Krzysztof Zaleski. “Territorial Defence, Comprehensive Defence and Total Defence: Meanings and Differences in the Estonian Defence Force.” *Journal on Baltic Security* 6, no. 2 (2020).
20. Kadri Kaska, Anna-Maria Osula, and Jan Stinissen, “The cyber defence unit of the Estonian defence league: Legal, policy and organisational analysis.” 2013, *NATO Cooperative Cyber Defence Centre of Excellence*, [https://ccdcoc.org/sites/default/files/multimedia/pdf/CDU\\_Analysis.Pdf](https://ccdcoc.org/sites/default/files/multimedia/pdf/CDU_Analysis.Pdf).
21. Sharon Cardash, Frank Cilluffo, and Rain Ottis. “Estonia's cyber defence league: A model for the United States?” *Studies in Conflict & Terrorism* 36, no. 9 (2013): 777-787.
22. Greg Austin, ed., *National cyber emergencies: The return to civil defence*. Routledge, 2020.
23. Monica Ruiz, “Establishing volunteer US cyber defense units: A holistic approach.” In 2017 *International Conference on Cyber Conflict* (CyCon US), pp. 45-58. IEEE, 2017.
24. Sharon Cardash, Frank Cilluffo, and Rain Ottis. “Estonia's cyber defence league: A model for the United States?” *Studies in Conflict & Terrorism* 36, no. 9 (2013): 777-787.
25. Monica Ruiz, “Establishing volunteer US cyber defense units: A holistic approach.” In 2017 *International Conference on Cyber Conflict* (CyCon US), 45-58. IEEE, 2017.

## NOTES

26. Viljar Veebel, Illimar Ploom, Liia Vihmand, and Krzysztof Zaleski. "Territorial Defence, Comprehensive Defence and Total Defence: Meanings and Differences in the Estonian Defence Force." *Journal on Baltic Security* 6, no. 2 (2020).
27. Çederts Çelzis, "Estonian voluntary cyber-soldiers integrated into national guard." *Deutsche Welle*, May 4, 2011.
28. Ruiz, "Establishing volunteer US cyber defense units: A holistic approach," 5-58. IEEE, 2017.
29. Ibid.
30. Viljar Veebel, Illimar Ploom, Liia Vihmand, and Krzysztof Zaleski. "Territorial Defence, Comprehensive Defence and Total Defence: Meanings and Differences in the Estonian Defence Force." *Journal on Baltic Security* 6, no. 2 (2020).
31. Tom Gjelten, "Volunteer cyber army emerges In Estonia." National Public Radio (4 January 2001), <http://www.npr.org/2011/01/04/132634099/in-estoniavolunteer-cyber-army-defends-nation> (2011).
32. Monica Ruiz, "Is Estonia's Approach to Cyber Defense Feasible in The United States?" *War on the Rocks*, January 9, 2018.
33. Ruiz, "Establishing volunteer US cyber defense units: A holistic approach," 45-58. IEEE, 2017.
34. Ibid.
35. Viljar Pernik and Emmet Tuohy. "Interagency Cooperation on Cyber Security: The Estonian Model." In *Effective Inter-Agency Interactions and Governance in Comprehensive Approaches to Operations*, NATO STO Symposium Proceedings AC/323 (HFM-236) TP/579. 2014.
36. Viljar Veebel, Illimar Ploom, Liia Vihmand, and Krzysztof Zaleski, "Territorial Defence, Comprehensive Defence and Total Defence: Meanings and Differences in the Estonian Defence Force." *Journal on Baltic Security* 6, no. 2 (2020).
37. Eneken Tikk, "Civil defence and cyber security: A contemporary European perspective." In *National Cyber Emergencies*, 76-92. Routledge, 2020.
38. Civil Air Patrol, "History of Civil Air Patrol," <https://www.gocivilairpatrol.com/about/history-of-civil-air-patrol>
39. Legal Information Institute, "36 U.S. Code § 40302 - Purposes," <https://www.law.cornell.edu/uscode/text/36/40302>.
40. Jim Moore, "The Only Skyhawk in The New York Sky," AOPA, September 10, 2020, <https://www.aopa.org/news-and-media/all-news/2020/september/10/the-only-skyhawk-in-the-new-york-sky>.
41. Jen Judson, "Army Space, Cyber and Special Operations commands form 'triad' to strike anywhere, anytime." *Defense News*, August 11, 2022, <https://www.defensenews.com/smr/space-missile-defense/2022/08/11/army-space-cyber-and-special-operations-commands-form-triad-to-strike-anywhere-anytime/>.
42. Maggie Miller, "House Lawmakers Propose Major Budget Increase for Key Cyber Agency." *The Hill*, June 29, 2021; Pope, Charles. "FY22 Budget Gives Air & Space Forces the Strength to meet Threats, Roth, Brown, Raymond Tell Senate." *Space Force News*, June 8, 2021.
43. Eric Geller, "Senate Confirms Jen Easterly as Head of U.S. Cyber Agency." *Politico*, July 12, 2021; Pope, Charles. "Space Force selects more than 900 personnel to transfer FY22." *Space Force News*, September 30, 2021.
44. Brent Ziarnick, "An aggressive Space Force begins with a Space Force Reserve," *The Hill*, May 5, 2020, <https://thehill.com/opinion/national-security/494796-an-aggressive-space-force-begins-with-a-space-force-reserve>.
45. Cyberspace Solarium Commission, 2020. US Cyberspace Solarium Commission Final Report.
46. Barnett Koven and Katy Lindquist, *Barriers to Special Operations Forces-Led Counterterrorism Effectiveness*. Joint Special Operations University Press. 2021.
47. Roderick Kramer. "Rethinking Trust." *Harvard Business Review*, June 2009.
48. Joseph Votel, Charles Cleveland, Charles Connett, and Will Irwin. "Unconventional warfare in the gray zone." *Joint Forces Quarterly* 80, no. 1 (2016): 101-109.
49. Mark Grzegorzewski and Chris Marsh. "Incorporating the Cyberspace Domain: How Russia and China Exploit Asymmetric Advantages in Great Power Competition." *Modern War Institute*, March 15, 2021.
50. Wilson VornDick. "From Minutemen to Byteforce: Unleash an American Cyber Auxiliary & App," *19fortyfive*, June 29, 2021, <https://www.19fortyfive.com/2021/06/from-minutemen-to-byteforce-unleash-an-american-cyber-auxiliary-app/>.
51. U.S. Department of Defense. "Department of Defense Law of War Manual." Accessed September 14, 2021. <https://dod.defense.gov/Portals/1/Documents/pubs/DoD%20Law%20of%20War%20Manual%20-%20June%202015%20Updated%20Dec%202016.pdf?ver=2016-12-13-172036-190>.



# US Allies Offensive Cyber: Entrapment Risk or Entanglement Nuisance

---

Major Mikkel Storm Jensen, Ph.D.

## INTRODUCTION

“I would now like to say something very important for those who may be tempted to interfere in these developments from the outside. No matter who tries to stand in our way or all the more so create threats for our country and our people, they must know that Russia will respond immediately, and the consequences will be such as you have never seen in your entire history.”

*- Vladimir Putin’s speech when Russian forces invaded Ukraine February 24, 2022.*

Putin’s threat to escalate the war in Ukraine in response to external interference presents a timely reason to reconsider who has the military means to trigger escalation and perhaps draw allies into the conflict. In 1984, Glenn H. Snyder wrote an analysis of states’ dilemmas in alliances with this issue at its core that has demonstrably had excellent explanatory and predictive power.<sup>1</sup> In the Cold War’s technological strategic context of nuclear and conventional military means, he found that: “In general, entrapment is a more serious concern for the lesser allies than for the superpowers [...] because the superpowers have a much greater capacity for taking initiatives (notably nuclear initiatives).”<sup>2</sup>

In NATO, the US controls much of the alliance’s conventional military capabilities and most of its nuclear weapons. Applying Snyder’s analysis, this vests the US with a sufficient level of control over NATO’s crisis management, to minimize the US’ risk of entrapment in conflicts. Emergence of cyberspace<sup>3</sup> as a new venue for military operations



**Mikkel Storm Jensen (Ph.D.)** is a major in the Danish army with an operational background in intelligence analysis. Since 2016, he has researched national cyber strategies. Initially on the state's role in societal resilience, but now mostly focuses on their use of cyber means for offensive purposes. This article forms part of his dissertation<sup>4</sup> on the influences of offensive cyber capabilities on military alliances, which he defended in May 2023.

changes the US strategic environment.<sup>5</sup> The US was initially NATO's only declared actor in cyberspace, but over the last decade more than half of NATO's members have begun developing offensive cyberspace operations (OCO) capabilities.<sup>6</sup> Based on Snyder's analysis, should the US add proliferation amongst friends and allies to its concerns over OCO proliferation amongst foes?<sup>7</sup>

The theoretical answer is "yes." Any increase in allies' potential for independent initiatives decreases US ability to control escalation, increasing the risk of entrapment. The real-world answer depends on the degree to which OCO has the potential for strategic impact. The counterargument is that OCO's potential military impact even in a crisis would be insignificant, thereby rendering allies' independent deployment of OCO a manageable risk insofar as entangling an otherwise involuntary US.

Hence, the question is the relative magnitude of the entrapment threat from US allies' OCO: Do US allies' growing OCO capabilities constitute a credible risk for entrapment, or are they a mere entanglement nuisance? US' strategies do not provide an answer.<sup>8</sup> Since 2018, they have signaled a more active role for US OCO capabilities to serve as a deterrent, both above and below the threshold of armed conflict. As yet, however, no guidance has been forthcoming as to how allies' OCO capabilities fit this intent.<sup>9</sup> Nor does the academic literature inform this subject, a void this article seeks to begin filling.

Following a brief review of pertinent academic literature, this article presents the theoretical tools deployed. After introducing mainly Snyder's analysis of alliance dilemmas, the theories are applied to the case of the US dominant position in NATO. The analysis then investigates OCO's influence on the outcomes of Snyder's analysis on entrapment by analyzing how the technical and operational attributes of military cyber capabilities effects differ from conventional and

nuclear means. It demonstrates how OCO are, in some respects, reasonable to analyze on par with nuclear weapons. The article then reviews the US-published statements and policies on her own and allies' OCO capabilities and compares with US policies during the late 1950s potential proliferation of nuclear weapons amongst NATO members.

The analysis establishes that OCO's potential for destruction is not comparable to nuclear weapons but still convincingly capable of creating strategic effects, e.g., escalation, particularly during a crisis. Thus, in Snyder's terms, OCO convincingly provides allies with new means for "independent strategic initiatives" and constitutes an entrapment risk to the US, particularly during a crisis, albeit less so than nuclear weapons. Furthermore, OCO-proliferation among US allies will be harder to detect and assess than nuclear capabilities. Also, influencing allies' decisions on OCO development will require different efforts than counter-ing allies' nuclear proliferation. Without aspiring to recommend whether the counter proliferation of NATO allies' OCO capabilities should be a US strategy, these findings suggest that the US could consider incentivizing allies by issuing statements on how to best develop OCO capabilities to support US policy objectives.

Two final caveats should be stated before proceeding to the analysis: Firstly, the analysis is based solely on information available to the public. Hence, classified arrangements between the US and allies may exist, rendering the points on the US' lack of shared strategic intents regarding allies' OCO moot. However, the findings on allies' potential as entrapment risk and the challenges with handling that risk still hold. Secondly, this analysis fully recognizes that for most NATO allies, going against the interests of the US, particularly in crisis or war, is something they would likely be highly reluctant to do. Again, this does not change the fact that states may act irrationally or out of desperation. Hence the analysis remains relevant.

### *Some Literature on Military Use of Cyber and Alliances*

The academic literature on OCO as military means has grown significantly over the last decade, particularly from the either explicitly or implicitly assumed great power perspective. Both theoretically, e.g., Libicki, and empirically, e.g., Brandon et al.<sup>10</sup> From the technical perspective, e.g., Schneider has argued why information technology represents a military revolution rather than an evolution.<sup>11</sup> Harknett and Smeets have reviewed the literature extensively and convincingly to discuss in what ways and how significantly offensive cyber operations can affect interstate conflict, but contribute mainly with focal points for further research.<sup>12</sup> Cimbala specifically investigates OCO's potential effects as a means for escalation management in general and the risks of nuclear weapons becoming involved.<sup>13</sup>

However, this literature is from the perspective of individual states. The literature is very limited regarding the use of OCO in or by military alliances: Taillat takes a close look at how some of the special technical and operational characteristics of OCO influence collective security in general, but do not investigate their impact on military alliances.<sup>14</sup> Smeets and



Fasana both discuss the values and risks of integration of offensive cyber in military operations, but neither look into its use in coalitions.<sup>15</sup> Relevant is also Ang's analysis of why and how small states, even if they are part of military alliances find it more difficult than large states to react to hostile activities in the cyber domain below the threshold of armed conflict.<sup>16</sup> Hughes and Colarik touch very briefly upon the theoretical utility of OCO within New Zealand's military cooperation with Australia.<sup>17</sup> However, they do not address challenges arising from the particular attribute that OCO are likely kept secret from allies. Instead, they assume that allies will share information on OCO within the Five Eyes intelligence collaboration network. Thus, Hughes et al neither question the interoperability of OCO in the coalition nor whether Australia or other allies will appreciate New Zealand's acquisition of offensive cyber or may have concerns, entrapment, or otherwise. Their assumption of information sharing is not likely to hold. Allies have strong incentives to keep OCO secret, as demonstrated by NATO's SCEPVA-framework (more on that later) for conducting OCO without sharing information.<sup>18</sup> White has analyzed some aspects of how cooperation in alliances on OCO and capabilities should be organized, but like Hughes et al, White does not address the challenges from classification of offensive cyber means.<sup>19</sup> Another aspect of potential concern over allies' OCO is provided by Jacobsen who highlights the secrecy induced technical risks to US cyber enabled intelligence collection.<sup>20</sup> Smeets has touched upon the threat from entrapment (as defined later in the article) to US allies from US operations conducted in or through the allies' cyberspace and also described NATO's emerging policies in the field.<sup>21</sup> This article aspires to enhance the academic understanding by looking at the entrapment threat from the US perspective.

## **ENTRAPMENT, ENTANGLEMENT, AND ABANDONMENT**

The question posed in this article concerns the effect of emerging military technologies on alliances seen from the perspective of the alliance's senior partner. It is a question primarily directed toward the state's considerations and resulting actions regarding risks from being in alliances. It deals in matters of complex security and actions, perhaps clandestine, for *raison d'état* rather than based on emerging interstate norms, the composition or interpretation of alliance treaties, or strategic culture. These are core analytical parameters of Realism, making that analytical prism a reasonable choice.

Glenn H. Snyder's pioneering *The Security Dilemma In Alliance Politics* provides a standard reference Realist framework for exactly such analysis.<sup>22</sup> In this, Snyder investigates the risk and trade-offs for states seeking security in an anarchic international system through alliances, deploying Mandelbaum's concepts of abandonment and entrapment to depict the negative counterpoints to the states' positive objective of increased security.<sup>23</sup> For more detailed analysis of how the dominant ally and its security dependent allies interact, Lake's *Entangling Relations* provides valuable perspectives.<sup>24</sup>



From the US perspective, Snyder's key concept in the present analyses is entrapment: "Entrapment means being dragged into a conflict over an ally's interests that one does not share, or shares only partially. The interests of allies are generally not identical; to the extent they are shared, they may be valued in different degree."<sup>25</sup> Snyder credits Mandelbaum for the term as he identified entrapment as a strategic risk in Thucydides' account of the Peloponnesian Wars:

"When Corcyra seeks an alliance with Athens, the Corinthians, the enemies of Corcyra warn the Athenians that accepting the Corcyrians as allies will lead to entrapment: "You will force us to hold you equally responsible with them, although you took no part in their misdeed."<sup>26</sup>

Mandelbaum, Snyder and Thucydides are all concerned with entrapment's worst-case scenario, namely involuntary involvement in a war because of an alliance. To investigate aspects of entrapment risks with less severe consequences, the analysis draws upon Kim's use of the term entanglement.<sup>27</sup> Kim renames Snyder's entrapment entanglement and defines it as a process whereby a state is compelled to aid an ally in an unprofitable enterprise because of an alliance. Kim then redefines and reintroduces entrapment as a separate subset of entanglement: "... a form of undesirable entanglement in which the entangling state adopts a risky or offensive policy not specified in the alliance agreement."<sup>28</sup>

In other words, Kim defines entanglement as a less serious, negative risk than entrapment. It should be noted that Kim's use deviates from another use of the term "entanglement" to describe the degree to which states are formally and politically bound in an alliance. In this neutral interpretation, entangling is not necessarily harmful and may even be the defining objective of the alliance.<sup>29</sup> The present analysis uses Snyder's and Mandelbaum's term *entrapment* for the most serious risks, e.g., those that may lead to war, and Kim's term *entanglement* for risks that have less serious, although still negative consequences.

Snyder's other key concept is abandonment. Abandonment is, mainly when there are little or no alternatives to the dominating ally as a security guarantor, primarily a concern for the smaller, dependent allies: "alliances are never absolutely firm, whatever the text of the written agreement; therefore, the fear of being abandoned by one's ally is ever-present. Abandonment, in general, is "defection," but it may take a variety of specific forms: the ally may realign with the opponent; he may merely de-align, abrogating the alliance contract; he may fail to make good on his explicit commitments; or he may fail to provide support in contingencies where support is expected."<sup>30</sup> Small allies' fear of abandonment may lead to independent and, from the perspective of the dominating ally, entrapping actions: "Asymmetries in indirect dependence chiefly affect the partners' relative fears of abandonment. Thus, when one state has a stronger strategic interest in its partner than vice versa, the first will

worry more about abandonment than the second.” Security dependent allies’ concerns and the resulting reactions are well demonstrated by De Gaulle’s question to Kennedy In 1961: “... whether we [the US] would be ready to trade New York for Paris.”<sup>32</sup> Thus France acquired an independent nuclear arsenal against the US wishes to ensure escalation in case of a Soviet invasion.<sup>33</sup>

## **THE US DOMINANT POSITION IN NATO AND THE RISK OF ENTRAPMENT**

NATO is a relevant empirical case study of alliances: It is the US’ oldest and largest collective defense arrangement. Furthermore, most NATO members have technologically advanced economies that bring OCO capabilities within their reach without significant additional investments. At least sixteen members already claim to pursue such means.<sup>34</sup> NATO’s efforts to integrate OCO since at least 2018 provide empirical evidence to the analysis and have produced academic debate and concrete outcomes, e.g., doctrines and organizational adaptations like the Cyberspace Operations Centre (CyOC).<sup>35</sup> Furthermore, NATO’s well-documented history allows investigation of historical analogies of emerging technologies.

Snyder argues that the threat from entrapment to alliance members, in general, is lesser the more they are in control of the alliance’s capabilities for initiatives with the potential to have strategic impact.<sup>36</sup> Military capabilities are in this analysis considered to be of strategic value if they have the potential to significantly influence outcomes in military conflict management.<sup>37</sup> According to Snyder, the large US military capabilities relative to her allies, have been a key reducing factor in the risk from entrapment in NATO.<sup>38</sup> The threat from escalation of the war in Ukraine right on the border of NATO accentuates the relevance of assessing allies’ emerging OCO-capabilities potential influence on crisis management: if allies’ OCO are strategically significant, Snyder suggests they increase US risk from entrapment.

US concerns over entanglement and entrapment were present during the formation of NATO.<sup>39</sup> This may explain why the key Article 5 in the treaty leaves some leeway – “such action as it deems necessary” – for the allies to react in case of an attack.<sup>40</sup> Also, the US has mitigated NATO’s nominal anarchic nature, where, in principle, a consensus is needed on every decision, by occupying key nodes and positions, e.g., SACEUR, and thus dominating not only through the US forces in Europe but also by having extensive control over the internal procedures and debates.<sup>41</sup>

It would be a gross mischaracterization to assert that the US has wielded unrestricted hegemonic power over the alliance at any point in NATO’s history. NATO allies have often pursued policy objectives that differed from US interests, particularly when external threats were perceived as low.<sup>42</sup> However, the US has always been the senior partner with a decisive influence over the alliance.<sup>43</sup> The advantages provided by this dominant position have played a significant role in keeping the US invested in NATO after the demise of the USSR.<sup>44</sup>

The US position has been reinforced by European reluctance to transform economic growth into military power to the same degree as the US and exacerbated by a significant decline in conventional European capabilities after the Cold War.<sup>45</sup> The crisis between Russia and NATO over Ukraine highlights the European allies' military dependency on the US. Applying Snyder's analysis, the US central role in the alliance's crisis management reduces her risk of entrapment.

Aspects of the management of the war in Ukraine demonstrate the importance of US control over military actions that could lead to escalation – and hence implicitly if allies undertook them without US consent, to entrapment.<sup>46</sup> Military crisis management – including with cyber means – is to a large degree dependent on the opponent's perception.<sup>47</sup> Hence, it is vital to notice that Russia has hitherto perceived US influence in NATO as close to hegemonic, insisting on negotiating solely with the US.<sup>48</sup> Paraphrasing Thucydides' entrapment case, the Russian perception presents a risk that NATO allies' independent actions could lure Russia to hold the US responsible. The analysis will not discuss crisis management models,<sup>49</sup> but simply, recalling Mr. Putin's barely veiled nuclear threats to deter external interference in Ukraine, refer to the intuitive observation that the impact of actions initiated by allies without US knowledge or consent carries a greater risk for entrapping consequences when international tensions are high.

## **THE CHALLENGES FROM ALLIES' OFFENSIVE CYBER**

So how does proliferation of emerging military cyber capabilities influence these dynamics? Defensive cyberspace operations (DCO) do not represent coercive means and are thus irrelevant to the question of alliances' use of military force.<sup>50</sup> The analytical focus should therefore be on OCO. While current NATO doctrine only distinguishes between OCO and DCO,<sup>51</sup> US doctrines distinguish between two different subcategories of OCO, namely cyber-enabled espionage, Cyberspace Exploitation (OCO-CE), and destructive attacks, Cyberspace Attack (OCO-CA).<sup>52</sup> OCO-CE are intrusive but non-destructive operations to collect intelligence, while cyberspace attacks are operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.<sup>53</sup> The US Air Force's doctrine adds further nuances: they rename OCO-CE "cyberspace ISR" and then straddles the grey zone between exploitation and attack by dividing cyberspace attacks into Cyber Operational Preparation of the Environment (C-OPE) which are non-intelligence enabling activities conducted to plan and prepare for potential follow-on military operations, and Cyberspace Effects Operations that are actively destructive or disruptive.<sup>54</sup>

Compared to analog means, OCO-CE constitutes a paradigm shift in small allies' intelligence collection opportunities by widening the scope and lowering the costs and associated risks.<sup>55</sup> However, as espionage is not a new phenomenon, allies' OCO-CE does not per se present a new challenge to the dominant US position in NATO. Even so, OCO-CE cannot be

completely discarded as an entrapment risk, as OCO-CE for the purpose of situational awareness, can be difficult to distinguish from OCO-CE conducted as preparations for cyberspace attacks: C-OPE in USAF terms. Hence, any detected intrusion may be considered threatening by the targeted entity.<sup>56</sup>

Cyber enabled destructive attacks, however, arguably constitutes a paradigm shift. OCO-CA's technical and tactical properties challenge the traditional realist understanding of what is possible for large states but impossible for small states based on their available resources.<sup>57</sup> Hitherto, conventional military means with strategic reach or effect, e.g. an intercontinental missile force, a blue water navy or nuclear weapons, have required states to undertake obvious and significant investments and develop large military-industrial bases. Such costs have limited proliferation and the necessary infrastructure is visible from space which enables external observers to assess states' conventional and nuclear strategic capabilities' size and efficacy and may glean information regarding their owner's intent.

The emergence of OCO-CA has changed this situation and hence the strategic context. Small states can acquire the necessary means: the cost of entry into the OCO-CA capable group of states is relatively low. In principle, OCO require commercially available IT equipment and a team of qualified researchers, software developers, and operators optimized by coupling it with national intelligence services' collection capabilities.<sup>58</sup> OCO has unlimited geographical reach if targets are linked to the Internet. As demonstrated by STUXNET, OCO can reach air-gapped targets with some extra effort.<sup>59</sup> Unlike conventional strategic means, OCO do not require large military and industrial investments to develop and deploy, which means that they can be clandestinely developed with little or no recognizable signature.

Why is this important? As demonstrated above, the US dominates the decision process in NATO, reducing the risk of entrapment. Lake provides insights that supplement Snyder's on alliance dynamics based on access to information: In a hegemony, the hegemonic partner dominates the decision process of other allies e.g., whether to attack or how to react to external attacks. However, Lake argues it is difficult to eliminate local decisions, especially in the light of asymmetric information.<sup>60</sup> Hence, the ability to develop OCO-CA clandestinely reduces the hegemon's ability to eliminate the initiatives of other allies.

The relative ease with which OCO-CA can be developed clandestinely reinforces alliance members' inclination to keep them secret even from allies.<sup>61</sup> Involved software is produced by organizations typically within or associated with national intelligence services, whose highly classified and un-sharable intelligence is a prerequisite for the "tailored" part of OCO-CA capabilities with tailored access.<sup>62</sup> Likely even generic OCO-CA means are often kept secret at the national level – perhaps because the cyber domain is still a new and hence immature domain for conflict. Generic OCO-CA means have yet to be transferred from national intelligence organizations to regular military forces to become an everyday part of military operations on a par with other means.<sup>63</sup> The secrecy surrounding OCO, even in alliances,

is underlined by the fact that NATO has had to develop the concept of “Sovereign Cyber Effects Provided Voluntarily by Allies,” or SCEPVAs to integrate OCO-CA in operations via the Cyber Operational Command, or CyOC.<sup>64</sup> This allows members to offer NATO OCO-effects, without disclosing anything about what means are used and what objectives are targeted.<sup>65</sup> NATO’s joint doctrine for cyberspace operations acknowledges that this is a suboptimal way to manage operations.<sup>66</sup> Still, the procedure is a compromise that allows members to support NATO operations with OCO capabilities without disclosing classified information. Historical evidence on multilateral operations involving OCO-CA is currently limited to the 2016 campaign against ISIS: the UK, Australia, and the US all deployed offensive cyber.<sup>67</sup> It suggests that inter-organizational de-confliction just within the US was problematic, and decisions, whether to inform let alone involve allies presented constant dilemmas.<sup>68</sup>

## US STATED POSITIONS ON OWN AND ALLIES’ OFFENSIVE CYBERSPACE CAPABILITIES

The US is relatively clear regarding the roles of her OCO: in 2018, a new National Cyber Strategy announced increased emphasis on the role of OCO as a means of deterrence by punishment. The unclassified Strategy is kept very general but is a shift towards in-domain deterrence.<sup>69</sup> It came alongside new, classified directions for U.S. Cyber Command (USCYBERCOM) that was allegedly given a broader scope for OCO and higher thresholds before presidential authorization had to be given.<sup>70</sup> In public interviews and official hearings, Mr. John Bolton, the then National Security Advisor, and General Paul Nakasone, commander of USCYBERCOM and NSA since 2018, have stressed the importance of the US doctrine of “persistent engagement”. The persistent engagement doctrine requires the ability to be constantly present in other nation’s networks to identify threats as they develop and punish hostile actions.<sup>71</sup> The 2023 National Cybersecurity Strategy retains the former strategy’s stated intent to disrupt and dismantle threat actors.<sup>72</sup>

But while US strategies are clear regarding unilateral use of OCO, available information is sparse on the US intent regarding OCO’s role in alliances. Regardless of whether or not the US consider allies’ OCO-capabilities desirable additions to e.g. NATO’s arsenal, the lack of public statements on the subject may leave allies guessing how best to develop their military cyber capabilities. To allies, e.g., Denmark, that depend fully on US security guarantees, it is often more important how military acquisitions, whether F-35 or OCO-capabilities, contribute to strengthening the alliance with the US than how they contribute to national defense.<sup>73</sup>

NATO’s recent developments in the field do not provide conclusive answers: In line with the rest of the article’s argument that the US has a dominant position in NATO, the introduction of the CyOC and the SCEPVA procedures could be interpreted as implicit US approval of allies’ emerging OCO. However, an alternative explanation could be that the US mainly sees the SCEPVA procedure to allow for US OCO in NATO operations without disclosing information on ways and means to allies.

Declassified parts of the US 2006 Strategy and the 2012 Presidential Directive mention international collaboration on defensive cyber issues.<sup>74</sup> DCO, including multinational collaboration, are uncontroversial regarding entrapment and occur in several arenas, including NATO.<sup>75</sup> None of the US strategies apparently place high value on allies' OCO capabilities. Neither does any of them mention NATO regarding OCO. The 2023-strategy mentions NATO (in sect. 5.3), but only with regards to defensive and resilience initiatives.<sup>76</sup> The 2006 Strategy mentions international cooperation as the very last area under the section on partnering, after industry and interagency.<sup>77</sup> The 2017 National Security Strategy mentions allies in just one sentence on threat information sharing and mutual assistance in attribution, defensive and hence uncontroversial tasks.<sup>78</sup> The 2018 National Cyber Strategy hints vaguely at multinational collaborative efforts to punish misbehavior in the cyber domain but does not mention OCO directly:

The imposition of consequences will be more impactful and send a stronger message if it is carried out in concert with a broader coalition of like-minded states. The United States will launch an international Cyber Deterrence Initiative to build such a coalition and develop tailored strategies to ensure adversaries understand the consequences of their malicious cyber behavior. The United States will work with like-minded states to coordinate and support each other's responses to significant malicious cyber incidents, including through intelligence sharing, buttressing of attribution claims, public statements of support for responsive actions taken, and joint imposition of consequences against malign actors.<sup>79</sup>

This intent is reflected in a paragraph in very broad terms on collaboration in the Defense Department's cyber strategy.<sup>80</sup> The 2023-strategy states a similar objective in sect. 5.4. The new is not more specific than the former, but the wording "*collaborative use of all tools of statecraft*" could include OCO. As of November 2023, nothing concrete regarding this initiative has been disclosed.<sup>81</sup>

## **NUCLEAR WEAPONS – A SOMEWHAT REASONABLE COMPARISON WHEN CONSIDERING ENTRAPMENT**

What justifies seeking an understanding of the emergence of OCO-CA's influence on US alliance policies in the historical case of the emergence of nuclear weapons?

Firstly, high-ranking US politicians and military officers have compared their concern over the emerging threats posed by OCO-CA to the threat from nuclear weapons, and their Russian and Chinese counterparts have expressed similar statements.<sup>82</sup> To the degree these perspectives influence national policy, they are relevant regardless of which degree they are reasonable from a technical perspective. Hence, the fact that some US decision makers' concerns over the emergence and proliferation of OCO-CA are comparable to their concern



over nuclear weapons justifies comparison with their predecessors' concerns and policy decisions when these weapons entered the world stage.

Secondly, historical evidence suggests that technological changes in a strategic context have the potential to destabilize international relations and raise the risk of escalation, especially if they, like OCO-CA, are perceived as giving the aggressor an advantage.<sup>83</sup> Nye argues that even though OCO differs in many ways from nuclear weapons, lessons can be drawn from comparisons, e.g., the need to develop strategies without empirical evidence or historical experience.

Elaborate constructs and prevailing political fashion led to expensive conclusions based on abstract formulas and relatively little evidence. [...] Cyber has the advantage that with widespread attacks by hackers, criminals, and spies, there is more cumulative evidence of a variety of attack mechanisms and of the strengths and weaknesses of various responses to such attacks. [However] no one has yet seen a cyber war, in the strict sense of the word, as defined above. [Historical disclosed attack examples] give some inklings of the auxiliary use of cyber attacks, but they do not test the full set of actions and reactions in a cyber war between states. [...] the problems of unintended consequences and cascading effects have not been experienced.<sup>84</sup>

The Russian full-scale invasion in 2022 of Ukraine has provided some observations regarding the efficacy of OCO in interstate war amongst near-peer opponents. As of November 2023, Russian OCO-CA appears not to have achieved significant results at neither the tactical, operational or strategic level.<sup>85</sup> This is not for lack of trying, though, as Russia has deployed destructive malware against Ukraine throughout the conflict along with less disruptive, but highly profiled attacks against private and government entities in states supporting Ukraine.<sup>86</sup> The reasons for the lack of impact of OCO-CA in the conflict are debated. Likely they are a combination of offensive and defensive factors, e.g., less competent and resourceful Russian cyber forces and better Ukrainian cyber resilience (with external support from both states and private entities) than assessed prior to the conflict.<sup>87</sup> However, the information available for academic analysis is still sparse at this point, and the events of this war still leaves analysts room to theorize over OCO-CA's potential.

Obviously, possession of OCO-CA capabilities does not give a small state the same ability to conduct strategic power projection as a large state's conventional means, let alone nuclear weapons. Also, OCO-CA's usually (although, as demonstrated by, e.g., NotPetya, far from always) limited, temporary, and reversible effects are completely different from nuclear weapons' spectacularly enormous, permanent, and irreversible destructivity.<sup>88</sup>

That said, OCO-CA does provide small states new opportunities to reach out far beyond their borders and inflict serious damage, e.g., on critical infrastructure. US strategies acknowledge the theoretical potential for catastrophic damage from OCO-CA and include them in the threats that the US nuclear arsenal is tasked to hedge against.<sup>89</sup>



Furthermore, as argued by, e.g., Cimbala, OCO-CA's technical and operational attributes make it a destabilizing means with significant potential for crisis escalation.<sup>90</sup> The ambiguities that accompany OCO-CA may further exacerbate the risk of escalation: Commanders have limited situational awareness.<sup>91</sup> Discovering that he is under cyberattack, the victim may be left in doubt whether he has discovered the full extent of the intrusion. Also, the process of intelligence-based attribution may be time-consuming and initially provide insufficient, low-confidence answers.<sup>92</sup> Lack of information on what has happened, who did it, and what will happen next, combined with a lack of international norms and historical experience from empirical precedence to draw on can lead to several unfortunate decisions.<sup>93</sup> These include unintended escalation and counter strikes against third parties, especially if the victim is already under pressure, e.g., as an effect of a triggered security dilemma.<sup>94</sup>

As in the classical security dilemma, even non-destructive cyber operations with underlying defensive intent, e.g., OCO-CE intended as routine espionage to maintain normal levels of situational awareness, may be perceived as offensive – or to use the USAF's term: cyberspace operational preparation of the environment – by an opponent and trigger escalation.<sup>95</sup> This is especially pronounced in the cyber domain where a perceived, if debated, dominance of the offensive tends to push towards instability.<sup>96</sup> These properties combined with a likely lack of insight into the situational awareness and threat perceptions of the opponent(s) make OCO-CA or even OCO-CE a potentially de-stabilizing means in a crisis. Particularly if the OCO are directed (or even just perceived as directed) against the most sensitive areas, e.g., nodes in a belligerent's nuclear weapons command and control.<sup>97</sup> The 2018 U.S. Nuclear Posture Review specifically acknowledge the cyber threat to such nodes.<sup>98</sup>

Finally, there is a significant difference between the threshold for using nuclear weapons and OCO. The threshold for using nuclear weapons is arguably the highest for any military means, as it has not been used since 1945, and the means is arguably considered taboo.<sup>99</sup> In contrast, many states have demonstrated a very low threshold for using OCO, often below the threshold of armed conflict.<sup>100</sup>

To round off the discussion in Clausewitzian terms, OCO's potential for achieving positive political ends, e.g., concluding a conflict to one's advantage, is very open for debate.<sup>101</sup> Still, OCO's potential to achieve negative political ends, e.g., escalation of a crisis, appears convincing.<sup>102</sup> OCO as a means for controlling escalation in crisis and war, is largely a question of assumptions and educated guesses. The use of OCO signals in a crisis even more uncertainty than signaling with traditional military means, making escalation even more challenging to control.<sup>103</sup>

## **US ALLIES, ENTRAPMENT, AND NUCLEAR WEAPONS: A LESSON FROM THE PAST**

So, if OCO-capabilities' strategic risks with regards to military crisis management, particularly during a crisis and heightened international tensions, are in some regards comparable

to nuclear weapons, how did the US react in the late 1950s when some NATO allies and other friendly nations wanted to acquire their own nuclear arsenals?

A declassified National Intelligence Estimate (NIE) – a high-level strategic assessment collaboration between all the US intelligence services – on the topic from 1958 provides insights on US concerns.<sup>104</sup> The NIE was downgraded from secret to confidential in 1999 and declassified in 2004. Because the NIE was originally intended for internal use in the US government only, it was likely written without consideration for diplomatic signaling or politeness to either friends or foes. Hence, the analyst can arguably have high confidence in their insights into the US decision process. The NIE precedes Snyder's 1984 article on dilemmas in alliances by two decades, but the analysis precisely captures US concerns over entrapment and allies' concerns over abandonment, which is stated as a major driver for the allies' pursuit of nuclear weapons.<sup>105</sup>

In 1958, the UK acquired nuclear weapons in the face of stiff US opposition.<sup>106</sup> France had also overcome the US obstructions and was on the brink of deploying an arsenal. In Europe, West Germany, Italy, and Sweden – the last friendly nation but not a NATO member, were beginning to move towards this goal.

The NIE predicted no change in the basic international [bi-polar] system if the allies and friendly Sweden achieved some nuclear capabilities. However, while the states still regard the US alliance as essential, nuclear capabilities could render them less responsive to US policy. The NIE assessed the reduced US influence as a negative, risk-enhancing outcome and predicted that it would increase the risk for both conventional and nuclear war to an undetermined degree. "Such a development is certain to produce strain and difficulties if nothing worse" if the European allies used them "to achieve deeply felt" national aims or the weapons become available to "almost totally irresponsible governments."<sup>107</sup>

In accordance with Lake's theoretical expectations, the NIE indicates that while the US's dominant position in NATO helped control the political debate, it was insufficient to quell the allies' interest in acquiring nuclear weapons.<sup>108</sup> UK and France partially developed their arsenals out of fear of US abandonment. The French sought to keep their program clandestine until September 1958 but were unsuccessful, as the NIE detailed in July of that year. The US gained some control over the UK's arsenal by supplying its main delivery systems, leaving the UK capability somewhat reliant on US support. France, however, was able to keep its nuclear arsenal completely independent of the US.<sup>109</sup> West Germany was eventually dissuaded by US assurances of commitment, made credible by a massive US military presence within her borders that provided assurance but also ensured Germany's deep security dependence on the US.<sup>110</sup> Italy's interest in nuclear capabilities was more motivated by the pursuit of international prestige rather than immediate security concerns. After a half-hearted effort in the early fifties, Italy latched on to the German initiatives to gain leverage with the US on matters other than the nuclear issue. Hence, they were easy to dissuade.<sup>111</sup> Sweden approached

the US in the late fifties with requests for support for their nuclear program. They were turned down but offered to come under the US nuclear umbrella if Sweden abstained from pursuing nuclear weapons. An independent Swedish program was technically possible but so expensive that it likely undermined her conventional deterrence capabilities. Hence, Sweden gave up its efforts.<sup>112</sup> Instead, Sweden pursued neutrality and defensive autonomy based on extensive investment in conventional forces. However, tacit collusion and US economic and technical support were still necessary to achieve a sufficient quality of conventional forces for defensive autonomy, placing Sweden in partial dependency.<sup>113</sup>

Compared to the current emergence of OCO amongst NATO members, similarities and differences appear. Firstly, in 1958, the US was concerned over the potential nuclear proliferation among allies and friendly states for reasons Snyder would recognize as concerns over entrapment. Nuclear proliferation would increase their scope for strategic initiatives, undermining US control and increasing the risk of international “strain and difficulties if nothing worse” if they used them “to achieve deeply-felt” national aims.<sup>114</sup> Some of the US concern was founded in the recognition that allies’ fear of abandonment might lead them to take independent (nuclear) actions counter to US interests. The capacity to do so was recognized as a strong motivating drive for the allies, particularly France and West Germany’s pursuit of nuclear weapons. Today OCO, particularly OCO-CA, presents an entrapment risk of a similar nature—both from a technical effects-based perspective and regarding allies’ possible motivations to acquire OCO. The counter-argument is that the physical impact of OCO is less catastrophically violent than that of nuclear weapons, and hence only an entanglement risk is valid and relevant. But, as demonstrated above, OCO has significant potential for influencing, e.g., escalation, especially during a crisis.

Secondly, in 1958, nuclear weapons were expensive, scientifically challenging, and required complex means for delivery, which made the allies’ nuclear capabilities relatively easy for US intelligence to detect and assess.<sup>115</sup> Today, OCO can be developed by allies with technologically advanced economies, as most NATO members, and it can be done without leaving much in the way of an intelligence footprint. The counter-argument that OCO, unlike nuclear weapons, only constitute a risk of entanglement due to their smaller impact is again arguably less convincing because the much lower entry barrier for the acquisition of OCO makes them much more accessible, as demonstrated by the speed with which they are increasing in NATO.<sup>116</sup>

Finally, in 1958, despite the costs and challenges required by allies to acquire nuclear weapons and delivery means, the normal level of US political and organizational dominance over their allies was insufficient to keep them attentive to US requests. US intelligence had to discover and evaluate the allies’ progress. An extraordinary military and diplomatic effort of sticks and carrots was necessary: A mixture of co-option (UK) and threats combined with positive incentives and promises of unflinching commitment (Sweden, West Germany, Italy)

eventually brought most of them fully or partially back in line. Only in France's case, the efforts failed.<sup>117</sup> Today, NATO allies can pursue OCO capabilities independent of US scientific or material assistance and realistically with minimal insight from US intelligence in their progress. Hence, involuntary oversight through intelligence collection on allies' OCO capabilities will likely provide a lower level of insight than the US had over the allies' nuclear capabilities in 1958. Also, this means that if the US should wish to incentivize her NATO allies to develop (or refrain from developing) their OCO capabilities in particular ways, several sticks were available in 1958, e.g., withholding scientific support and means of delivery, are less efficient today. Positive and negative incentives for following agreements remain viable, but as mentioned, the verify-part of "trust but verify" on OCO will be difficult compared to nuclear weapons.

## CONCLUSION

### *NATO Allies' OCO Capabilities Constitute an Entrapment Risk to the US*

This article poses the question whether US allies' new OCO capabilities risks entrapping the US or are they more likely to merely constitute an entanglement nuisance—a question to which current literature provides little in the way of helpful answers.

The proposed argument was the following: If OCO brings into allies' reach means that can create an international crisis or seriously undermine US control of the management of a crisis, then allies OCO capabilities constitute an entrapment risk. If allies' OCO capabilities only have limited potential for military impact, they only justify minor concern and thus constitute a limited risk of nuisance due to unwanted entanglement.

The analysis explains how OCO's destruction potential of non-U.S. NATO allies falls far short of the threat of nuclear weapons. Yet this same analysis compellingly concludes that these OCO capabilities can deliver strategic effects, to include palpable escalation during an international crisis. They also are much easier to acquire and have an unlimited range, and do not require complex and costly delivery systems. Thus, in Snyder's terms, OCO convincingly provides allies with new means for "independent strategic initiatives."<sup>118</sup> Thus NATO and other US allies with technologically advanced economies may pose more than a minor risk of entanglement.

Recalling the caveat that NATO allies have grave incentives to adhere to US interests, the analysis finds that in extraordinary circumstances, allies' OCO constitutes an entrapment risk to the US, albeit less so than nuclear weapons. Historical evidence that OCO has been deployed by many states and on many occasions below the threshold of armed conflict suggests that states' threshold for using OCO is lower than for nuclear and even conventional means. Again, recalling the caveat, this still suggests a lower threshold for allies' independent initiatives involving OCO.

Furthermore, the acquisition of OCO can realistically be achieved clandestinely and without US scientific support or special raw materials, rendering proliferation harder to detect, and capabilities harder to assess, thus influencing allies' decisions on OCO development requires different efforts than nuclear proliferation. Positive incentives remain viable, as do negative ones if allies (with more difficulty compared to nuclear counter-proliferation) are caught violating agreements. However, the direct 1958-options of disincentives, e.g., withholding scientific support and/or access to delivery means seem less effective in the context of OCO.

The arguments above are not as such an argument for whether or not the US should discourage, condone or encourage allies to acquire OCO-capabilities. They are arguments for considering the potential influence of OCO, particularly OCO-CA, in alliances on the means' own terms as their tactical and technical properties demonstrably differ sufficiently from conventional means for it to be relevant to take these differences into account.

The findings lead to another observation: Whether or not counter-proliferation of NATO allies' OCO capabilities should be a US strategy, a clear statement from the US as to how allies can best develop OCO capabilities to support US policy objectives would provide illumination that is missing in the public discussion today. This is particularly important to allies for whom improving relations with the US is a (or even the) major factor when considering acquiring military capabilities, including for OCO. 🛡️

## NOTES

1. Glenn H. Snyder, "The Security Dilemma in Alliance Politics, *World Politics* 36, no. 4 (July 1984), 461–95, <https://doi.org/10.2307/2010183>.
2. Snyder, 484.
3. A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. DoD, "DOD Dictionary of Military and Associated Terms" (Department of Defense, 2020), 55.
4. Mikkel Storm Jensen, "Offensive Cyber Capabilities and Alliances: Questionable Assets for Prestige, New Risks of Entrapment" (Copenhagen, University of Southern Denmark, 2023), [https://portal.findresearcher.sdu.dk/files/228130107/Phd\\_thesis\\_Mikkel\\_Storm\\_Jensen\\_2023\\_e\\_publication.pdf](https://portal.findresearcher.sdu.dk/files/228130107/Phd_thesis_Mikkel_Storm_Jensen_2023_e_publication.pdf).
5. For a discussion of what constitutes the strategic environment, see B. J. Sokol, ed., *The Marine Corps War College Strategy Primer* (Quantico, VA: Marine Corps University Press, 2021), 13–23.
6. Max Smeets, "NATO Members' Organizational Path Towards Conducting Offensive Cyber Operations: A Framework for Analysis" International Conference on Cyber Conflict, CYCON 2019-May (2019): 7, <https://doi.org/10.23919/CYCON.2019.8756634>.
7. Donald Trump, "National Cyber Strategy of the United States of America" (The White House, September 2018), 2–3, <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>; ODNI, "ODNI Annual Threat Assessment" (Washington DC: Office of the Director of National Intelligence, 2021), <https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf>.
8. Joe Biden, "National Cybersecurity Strategy 2023" (The White House, 2023), <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>; Trump, "National Cyber Strategy of the United States of America."
9. Jensen, "Offensive Cyber Capabilities and Alliances," 115, 119.
10. Brandon Valeriano, Benjamin M. Jensen, and Bryan C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (New York: Oxford University Press, 2018); Martin C. Libicki, *Crisis and Escalation in Cyberspace*, RAND Corporation Monograph Series (Santa Monica, CA: Rand Project Air Force, 2012).
11. Jacquelyn Schneider, "The Capability/Vulnerability Paradox and Military Revolutions: Implications for Computing, Cyber, and the Onset of War," *Journal of Strategic Studies* 42, no. 6 (September 2019), 884–85, <https://doi.org/10.1080/01402390.2019.1627209>.
12. Richard J. Harknett and Max Smeets, "Cyber Campaigns and Strategic Outcomes," *Journal of Strategic Studies*, 2020, <https://doi.org/10.1080/01402390.2020.1732354>.
13. Stephen J. Cimbala, "Nuclear Crisis Management and Deterrence: America, Russia, and the Shadow of Cyber War," *The Journal of Slavic Military Studies* 30, no. 4 (October 2, 2017), 487–505, <https://doi.org/10.1080/13518046.2017.1377007>.
14. Stéphane Taillat, "Disrupt and Restraint: The Evolution of Cyber Conflict and the Implications for Collective Security," *Contemporary Security Policy* 40, no. 3 (July 3, 2019): 368–81, <https://doi.org/10.1080/13523260.2019.1581458>.
15. Max Smeets, "The Strategic Promise of Offensive Cyber Operations," *Strategic Studies Quarterly*, Fall (2018): 90–113; Kenton G Fasana, "Another Manifestation of Cyber Conflict: Attaining Military Objectives through Cyber Avenues of Approach," *Defence Studies* 18, no. 2 (2018), 167–87, <https://doi.org/10.1080/14702436.2018.1462661>; <https://doi.org/10.1080/14702436.2018.1462661>.
16. Benjamin Ang, "Small States Learn Different Survival Lessons," *The Cyber Defense Review*, no. Winter/22 (2021), 92–99.
17. Daniel Hughes and Andrew Colarik, "Small State Acquisition of Offensive Cyberwarfare Capabilities: Towards Building an Analytical Framework," *Intelligence and Security Informatics*, ed. Michael Chau, G. Alan Wang, and Hsinchun Chen (11th Pacific Asia Workshop on Intelligence and Security Informatics, Cham: Springer International Publishing, 2016), 174–75.
18. Mikkel Storm Jensen, "Five Good Reasons for NATO's Pragmatic Approach to Offensive Cyberspace Operations," *Defence Studies*, May 30, 2022, 1–25, <https://doi.org/10.1080/14702436.2022.2080661>.
19. White, "Ally or Die: The Unlearned Joint Organizing Lesson and Key to Survival."
20. Jeppe T. Jacobsen, "Europe Is Developing Offensive Cyber Capabilities. The United States Should Pay Attention." Council on Foreign Relations, 2017, <https://www.cfr.org/blog/europe-developing-offensive-cyber-capabilities-unit-ed-states-should-pay-attention>.
21. Max Smeets, "Intelligence and National Security US Cyber Strategy of Persistent Engagement & Defend Forward: Implications for the Alliance and Intelligence Collection," 2020, <https://doi.org/10.1080/02684527.2020.1729316>; Max Smeets, "NATO's Cyber Policy 2002–2019: A Very, Very Brief Overview." Cyber References Project (blog), 2020, <http://maxsmeets.com/2019/12/natos-cyber-policy-between-2002-2019-a-very-very-brief-overview/>.



## NOTES

22. Rosenberger, *Making Cyberspace Safe for Democracy*. Snyder, "The Security Dilemma in Alliance Politics;" Michael Beckley, "The Myth of Entangling Alliances: Reassessing the Security Risks of U.S. Defense Pacts." *International Security* 39, no. 4 (2015), 12.
23. Michael Mandelbaum, *The Nuclear Revolution: International Politics before and after Hiroshima* (New York: Cambridge University Press, 1981), chapter 6; Snyder, "The Security Dilemma in Alliance Politics," 466.
24. David A. Lake, *Entangling Relations* (Princeton, NJ: Princeton University Press, 1999).
25. Snyder, "The Security Dilemma in Alliance Politics," 467.
26. Mandelbaum, *The Nuclear Revolution*, 151.
27. Tongfi Kim, "Why Alliances Entangle But Seldom Entrap States," *Security Studies* 20, no. 3 (July 2011), 350-77, <https://doi.org/10.1080/09636412.2011.599201>.
28. Kim, 355.
29. R. E. Osgood, NATO, *The Entangling Alliance* (Chicago, 1962).
30. Snyder, "The Security Dilemma in Alliance Politics," 466.
31. Snyder, 473.
32. De Gaulle, "Foreign Relations of the United States, 1961-1963, Volume XIV, Berlin Crisis, 1961-1962 - Office of the Historian," May 31, 1961, <https://history.state.gov/historicaldocuments/frus1961-63v14/d30>.
33. Alexander Lanoszka, "Protection States Trust?: Major Power Patronage, Nuclear Behavior, and Alliance Dynamics" (2014), 185-88.
34. Smeets, "NATO Members' Organizational Path Towards Conducting Offensive Cyber Operations: A Framework for Analysis."
35. NATO, "AJP-3.20, Allied Joint Doctrine for Cyberspace Operations (Edition A)" (NATO Standardization Office, 2020), [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/899678/doc-trine\\_nato\\_cyberspace\\_operations\\_ajp\\_3\\_20\\_1\\_.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doc-trine_nato_cyberspace_operations_ajp_3_20_1_.pdf); L. Brent, "NATO's Role in Cyberspace," *NATO Review*, February 12, 2019, <https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html>.
36. Snyder, "The Security Dilemma in Alliance Politics," 484.
37. Smeets, "The Strategic Promise of Offensive Cyber Operations," 92.
38. Snyder, "The Security Dilemma in Alliance Politics," 484.
39. Lawrence A. Kaplan, "The United States and the Origins of NATO 1946-1949," *The Review of Politics* 31, no. 2 (1969): 218, 221.
40. Lake, *Entangling Relations*, 170.
41. Lake, 171.
42. C. Layne, "US Hegemony and the Perpetuation of NATO," *The Journal of Strategic Studies* 23, no. 3 (2000), 61.
43. Peter Viggo Jakobsen, "The Indispensable Enabler: NATO's Strategic Value in High-Intensity Operations Is Far Greater Than You Think," *Strategy in NATO: Preparing for an Imperfect World*, ed., L. Odgaard, 2014, 61.
44. Adrian Hyde-Price, "NATO and the European Security System - A Neo-Realist Analysis," *Theorising NATO - New Perspectives on the Atlantic Alliance* (London: Routledge, 2015), 48, 50, <https://doi.org/10.4324/9781315658001-3>.
45. Anthony H Cordesman, "NATO and the Ukraine: Reshaping NATO to Meet the Russian and Chinese Challenge" (Washington, DC: Center for Strategic and International Studies, 2022), 5-6, [https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220216\\_Cordesman\\_NATO\\_Ukraine.pdf?cS8vKRN0doYvg3t\\_y6QMZMSCpadAo90a](https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220216_Cordesman_NATO_Ukraine.pdf?cS8vKRN0doYvg3t_y6QMZMSCpadAo90a).
46. Jack Detsch Gramer Robbie, "Biden Administration Debates Legality of Arming Ukrainian Resistance," *Foreign Policy*, February 24, 2022, <https://foreignpolicy.com/2022/02/24/biden-legal-ukraine-russia-resistance/>.
47. Martti J Kari, "Russian Strategic Culture in Cyberspace Theory of Strategic Culture – a Tool to Explain Russia's Cyber Threat Perception and Response to Cyber Threat Russian Strategic Culture in Cyberspace Theory of Strategic Culture – a Tool to Explain" (Ph.D. Thesis, University of Jyväskylä, 2019).
48. Fiona Hill, "Russia's Assault on Ukraine and the International Order: Assessing and Bolstering the Western Response," Brookings (blog), February 2, 2022, <https://www.brookings.edu/testimonies/russias-assault-on-ukraine-and-the-international-order-assessing-and-bolstering-the-western-response/>; Michael Crowley and David E. Sanger, "U.S. and NATO Respond to Putin's Demands as Ukraine Tensions Mount," *The New York Times*, January 27, 2022, sec. U.S., <https://www.nytimes.com/2022/01/26/us/politics/russia-demands-us-ukraine.html>.



## NOTES

49. See e.g., C. Peoples, "Chapter 18: Strategic Studies and Its Critics," in *Strategy in the Contemporary World: An Introduction to Strategic Studies*, ed., John Baylis, James J. Wirtz, and Colin S. Gray, 5th edition (Oxford: Oxford University Press, 2016).
50. Robert J. Art and Robert Jervis, eds., *International Politics: Enduring Concepts and Contemporary Issues*, 12. ed (Boston: Pearson, 2015), 151-65.
51. NATO, "AJP-3.20, Allied Joint Doctrine for Cyberspace Operations (Edition A)," 16.
52. Joint Chiefs of Staff, "JP 3-12 Cyberspace Operations" (2018), U.S. Joint Chiefs of Staff, June 8, 2018), II-6, [https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3\\_12.pdf](https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf).
53. Department of the Army, Field Manual No. 3-13 Information Operations: Doctrine, Tactics, Techniques, and Procedures, 2003, 2-II, 2-9, <https://irp.fas.org/doddir/army/fm3-13-2003.pdf>.
54. U.S. Air Force, Air Force Doctrine Publication 3-12, Cyberspace Operations, U.S. Air Force, February 1, 2023, 7, [https://www.google.com/search?rlz=1C1GCEA\\_en&sxsrf=APwXEdlIDebLCjKu6M0E5rKYa0W-IB-WNA:1687337290580&q=jp+3-12+cyberspace+operations&sa=X&ved=2ahUKEwiTnMie\\_dP\\_AhXEYPEDHeFP-C8QQ1QJ6BAhHEAE](https://www.google.com/search?rlz=1C1GCEA_en&sxsrf=APwXEdlIDebLCjKu6M0E5rKYa0W-IB-WNA:1687337290580&q=jp+3-12+cyberspace+operations&sa=X&ved=2ahUKEwiTnMie_dP_AhXEYPEDHeFP-C8QQ1QJ6BAhHEAE).
55. Klaus Solberg Søylen, 'Economic and Industrial Espionage at the Start of the 21st Century – Status Quaestionis', *Journal of Intelligence Studies in Business* 6, no. 3, December 30, 2016, <https://doi.org/10.37380/jisib.v6i3.196>.
56. Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust and Fear between Nations* (New York: Oxford University Press, 2017), 76, <https://doi.org/10.1093/acprof:oso/9780190665012.001.0001>.
57. Micheal Handel, *Weak States in the International System*, 2nd ed. (Frank Cass & Co. Ltd., 1990), 83.
58. Adam P Liff, 'Cyberwar: A New "Absolute Weapon"? The Proliferation of Cyberwarfare Capabilities and Interstate War', *The Journal of Strategic Studies* 35, no. 3 (2012), 418, <https://doi.org/10.1080/01402390.2012.663252>; "An Interview with Paul M. Nakasone," *Joint Force Quarterly*, no. 92 (2019): 4-9.
59. James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival* 53, no. 1 (2011), 23-40, <https://doi.org/10.1080/00396338.2011.555586>.
60. Lake, *Entangling Relations*, 55.
61. Jensen, "Five Good Reasons for NATO's Pragmatic Approach to Offensive Cyberspace Operations."
62. Fred M. Kaplan, *Dark Territory: The Secret History of Cyber War* (New York: Simon & Schuster, 2016), chap. 8.
63. Pablo Breuer, Interview via Skype October 23, 2020 with Dr. Pablo Breuer, interview by Mikkel Storm Jensen; Gen. Michael V. Hayden, USAF, Ret, "The Future of Things 'Cyber,'" *Strategic Studies Quarterly* 5, no. 1, Spring 2011, 5.
64. Bernard E. Harcourt, *Exposed: Desire and Disobedience in the Digital Age* (Cambridge: Harvard University Press, 2015), 8-10. Wiesław Goździewicz, "Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA)," *Cyber Defense Magazine*, November 11, 2019, <https://www.cyberdefensemagazine.com/sovereign-cyber/>.
65. NATO, "AJP-3.20, Allied Joint Doctrine for Cyberspace Operations (Edition A)," II, 21.
66. NATO, 26.
67. J. Flemming, Director's Speech at Cyber UK 2018 - GCHQ.GOV.UK, GCHQ, April 12, 2018, <https://www.gchq.gov.uk/speech/director-cyber-uk-speech-2018>; Mike Burgess, Director-General ASD Speech to the Lowy Institute | ASD Australian Signals Directorate, Australian Signals Directorate, March 27, 2019, <https://www.asd.gov.au/publications/director-general-asd-speech-lowy-institute>; Sanger and Schmitt, "U.S. Cyberweapons, Used Against Iran and North Korea, Are a Disappointment Against ISIS," *The New York Times*, June 12, 2017, [https://www.nytimes.com/2017/06/12/world/middleeast/isis-cyber.html?rref=collection%2Fsectioncollection%2Ftechnology&action=click&contentCollection=technology&region=rank&module=package&version=highlights&contentPlacement=1&pgtype=sectionfront&\\_r=0](https://www.nytimes.com/2017/06/12/world/middleeast/isis-cyber.html?rref=collection%2Fsectioncollection%2Ftechnology&action=click&contentCollection=technology&region=rank&module=package&version=highlights&contentPlacement=1&pgtype=sectionfront&_r=0).
68. USCYBERCOM, "USCYBERCOM After Action Assessments of Operation GLOWING SYMPHONY" (National Security Archive, November 22, 2016), <https://nsarchive.gwu.edu/briefing-book/cyber-vault/2020-01-21/uscycybercom-after-action-assessments-operation-glowing-symphony>; Steven Loleski, "From Cold to Cyber Warriors: The Origins and Expansion of NSA's Tailored Access Operations (TAO) to Shadow Brokers," *Intelligence and National Security* 34, no. 1 (2019), 123, <https://doi.org/10.1080/02684527.2018.1532627>; Nakashima, "U.S. Military Cyber Operation to Attack ISIS Last Year Sparked Heated Debate over Alerting Allies," *The Washington Post*, May 9, 2017, [https://www.washingtonpost.com/world/national-security/us-military-cyber-operation-to-attack-isis-last-year-sparked-heated-debate-over-alerting-allies/2017/05/08/93a120a2-30d5-11e7-9dec-764dc781686f\\_story.html](https://www.washingtonpost.com/world/national-security/us-military-cyber-operation-to-attack-isis-last-year-sparked-heated-debate-over-alerting-allies/2017/05/08/93a120a2-30d5-11e7-9dec-764dc781686f_story.html).
69. Trump, "National Cyber Strategy of the United States of America;" Smeets, "Intelligence and National Security US Cyber Strategy of Persistent Engagement & Defend Forward: Implications for the Alliance and Intelligence Collection."

## NOTES

70. Sanger, "Trump Loosens Secretive Restraints on Ordering Cyberattacks," *The New York Times*, 2018, <https://www.nytimes.com/2018/09/20/us/politics/trump-cyberattacks-orders.html?action=click&module=RelatedCoverage&pgtype=Article&region=Footer>.
71. Nakasone, "A Cyber Force for Persistent Operations," *Joint Force Quarterly*, 2019, 10–14; Nakasone, Statement of General Paul M. Nakasone Commander USCYBERCOM before the Senate Committee on Armed Services (Senate Committee on Armed Services, February 14, 2019), [https://www.armed-services.senate.gov/imo/media/doc/Nakasone\\_02-14-19.pdf](https://www.armed-services.senate.gov/imo/media/doc/Nakasone_02-14-19.pdf); Nakasone and Michael Sulmeyer, "How to Compete in Cyberspace," *Foreign Affairs*, August 25, 2020, <https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity>; JFQ, "An Interview with Paul M. Nakasone;" Nakashima, "White House Authorizes 'Offensive Cyber Operations' to Deter Foreign Adversaries," *The Washington Post*, September 20, 2018, [https://www.washingtonpost.com/world/national-security/trump-authorizes-offensive-cyber-operations-to-deter-foreign-adversaries-bolton-says/2018/09/20/b5880578-bd0b-11e8-b7d2-0773aale33da\\_story.html](https://www.washingtonpost.com/world/national-security/trump-authorizes-offensive-cyber-operations-to-deter-foreign-adversaries-bolton-says/2018/09/20/b5880578-bd0b-11e8-b7d2-0773aale33da_story.html); Nakashima, "Trump Gives the Military More Latitude to Use Offensive Cyber Tools against Adversaries," *The Washington Post*, 2018, [https://www.washingtonpost.com/world/national-security/trump-gives-the-military-more-latitude-to-use-offensive-cyber-tools-against-adversaries/2018/08/16/75f7a100-a160-11e8-8e87-c869fe70a721\\_story.html?noredirect=on&utm\\_term=.89e4be3895b0](https://www.washingtonpost.com/world/national-security/trump-gives-the-military-more-latitude-to-use-offensive-cyber-tools-against-adversaries/2018/08/16/75f7a100-a160-11e8-8e87-c869fe70a721_story.html?noredirect=on&utm_term=.89e4be3895b0).
72. Biden, "National Cybersecurity Strategy 2023," 14.
73. Mikkel Storm Jensen, "Denmark's Offensive Cyber Capabilities: Questionable Assets for Prestige, New Risks of Entrapment," *Scandinavian Journal of Military Studies* 5, no. 1 (September 9, 2022), 111-128, <https://doi.org/10.31374/sjms.139>.
74. D. Rumsfeld, "National Military Strategy for Cyberspace Operations 2006: (Washington, DC: US DOD, 2006), 17; B. Obama, "Presidential Policy Directive/PPD-20," Presidential Policy Directive, 2012, <https://fas.org/irp/offdocs/ppd/ppd-20.pdf>.
75. NATO Cyber Defence Factsheet, NATO, 2021, [https://www.nato.int/nato\\_static\\_f12014/assets/pdf/2021/4/pd-f12014-factsheet-cyber-defence-en.pdf](https://www.nato.int/nato_static_f12014/assets/pdf/2021/4/pd-f12014-factsheet-cyber-defence-en.pdf).
76. Biden, "National Cybersecurity Strategy 2023," 31.
77. Rumsfeld, "National Military Strategy for Cyberspace Operations 2006," 17.
78. Trump, "National Security Strategy of the United States of America" (The White House, 2017), 20, <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>.
79. Trump, "National Cyber Strategy of the United States of America," 21.
80. DoD, "2018 DoD Cyber Strategy and Cyber Posture Review Sharpening Our Competitive Edge in Cyberspace" (U.S. Department of Defense, 2018), 5, [https://media.defense.gov/2018/Sep/18/2002041659/-1/-1/1/Factsheet\\_for\\_Strategy\\_and\\_CPR\\_FINAL.pdf](https://media.defense.gov/2018/Sep/18/2002041659/-1/-1/1/Factsheet_for_Strategy_and_CPR_FINAL.pdf).
81. Biden, "National Cybersecurity Strategy 2023," 32.
82. P. Cirenza, "The Flawed Analogy between Nuclear and Cyber Deterrence," *Bulletin of the Atomic Scientists* (blog), February 22, 2016, <https://thebulletin.org/2016/02/the-flawed-analogy-between-nuclear-and-cyber-deterrence/>.
83. Todd S. Sechser, Neil Narang, and Caitlin Talmadge, "Emerging Technologies and Strategic Stability in Peacetime, Crisis, and War," *Journal of Strategic Studies* 42, no. 6 (2019), 883, <https://doi.org/10.1080/01402390.2019.1626725>; Rebecca Slayton, "What Is the Cyber Offense-Defense Balance?: Conceptions, Causes, and Assessment," *International Security* 41 (2016), 72-109.
84. Joseph S Nye, "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly*, no. Winter 2011, 25.
85. See e.g., Jon Bateman, "Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications" (Washington, DC: Carnegie Endowment for International Peace, December 2022), [https://carnegieendowment.org/files/Bateman\\_Cyber-FINAL21.pdf](https://carnegieendowment.org/files/Bateman_Cyber-FINAL21.pdf); J. Reddick, "Finland, Now a NATO Member, Sees an Uptick in Cyberattacks," *The Record*, April 21, 2023, <https://therecord.media/finland-reports-uptick-in-cyberattacks-after-nato-membership>; "Ministries Hit by Cyber-Attacks," Pressemelding, Government.no (regjeringen.no, July 24, 2023), <https://www.regjeringen.no/en/aktuelt/ministries-hit-by-cyber-attacks/id2990098/>; FMI, "DDoS-angreb på offentlige hjemmesider under Forsvarsministeriet i december," Forsvarsministeriets Materiel- og Indkøbsstyrelse, January 4, 2023, <https://www.fmi.dk/da/nyheder/2023/pm-DDoS-angreb-paa-offentlige-hjemmesider-under-Forsvarsministeriet-i-december-2022/>.
86. Bateman, "Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications," 11.
87. Bateman, 33.
88. Liff, "Cyberwar: A New 'Absolute Weapon'?" The Proliferation of Cyberwarfare Capabilities and Interstate War," 416; Bryan R. Early and Victor Asal, "Nuclear Weapons and Existential Threats: Insights from a Comparative Analysis of Nuclear-Armed States," *Comparative Strategy* 33, no. 4 (August 8, 2014), 281, <https://doi.org/10.1080/01495933.2014.941720>; Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, 2018, <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>.

## NOTES

89. Schneider, 'The Capability/Vulnerability Paradox and Military Revolutions: Implications for Computing, Cyber, and the Onset of War', 856; Rumsfeld, 'National Military Strategy for Cyberspace Operations 2006', C-1; DOD, '2018 Nuclear Posture Review' (Department of Defense, 2018), 38, <https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF>.
90. Cimbala, 'Nuclear Crisis Management and Deterrence'.
91. Carl von Clausewitz, *On War*, Vol. 1., trans. J.J. Graham (Kegan Paul, Trench, Trubner & Co Ltd, 1918), 34, [https://oll-resources.s3.us-east-2.amazonaws.com/oll3/store/titles/2050/Clausewitz\\_1380-01\\_EBk\\_v6.0.pdf](https://oll-resources.s3.us-east-2.amazonaws.com/oll3/store/titles/2050/Clausewitz_1380-01_EBk_v6.0.pdf).
92. Jon R Lindsay, 'Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack,' *Journal of Cybersecurity* 1, no. 1 (2015), 56, <https://doi.org/10.1093/cybsec/tyv003>.
93. Libicki, *Crisis and Escalation in Cyberspace*, 93-97.
94. Libicki, 45-49.
95. Buchanan, *The Cybersecurity Dilemma*, chap. 4.
96. Slayton, "What Is the Cyber Offense-Defense Balance?: Conceptions, Causes, and Assessment."
97. Wan Wilfred, Kastelic Andraz, and Krabill Eleanor, "The Cyber-Nuclear Nexus: Interactions and Risks" (UNIDIR, November 2021), 19, <https://doi.org/10.37559/WMD/21/NRR/03>.
98. 2018 Nuclear Posture Review, viii, 57.
99. Nina Tannenwald, "How Strong Is the Nuclear Taboo Today?" *The Washington Quarterly* 41, no. 3 (July 3, 2018): 89-109, <https://doi.org/10.1080/0163660X.2018.1520553>.
100. Valeriano, Jensen, and Maness, *Cyber Strategy*.
101. For a conceptual discussion on how to assess states' "cyber power," see Jelle J. Van Haaster, "Assessing Cyber Power," 8th International Conference on Cyber Conflict, Tallinn, 2016).
102. Clausewitz, *On War*, Vol. 1., 42.
103. Lawrence J. Cavaola, David C. Gompert, and Martin Libicki, "Cyber House Rules: On War, Retaliation and Escalation," *Survival* 57, no. 1, January 2, 2015, 81-104, <https://doi.org/10.1080/00396338.2015.1008300>; David C. Gompert and Martin Libicki, "Waging Cyber War the American Way," *Survival* 57, no. 4, July 4, 2015, 10,12, <https://doi.org/10.1080/00396338.2015.1068551>; Joseph S. Nye Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (2016): 49.
104. CIA et al., "Development of Nuclear Capabilities by Fourth Countries: Likelihood and Consequences" (National Intelligence Estimate (NIE) No. 100-2-58 (Washington, DC: Director of Central Intelligence, 1958), [https://www.cia.gov/library/readingroom/docs/DOC\\_0001108555.pdf](https://www.cia.gov/library/readingroom/docs/DOC_0001108555.pdf).
105. CIA et al., 11.
106. Lanoszka, "Protection States Trust?: Major Power Patronage, Nuclear Behavior, and Alliance Dynamics." 176.
107. CIA et al., "Development of Nuclear Capabilities by Fourth Countries: Likelihood and Consequences" (NIE No. 100-2-58, 3, 14, 16, 18, 19.
108. CIA et al., 17; Lake, *Entangling Relations*, 55.
109. Lanoszka, "Protection States Trust?: Major Power Patronage, Nuclear Behavior, and Alliance Dynamics," 177-83, 187-89.
110. Lanoszka, 112-38.
111. L. Nuti, "Italy's Nuclear Choices," UNISCI Discussion Papers 25, no. January (2011), 171-73.
112. Wilhelm Agrell, *Svenska Forintelsesvapen* (Falun: Historiska Media, 2002), 298-348.
113. Thomas Jonter, *The Key to Nuclear Restraint* (London: Palgrave and Macmillan, 2016), 93-124, 255-69.
114. CIA et al., "Development of Nuclear Capabilities by Fourth Countries: Likelihood and Consequences" (NIE No. 100-2-58, 18).
115. CIA et al., 11.
116. Smeets, "NATO Members' Organizational Path Towards Conducting Offensive Cyber Operations: A Framework for Analysis," 7.
117. Lanoszka, "Protection States Trust?: Major Power Patronage, Nuclear Behavior, and Alliance Dynamics."
118. Snyder, "The Security Dilemma in Alliance Politics," 484.



# Risks to Zero Trust in a Federated Mission Partner Environment

---

Keith Strandell  
Dr. Sudip Mittal

## ABSTRACT

*Recent cybersecurity events have prompted the federal government to begin investigating strategies to transition to Zero Trust Architectures (ZTA) for federal information systems. Within federated mission networks, ZTA provides means to minimize the potential for unauthorized release and disclosure of information outside bilateral and multilateral agreements. But when federating with mission partners, there are potential risks that may undermine the benefits of Zero Trust. This article explores risks associated with integrating multiple identity models and proposes two potential avenues to investigate mitigation of these risks.*

## INTRODUCTION & BACKGROUND

Within days following the cyberattack on the Colonial Pipeline, U.S. President Joseph R. Biden Jr., signed into effect Executive Order 14028: Improving the Nation's Cybersecurity.<sup>1</sup> Prompted by recent "sophisticated and malicious" cyberattacks, the order acts as a catalyst for federal agencies to take necessary and immediate steps to coordinate with industry on improving information sharing, adopting best practices, and migrating federal information systems from perimeter-based security to a Zero Trust Architecture (ZTA). The foundational elements of Zero Trust are micro-segmentation and a well-informed trust algorithm. When effectively implemented with data tagging, Zero Trust provides a strong compartmentalization model that lends itself to federated mission partner environments. However, in an environment where mission partners are responsible for bringing to the table their own identity models, consideration must be given to risks associated with federating multiple mission partners.

© 2023 Keith Strandell, Dr. Sudip Mittal



**Keith Strandell** is the Materiel Leader for the Royal Saudi Air Force AWACS Modernization Program and previously served as the Materiel Leader for life cycle management of enterprise applications within the Enterprise Services portfolio for the United States Air Force's Enterprise Information Technology (EIT) construct, including capabilities such as the Air Force's Office 365 instance in the Impact Level 5 environment. Keith started his career as a Communication and Information Officer in the Air Force, leading the Network Security and Information Assurance offices at Travis Air Force Base. From there, he transitioned to a Technical Program Management role leading various hardware and software acquisition/development efforts related to battle control, intelligence, and Enterprise Information Technology systems. Included in this time frame were four years managing Foreign Military Sales cases across the Pacific, European, and Central Commands. Keith is currently pursuing a Ph.D. in Computer Science & Engineering at Mississippi State University.

In this article, we investigate the risks associated with a multi-partner environment built on ZTA that federates with each mission partner's identity model. For purposes of isolating the impact of federated identities, the operating assumption is that the environment has fully implemented micro-segmentation and data tagging such that the primary risks are associated with the integration of multiple identity models. In addition to assessing the risks, we recommend two potential areas of investigation that may alleviate some of the risks associated with this architecture.

## MISSION PARTNERS AND DATA PROTECTION

Combatant Commands (COCOMs) work with a variety of international mission partners, the most obvious being foreign militaries. However, there is a significant degree of cooperation that occurs with other agencies. In January 2010, U.S. Southern Command (USSOUTHCOM) responded to a request for earthquake relief support by Haiti. This Humanitarian Assistance and Disaster Response (HA/DR) operation required coordination with multiple international organizations, including foreign government agencies, nongovernment agencies, and foreign militaries. In order to share information effectively, data were kept unclassified to the maximum extent possible and public platforms were used for dissemination.<sup>2</sup> Another example of cooperation with international partners can be found in a recent partnering among U.S. Africa Command (USAFRICOM), the International Criminal Police Organization (INTERPOL), and local law enforcement from several West African nations. The operation targeted illegal fishing and "other maritime crimes" along the West African coast.<sup>3</sup> Not only do these mission sets require sharing of unclassified data, but they also demonstrate the potential for both persistent and transient user bases operating in the same environment.





**Sudip Mittal** is an Assistant Professor in the Department of Computer Science & Engineering at Mississippi State University. He graduated with a Ph.D. in Computer Science from the University of Maryland Baltimore County in 2019. His primary research interests are cybersecurity and artificial intelligence. Mittal's goal is to develop the next generation of cyber defense systems that help protect various organizations and people. At Mississippi State, he leads the Secure and Trustworthy Cyberspace (SECRETS) Lab and has published over 70 journal articles and conference papers in leading cybersecurity and AI venues. Mittal has received funding from the NSF, USAF, USACE, and other agencies within the U.S. Government. He also serves as a Program Committee member or Program Chair of leading AI and cybersecurity conferences and workshops. Mittal's work has been cited in the Los Angeles Times, Business Insider, WIRED, the Cyberwire, and other venues. He is a member of the ACM and IEEE.

Attempting to create a collaborative environment to facilitate data sharing that allows for multiple missions and user bases increases the need for effective controls to prevent the unauthorized release and disclosure of information such as Controlled Unclassified Information (CUI). For example, data controlled as Not Releasable to Foreign Nationals (NOFORN) are not releasable to foreign mission partners; however, these data may need to reside in this environment due to a need to release to non-foreign entities such as the Federal Emergency Management Agency. Similarly, data controlled as "CUI//REL TO USA, FVEY" are releasable to members of the Five Eyes alliance.<sup>4</sup> A comparable protection requirement exists for mission partner data. The Mission Partner Environment framework is designed to facilitate collaboration and sharing with "participants within a specific partnership or coalition."<sup>5</sup> The implication is a requirement to ensure data are shared only within designated groups. For example, assume there are existing agreements among the United States, country A, and country B, as depicted in Figure 1. In this image, the overlapping areas represent shared data based on these partnerships. Each country contributing data to the environment expects the information it uploads to the system to be protected accordingly. That is to say, data transferred to the United States as part of a bilateral agreement with country A must not be released to country B without the express consent of country A.

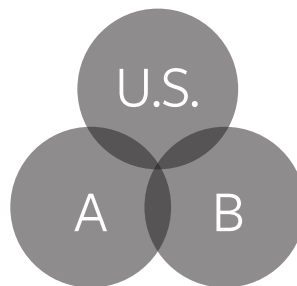


Figure 1: Multi-country data sharing partnerships.



## ZERO TRUST AND FEDERATION

The operating assumption in ZTA is that the network is compromised and therefore steps must be taken to minimize the potential impact of unauthorized access. Through micro-segmentation and data tagging, a ZTA can provide a framework in which compartmentalization is baked into the security model. The result is smaller trust zones, which reduce the potential for lateral movement of an adversary exploiting a vulnerability (see Figure 2). However, to realize the benefits fully, the ZTA must also implement a trust algorithm that takes in relevant data feeds to provide continuous authentication and authorization decisions on access requests. A robust trust algorithm will have access to contextual information on the requesting entity and device, the target resource, resource access policies, and threat intelligence.<sup>6</sup> Access to these information feeds provides a more complete view of the request and associated risks. For example, consider the ability to access data related to the requesting entity's device configuration to compare those data with data on known configurations and thus to predict the level of vulnerability associated with the device.<sup>7</sup> Such an assessment increases the insight into the risk of a given request.

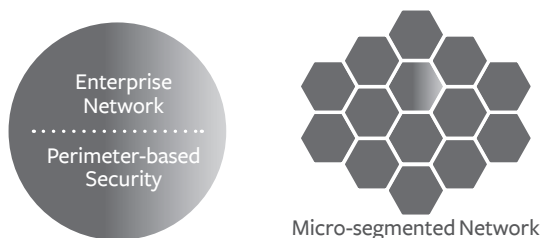


Figure 2: Lateral Movement in Perimeter Network vs. Zero Trust.

Federation in ZTA poses an interesting conundrum because, in an architecture that strives to remove trust, it introduces an inherent trust among the federated organizations. Here, the mission partners act as identity providers and are responsible for authenticating their users. Once authenticated, the identity is securely transferred to support the trust algorithm making the authorization decision. This model eliminates the need for the user to maintain security information related to a separate identity, which can reduce the risk of compromise associated with user behavior. However, it can undermine the rigor of the trust algorithm by preventing access to contextual information related to the requesting entity.

## RISKS FEDERATING WITH MISSION PARTNER IDENTITY SOLUTIONS

Zero Trust touts a robust trust algorithm rooted in the ability to verify a user's identity. However, in a federated model, the algorithm is only as strong as the weakest identity solution. Figure 3 depicts a simplified model of a federated ZTA environment. The network supports countries A, B, and C. The entities in each country (e.g., military, law enforcement) have their own distinct identity models that are federated with the system. The Registered

User List provides a means for restricting users, standardizing attributes, and providing redirects to the appropriate identity system for authentication.

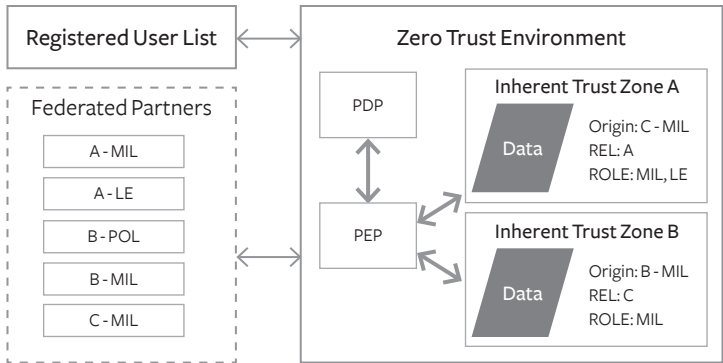


Figure 3: Notional Federated ZTA Environment

Ideally, each identity system would adhere to a minimum baseline that supports a context-rich authentication model. However, when balancing risk and mission requirements, mission may take priority and drive risky behavior or decisions. As such, there is the potential for integration with substandard models, which increases the risk of unauthorized access to the system. Assuming an ideal implementation of ZTA in the model above, access to a given Inherent Trust Zone will be restricted to an appropriate user base, and users granted access to a given zone cannot move laterally. Hence, a user who accesses Zone A above will not have access to Zone B without having gone through a separate access request. Therefore, in the model provided, the “C – MIL” identity system offers the widest potential reach for a threat, because it is the only one whose user base has authorized access to both Inherent Trust Zones.

Successful implementation of Zero Trust is predicated on a robust Trust Algorithm with access to contextual information around a given access request. For example, relevant information for an access request could include multiple authentication factors, device registration check, and device health status. The ability to access the contextual information around the requesting entity is a challenge in federated models.<sup>8</sup> This model assumes contextual checks occur within the authentication pipeline managed by the mission partner, and therefore the ZTA environment is effectively blind to the degree of rigor used to authenticate a user. If it is assumed the authentication model for the “C – MIL” identity system is strictly a username and password, it becomes a prime target for adversaries looking to access the system. Given the strength of ZTA in containerizing information, an adversary should only have access to those Inherent Trust Zones to which the compromised account has access. In this model, the obvious impact of a compromised “C – MIL” user account would be the unauthorized disclosure of data in Inherent Trust Zones B and A. However, there is also the potential to upload misinformation and malicious code that could compromise entities in countries A and B.

The effective establishment and enforcement of a common, robust authentication process increase the security of the system; however, they do not address vulnerabilities in the supply chain. On December 8, 2020, it was discovered that SolarWinds had been compromised. The hack, attributed to Russia, affected approximately 17,000 SolarWinds clients, including several federal agencies such as the Department of Homeland Security and the Department of Defense. The attackers targeted a third-party vendor, Orion, that had a long-standing relationship with SolarWinds. Because Orion had been infiltrated, when clients of SolarWinds updated their software they inadvertently loaded malware onto their devices and thus gave hackers access to their networks, which in many instances resulted in significant data breaches.<sup>9</sup> The attack is significant in that it focused on popular network infrastructure devices, which allowed for the vast attack surface. A comparable attack on the identity components used by “C – MIL” could provide an adversary with the ability to hijack existing credentials or bypass authentication processes. There also exists the potential for introducing fraudulent credentials, but, that can be mitigated with the effective implementation of a Registered User List.

This risk is amplified by strategic competitors’ ability to leverage the Diplomatic, Informational, Military, and Economic (DIME) framework to deliberately position state-sponsored technology that provides them covert access. Strategic competitors such as the People’s Republic of China (PRC) and Russia are actively exercising DIME strategies to advance their influence in regions around the world. General Stephen J. Townsend noted in his statement to the House Armed Services Committee that both countries have an “inside track” in central and southern Africa. He also stated that Russia is actively buying influence in the region and the PRC is investing billions in infrastructure and development in Africa.<sup>10</sup> Within USSOUTHCOM’s area of responsibility (AOR), the PRC holds \$165B in loans and is using COVID-19 as a pretext to indebt nations in the region further while enhancing its integration with their infrastructure and technology. For example, as part of their COVID-19 response, the PRC was offering to donate Huawei technology.<sup>11</sup> The significant investments these competitors are infusing into the region provide the pretext to gain access to senior government officials with the leverage to secure deals that further embed their technology or allow insight/access to processes like identity management. The infrastructure investments in these regions serve, at a minimum, as a method to increase reliance and influence. However, they also introduce the potential supply risk noted above. Specific to the PRC, there are concerns related to the Military-Civil Fusion Strategy and how involved vendors such as Huawei are with the People’s Liberation Army and the extent of their collaborations.<sup>12</sup>

This concern is furthered by incidents which suggest not only security issues but the intentional inclusion of surveillance capabilities that lend themselves to espionage.<sup>13</sup> While the Huawei push is focused on 5G, the concern extends to any presumably state-sponsored technology that may serve as critical infrastructure for mission partner networks. Coupled

with the potential for growing an insider threat, there is the potential to undermine the processes of the Registered User List and reintroduce the risk of fraudulent accounts.

## POTENTIAL ENHANCEMENTS

Reducing the risks associated with federating multiple identity providers in the model depicted requires introducing an additional layer into the authentication process that provides contextual data. Two promising designs for consideration are blockchain and Adaptive Neuro-Fuzzy Inference System (ANFIS). The former shows promise in reducing the likelihood of compromised credentials while the latter has the potential to identify and flag behaviors that deviate from the norm.

### *Blockchain*

Blockchain first gained popularity as the digital ledger supporting bitcoin transactions; more recent implementations have shown its promise as a mechanism for augmenting or replacing existing authentication systems. The strength of blockchain lies in its immutable, secure nature, which comes from the combination of Merkle Tree hashing, encryption, distributed architecture, and consensus protocol.<sup>14</sup> Smart contract implementations of blockchain can support authentication models through its abilities both to store data and to automate processes. It has been proposed, for example, as an authentication model for a cloud-centric database that requires access from both internal and external users.<sup>15</sup> Blockchain has been shown to be capable of storing digital identities and data necessary to support authentication. It has also been shown to be capable of authenticating devices in an Internet of Things (IoT),<sup>16</sup> which may be leveraged to support an agent-based model that allows a user to register a limited number of devices. Within a federated network, blockchain has the potential to introduce a layer of managed context that decreases the likelihood of an account being compromised.

### *Adaptive Neuro-Fuzzy Inference System*


Adaptive Neuro-Fuzzy Inference System is a machine learning framework that couples the learning capabilities of adaptive neural networks with the fuzzy inference system's ability to detect ambiguities in decision-making criteria. This combination makes it well-suited for applications such as nonlinear analysis, control systems, and expert systems. The ANFIS framework has been leveraged in areas such as an improving pattern password authentication performance for touchscreens,<sup>17</sup> anomaly classification to support intrusion detection in a vehicular ad hoc network,<sup>18</sup> and a continuous authentication system for mobile devices.<sup>19</sup> The latter utilizes ANFIS to learn passive and active patterns of use for a given mobile user in order to define a behavioral model. This allows the authentication system to monitor behaviors continuously and support implicit authentication while also flagging deviations.<sup>20</sup>

For the purposes of a federated ZTA environment, ANFIS has the potential to be leveraged in both a client-side and server-side model. A client-side model could potentially generate a confidence score specific to a user's behaviors that is passed as context for authentication. This could support identifying a compromised device. A server-side variant may support identification of anomalous behavior relative to an archetype based on attributes. For example, if a certain user base only logs in periodically to check email and a specific user's behavior is significantly more active, that anomalous behavior may represent an insider threat or compromised credentials.

## **CONCLUSION**

The transition from perimeter-based cybersecurity to ZTAs should result in significant improvements in the overall security posture of enterprise networks. Specifically, it shows promise in the realm of multinational operations in which cooperation can often be born out of necessity and built on a tentative trust among mission partners. The inherent compartmentalization of a robust ZTA lends itself well to an environment rooted in mission partners' trust that their data are protected from unauthorized release and disclosure. Unfortunately, the benefits of Zero Trust can be undermined by the federating of multiple identity models, a risk made worse by actions of strategic competitors to employ the DIME framework to enhance their regional footprints, advance their influence, and deploy state-sponsored technologies. These activities increase the opportunities for social engineering, political influence, and clandestine cyber operations. Some of the risks can be mitigated by limiting federation to mission partners with known, trusted architectures and limited ties to strategic competitors while offering to host all other partners. This model, however, has the potential to be compromised when mission requirements outweigh the cybersecurity risks. To secure the environment's security posture further, additional measures should be investigated.

Two promising options for enhancing the authentication model that could be investigated as augmenting technologies are blockchain and Adaptive Neuro-Fuzzy Inference Systems. Blockchain gained popularity as the digital ledger supporting bitcoin transactions. However, recent efforts go well beyond that, using blockchain for authentication as part of a self-sovereign identity model. In 2019, a group of credit unions piloted the use of blockchain and noted the improvement in the authentication model could reduce a credit union's annual fraud expenses by \$150K just by reducing the authentication risks tied to call centers.<sup>21</sup> ANFIS is a machine learning model that integrates adaptive neural networks with a fuzzy inference system. In a study on its potential use to support "continuous implicit authentication" on mobile devices, ANFIS was used to learn user behaviors for supporting implicit user authentication and identification of both informed and uninformed adversary attacks. While the model showed a 5% increase in user recognition, the improvement in informed adversary attacks was negligible and it underperformed on identifying uninformed adversary

attacks.<sup>22</sup> The ANFIS architecture does show promise for user authentication on mobile devices. However, if paired with an identity model, it may be used as part of an enterprise authentication solution that focuses on learning archetype behaviors to identify when a user's behavior deviates from the normal behaviors of users assigned to the same role, or from the user's own behavior pattern. 

## **DISCLAIMER**

The views expressed in this work are those of the authors and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, the Department of the Air Force, or the Department of Defense.

## NOTES

1. Joseph Biden, “Exec. Order No. 14028,” 3 C.F.R. 86 (May 2021).
2. Gary Cecchine et al., *The U.S. Response to the 2010 Haiti Earthquake* (RAND Corporation, 2013).
3. U.S. Africa Command Public Affairs, “AFRICOM and law enforcement cooperation enhances maritime security in West Africa,” April 2022.
4. *Controlled Unclassified Information Markings*, Office of the Under Secretary of Defense for Intelligence & Security and Director for Defense Intelligence (Counterintelligence, Law Enforcement & Security), September 2020.
5. J-6, Chairman of the Joint Chiefs of Staff, *Requirements Management Process for Mission Partner Environment*, Instruction CJCSI 6290.01 (September 2019).
6. Scott Rose et al., “NIST Special Publication 800-207,” August 2020.
7. Paulo Shakarian, Jana Shakarian, and Kazuaki Kashiara, Systems and methods for vulnerability-based cyber threat risk analysis and transfer (US Patent 2022/0078203 A1, filed March 2021).
8. Koudai Hatakeyama, Daisuke Kotani, and Yasuo Okabe, “Zero Trust Federation: Sharing Context under User Control towards Zero Trust in Identity Federation,” in *2021 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)* (2021), 514-519.
9. Rahaf Alkhadra et al., “Solar Winds Hack: In-Depth Analysis and Countermeasures,” in *12th International Conference on Computing Communication and Networking Technologies (ICCCNT)* (2021), 1-7.
10. Stephen Townsend, “Hearing to Receive Testimony on United States Central Command and United States Africa Command in Review of the Defense Reauthorization Request for Fiscal Year 2022 and the Future Years Defense Program,” April 2021, [www.alderreporting.com](http://www.alderreporting.com).
11. Craig Faller, “Statement of Admiral Craig S. Faller, Commander, United States Southern Command Before the 117th Congress Senate Armed Services Committee,” 2021,
12. Elsa Kania and Lorand Laskai, “Myths and Realities of China’s Military-Civil Fusion Strategy,” Center for a New American Security, January 2021.
13. Elsa Kania, *Securing our 5G future: The Competitive Challenge and Considerations for U.S. Policy* (Center for a New American Security, November 2019).
14. Harsh Sheth and Janvi Dattani, “Overview of blockchain technology,” *Asian Journal For Convergence In Technology* (AJCT), ISSN-2350-1146, 2019.
15. Gaurav Deep et al., “Authentication protocol for cloud databases using blockchain mechanism,” *Sensors* 19, no. 20 (2019): 4444.
16. Mohamed Tahar Hammi et al., “Bubbles of Trust: A decentralized blockchain-based authentication system for IoT,” *Computers & Security* 78 (2018): 126-142.
17. Orcan Alpar, “Intelligent biometric pattern password authentication systems for touchscreens,” *Expert Systems with Applications* 42, no. 17 (2015), 6286-6294, <https://www.sciencedirect.com/science/article/pii/S0957417415002948>.
18. B. Karthiga et al., “Intelligent Intrusion Detection System for VANET Using Machine Learning and Deep Learning Approaches,” *Wireless Communications and Mobile Computing* (2022).
19. Feng Yao et al., “Continuous implicit authentication for mobile devices based on adaptive neuro-fuzzy inference system,” in *2017 International Conference on Cyber Security And Protection Of Digital Services (Cyber Security)* (IEEE, 2017), 1-7.
20. Yao et al., 3-5.
21. Hyperledger Foundation, “Case Study: How CULedger protects credit unions against fraud with Hyperledger Indy,” September 2020.
22. Yao et al., 6.



# Coalition Strategic Cyber Campaigns: Functional Engagement as Cyber Doctrine for Middle Power Statecraft

---

Joseph Szeman  
Christian Leuprecht

## INTRODUCTION

**T**he volatile geopolitical environment, a resurgence of interstate conflict, erosion of multilateral institutions, and diplomatic, information, military, and economic competition put the rules-based international order at risk. The cyber domain is a microcosm of geopolitical rivalry among adversarial state actors, competing political systems and visions of the international political order. Both state and non-state actors have extended instability and competition into cyberspace by exploiting global dependence on information and communication technologies (ICT), consistently and at scale, to advance their national interests and degrade those of their rivals, short of the threshold of armed conflict.<sup>1</sup> Between 2005 and 2022, China, Iran, North Korea, and Russia sponsored nearly 77 percent of suspected operations.<sup>2</sup> The same malicious actors orchestrated over 80 percent of adversarial cyber campaigns recorded between 2000 and 2020.<sup>3</sup> As geopolitical rivalries escalate and societies become ever-more reliant on ICTs, the exploitation of cyberspace for strategic gain is sure to increase.

The expanding use of cyber operations amid broadening geopolitical instability has particular implications for traditional middle powers, notably Canada, Australia, Norway, and the Netherlands, among others. They occupy privileged positions at the core of the global political economy but have limited ability to shape the geopolitical environment and few resources to protect and project their national interests. Many of the world's most influential middle powers are also longstanding U.S. allies, have high levels of digital connectivity, strong knowledge-based economies, leading research institutions, and membership in coveted multilateral groupings and security alliances. Compounded by their hard-power resource constraints, for adversaries, middle powers represent low-risk, high-reward targets for exploitation in cyberspace. Middle powers thus have

© 2023 Joseph Szeman, Christian Leuprecht



**Joseph Szeman** is a political studies and history graduate of Queen's University at Kingston, where he has conducted research on strategic culture, deterrence, and coercion in cyberspace.

strong incentives but limited capacity to prevent the cyber-enabled degradation of their sovereignty, stability, and economic competitiveness.

How should middle powers respond to adverse changes in their environment resulting from a weakened rules-based international order and unrestricted cyber activity targeting its interests and instruments of national power? Albert Hirschman's classic book *Exit, Voice, and Loyalty* posits a framework for agency to act on consequential change: an actor can *exit*, use *voice*, or demonstrate *loyalty*.<sup>4</sup> By choosing to *exit*, an actor accepts the undesirable change in its environment and alters its behavior to adapt to the new situation.<sup>5</sup> For example, a middle power could respond to cyber activity that undermines its interests by abandoning its status and role as a middle power, which would downgrade its international standing and influence. Choosing *loyalty* means the actor accepts the undesirable change in their environment but does not alter their behavior.<sup>6</sup> In this case, a middle power accepts the changes to its environment and the resulting threats to its interests by not altering its response, instead choosing to maintain the status quo of its current efforts in cyberspace. This article contends that a *loyalty* response, which characterizes current multilateral efforts to develop explicitly accepted cyber norms, has not (and will not) provide middle powers with an effective solution to the increasing threats they face from malicious state-sponsored cyber activity. Lastly, Choosing *voice* means taking deliberate action to revert the environment to its original condition.<sup>7</sup> For example, a middle power could attempt to reverse changes to its environment, asserting itself in and through cyberspace by devising strategies to uphold the international order, advance its interests, and protect its sovereignty.

There are few lessons to be drawn from existing scholarship, which examines the cyberspace doctrine



**Christian Leuprecht** is Class of 1965 Distinguished Professor in Leadership, Department of Political Science and Economics, Royal Military College, Editor-in-Chief of the *Canadian Military Journal*, Director of the Institute of Intergovernmental Relations in the School of Policy Studies at Queen's University, senior fellow at the Macdonald Laurier Institute, and Adjunct Research Professor in the Australian Graduate School of Policing and Security, Charles Sturt University.

and operations of only a handful of great powers and authoritarian states. Comparatively, there is a dearth of research on the roles, incentives, activities, and ambitions of other states in cyberspace—particularly traditional middle powers, which differ from great powers in intent, capability, and opportunity. Moreover, existing approaches to leveraging operations in cyberspace as a tool of statecraft have not been developed with the characteristics, incentives, and resources of middle powers in mind, which makes them ill-suited to being readily adopted and operationalized by those countries.

Absent a cyber doctrine tailored to their unique geopolitical realities, middle powers are likely accumulating a strategic cyberspace-deficit relative to potential adversaries that have more readily grasped the opportunity space offered by the strategic use of cyber operations. This article aims to fill this gap: how should middle powers respond to deleterious changes in their geopolitical (and cyberspace) environments? By means of coalition cyber strategy campaigns: proactively shaping the boundaries of adversarial cyber activity as a *voice* strategy to participate more actively and effectively in efforts to develop cyber norms. This strategy, tentatively termed “functional engagement,” draws on and modifies research on cyber persistence theory and the cyberspace strategy of persistent engagement in response to the resource constraints and strategic interests of middle powers.

First, this article describes the broad constitutive characteristics of middle powers. The first section contextualizes the unique foreign policy interests of middle powers and identifies what types of middle powers would benefit most from a strategy of functional engagement. To illustrate the challenges facing middle powers that seek to pursue a loyalty-based approach, the second section broadly outlines the failures of multilateral efforts to establish explicitly accepted cyber norms. The third section describes the contours of

cyber persistence theory and argues that, as a complement to ongoing multilateral efforts, the boundaries of tacitly acceptable state behavior in cyberspace, and potentially even in the wider geopolitical environment, can be cumulatively shaped by employing cyber operations in response to unacceptable behavior (the voice approach). The fourth section illustrates the point: it draws on traditional middle powers that are vulnerable to exploitation in cyberspace yet have limited resources to respond in order to formulate the concept of functional engagement as an approach tailored to middle powers. This section posits functional engagement as an alternative strategy, using Canada as a critical case study, given its geopolitical identity as a middle power, the threats emanating from cyberspace, and the relatively limited resources at its disposal.

## **THE CHARACTERISTICS OF MIDDLE POWERS**

Analysts had initially bifurcated the international community into small and great state powers, but it soon became apparent that some small states were more powerful than others. Relative strength was to be recognized in the form of a “scheme of gradation,” which, in the 1930s, gave rise to the concept of “middle powers.”<sup>8</sup> The concept gained momentum thanks to the concerted diplomatic efforts of Canada and Australia to justify and solidify their international influence and core roles in the post-1945 global order.<sup>9</sup> In 1947, Canadian diplomat and historian George Glazebrook asserted that the formation of the United Nations would enable “middle powers” to be “capable of exerting a degree of strength and influence not found in the small powers.”<sup>10</sup> A growing number of states have since either self-identified or been described by others as middle powers, including: Argentina, Australia, Canada, Brazil, Denmark, Japan, Malaysia, the Netherlands, Norway, Nigeria, Spain, Sweden, South Korea, and Turkey.<sup>11</sup> Although the question of what constitutes the attributes of a middle power is controversial, international relations scholars generally identify at least three useful theoretical perspectives: hierarchical, functional, and behavioral.<sup>12</sup>

First, the hierarchical approach categorizes states by measuring objective capability, asserted position, and recognized status.<sup>13</sup> It typically ranks states according to economic, military, or social metrics.<sup>14</sup> Their capabilities, international standing, or status rank these states in the “middle” of the international system: greater than those of small states but lesser than great powers. To explain the unique foreign policy behavior of middle powers, functional and behavioral approaches take the middle power concept further, beyond the status of a mere tool for ranking real capability.

The functional perspective argues that middle powers may on occasion exert influence in international affairs in specific instances based on their relative capabilities, interests, and degree of involvement.<sup>15</sup> By contrast, great powers are always capable of exercising international influence, while lesser states (than middle powers) are unable to exert real influence.<sup>16</sup> At the core of the functional concept is the idea that a state with relatively limited military

and economic capacity may nonetheless be successful in accruing “degrees of influence and authority among great powers and its neighbors that even reach into global forums.”<sup>17</sup> This view holds that middle powers commit to maintaining the status quo, security, and order in the international system through leadership on specific global problems and foreign policy niches of their choosing.<sup>18</sup>

Lastly, the behavioral approach is the dominant contemporary paradigm for characterizing foreign policy behavior by middle powers. Sometimes also referred to as the middle power internationalist approach, the behavioral approach contends that a country is a middle power if it exhibits a certain type of foreign policy behavior—namely, advocating for compromise and seeking multilateral solutions to international problems.<sup>19</sup> Within this understanding, middle powers rely on international law to ensure predictability in global interactions, and on international organizations to provide forums through which they can establish and enforce acceptable conduct. To this end, middle powers focus their foreign policy efforts on global normative arrangements promoted through international organizations.<sup>20</sup> Accordingly, the behavioral approach reflects a “particular style of diplomacy, or a strategy backed by a commitment to liberal values and the absence of unilateralism which is a defining trait of a great power.”<sup>21</sup>

The behavioral approach parses into “traditional” and “emerging” middle powers.<sup>22</sup> Traditional middle powers are “wealthy, stable, egalitarian, social democratic and not regionally influential,” exhibit “a weak and ambivalent regional orientation,” and offer appeasing concessions to pressures for global reform”: Australia, Canada, Norway, and the Netherlands are examples of traditional middle powers.<sup>23</sup> In contrast, emerging middle powers are semi-peripheral to the core of the global political economy, “materially inegalitarian and recently democratised states that demonstrate much regional influence and self-association” and that seek to reform the global order. Examples of emerging middle powers include Argentina, South Africa, Malaysia, and Turkey.<sup>24</sup> Both traditional and emerging middle powers benefit from the status quo of the current liberal international order.<sup>25</sup> However, lacking in capacity to alter the global balance of power or affect deep change in the international system, both types of middle powers are vulnerable to global instability that threatens to upend the status quo. Traditional middle powers, therefore, seek to legitimize and stabilize the international order since they already occupy privileged positions at the core of the global political economy. In essence, their interests are best asserted by defending and upholding the status quo of this order. Whereas emerging middle powers may benefit from their regional economic dominance within the international order, they do not occupy privileged positions within the global political economy and thus have an incentive to transform the international order.

Although the constitutive features of middle powers are up for debate, common to all three approaches is an understanding that middle powers have limited economic or military capabilities and are capable of exerting only narrow influence in the international system

(the hierarchical perspective). To address these challenges and participate in foreign affairs, middle powers focus their resources on specific, relevant issues (the functional perspective), or towards enhancing their influence through explicit bargaining processes, conflict management, and multilateralism (the behavioral perspective). The distinction between traditional and emerging middle powers is a function of divergent interests and incentives. As legitimizers and stabilizers of their privileged role within the current global order, traditional middle powers in particular stand to face the most significant disruption from contemporary threats to the established rules-based international order—including from cyberspace. Owing to their roles within in the international system, they have a particular incentive to address cyber threats.

### **THE LOYALTY APPROACH AND THE ISSUE OF MULTILATERAL EFFORTS TO DEVELOP “CYBER NORMS”**

In principle, the deteriorating stability of cyberspace makes the diffusion of transnational norms to regulate the behavior of state actors in cyberspace appealing to great and middle powers alike. Over the years, these efforts have taken a multilateral shape, touching numerous organizations, including the United Nations, G7, G20, and the Council of Europe.<sup>26</sup> Within more exclusive multilateral security alliances, additional attempts have also sought to codify an understanding of norms in cyberspace and the applicability of international law to cyber operations through NATO’s “Tallinn Manual.”<sup>27</sup>

Multilateral efforts to establish cyber norms have been floundering for good reason. First, liberal and illiberal states differ fundamentally in their respective visions of the future of cyberspace and the rules-based international order.<sup>28</sup> Illiberal regimes are working to shape the digital ecosystem in line with authoritarian values, advancing the state-centric concept of “cyber sovereignty” to prioritize the role of regime security and preservation over individual liberty. Russia and China, backed by other member states of the Shanghai Cooperation Organisation, have championed the concept of “information security” instead of “cyber security.” Information security aims to control information flows that could jeopardize internal stability and seeks to prevent the dissemination of information that is incompatible with countries’ internal political, economic, and social stability, as well as their spiritual and cultural environment.<sup>29</sup> States that adhere to the concept of information security fundamentally perceive the content of information itself as a threat, from which follows deeper state surveillance and control over online content to preserve regime stability. The fundamental divide between, on the one hand, the United States and its Western allies and, on the other, Russia, China, and other illiberal states, indicates that great power competition and divergent conceptions of cyberspace, particularly regarding the free flow of information, the applicability of international humanitarian law, and the doctrine of state responsibility, permeate multilateral negotiations.<sup>30</sup> Consensus on a normative framework for state behavior in cyberspace is thus constrained by broader competitive interactions between great powers



and perceived threats that the liberal order and the interconnectedness of cyberspace pose to illiberal regimes.<sup>31</sup>

At the same time, multilateral efforts have grown increasingly divorced from the operational realities of conducting cyber operations.<sup>32</sup> Indian diplomat Arun Sukumar argues that multilateral efforts are doomed to fail since states are rapidly scaling up their offensive cyber capabilities and are “buying time” to test the possible effects of new offensive cyber capabilities.<sup>33</sup> Illiberal states are concerned that any further endorsement of international law will undermine asymmetric advantages they derive from operating in cyberspace.<sup>34</sup> Even during the most productive years of UN-led efforts to develop cyber norms, the pace, scale, sophistication, and severity of cyber operations of all types conducted by Russia and China have continued unabated. In 2015, as UN diplomats and scholars hailed their recent international consensus on the applicability of international law to cyberspace, Russian cyber actors disrupted parts of the Ukrainian power grid and sabotaged the computer networks of French TV channel TV5 Monde.<sup>35</sup> In 2017—the same year that the Group of Governmental Experts process collapsed over a lack of consensus on the applicability of international humanitarian law to cyberspace—the release and global proliferation of the NotPetya malware, which incurred estimated losses in the tens of billions, was attributed to Russian state actors.<sup>36</sup> Despite efforts to curb economic espionage and intellectual property theft, an extensive US investigation concluded in 2018 that China has buoyed its economic growth with persistent campaigns of widespread, cyber-enabled technology transfer and intellectual property theft causing estimated losses to the US economy ranging from US\$225 billion to US\$600 billion annually.<sup>37</sup> By July 2021, the US and an “unprecedented” number of allies and partners, including the Five Eyes, the European Union, NATO, and Japan jointly condemned widespread cyber espionage campaigns conducted on behalf of the Chinese government.<sup>38</sup> Yet, the boundaries, scope, and scale of malicious state cyber activity have been expanding apace.

After two decades, norms for state behavior in cyberspace remain “contested, voluntary, unenforceable, vague and weakly internalized.”<sup>39</sup> Some scholars are highly pessimistic, asserting that great power dynamics and fundamental disagreements between liberal and illiberal states over the preferred shape of the international order have so permeated multilateral processes that agreement among cyber powers is unlikely. Traditional middle powers lack the real capabilities necessary to deter or coerce malicious state actors effectively. Yet, they are especially vulnerable to weak normative frameworks for state behavior in cyberspace. Regardless, traditional middle powers have continued to approach the geopolitics of cyberspace through the attractive and familiar behavioralist tradition of middle power internationalism, in futile attempts to rally like-minded peers and illiberal states alike into agreeing to binding international frameworks. We characterize this approach as the loyalty response, since middle powers are maintaining their reliance on multilateral institutions and great powers to address issues of geopolitical rivalry, competition, and instability in cyberspace. This approach has proven ineffective, and multilateral efforts alone have proven



insufficient to meet the urgent challenge of setting clear, reasonable, and enforceable international rules for cyberspace. As the development of an explicit normative framework drags on, the empirical record of the past two decades shows that states are increasingly using cyber capabilities as tools of statecraft to achieve strategic advantage in the international environment. Curiously, these activities have largely remained below the threshold of armed conflict, which may indicate that cyberspace norms are actually being shaped tacitly through operations, rather than in the boardrooms of multilateral organizations.<sup>40</sup>

### **A VOICE APPROACH: CYBER PERSISTENCE AND SHAPING CYBER NORMS THROUGH TACIT BARGAINING**

The extensive record of cyberspace competition occurring without escalation to armed conflict signals the emergence of a “new competitive space” wherein explicit agreement over the substantive character of acceptable behavior remains immature.<sup>41</sup> In essence, state actors appear to acknowledge tacitly that most competitive interactions in cyberspace are “bounded by a strategic objective to advance national interests while avoiding war,” and thus are most easily and effectively employed as tools to achieve strategic advantage below the threshold of armed conflict and just short of war.<sup>42</sup> The empirical record of the last decade and scholarship on cyber escalation appear to confirm this assertion.<sup>43</sup>

To characterize the nature of strategic competition between states in cyberspace, scholars have, in recent years, coined the term “cyber persistence,” which aims to capture how states employ cyber operations as tools of statecraft to change the relative balance of power and achieve strategic advantage in the international environment.<sup>44</sup> The dynamics of cyber persistence are derived from a fundamental feature of networked computing: interconnectedness, which produces a “structural imperative” for constant contact among all adversaries in the global system.<sup>45</sup> Interconnectedness increases the scale at which a state’s “core economic, political, social, and military capability and capacity could be undermined” by cyber actors without regard for the constraints of geography and without the degree of control over the global commons on which the projection of conventional force is premised.<sup>46</sup> Cyberspace is both initiative-persistent or offense-dominant insofar as it favors the attacker over the defender at “very low entry costs for core access,” as it offers asymmetric opportunities for attackers to generate cyber operations at scale against larger rivals that are orders of magnitude greater than would otherwise be possible outside of cyberspace.<sup>47</sup> Together, interconnectedness, initiative persistence, and asymmetry facilitate constant contact among all states, thereby producing a strategic environment that is structurally characterized by persistent (as opposed to episodic) competitive interactions below the threshold of armed conflict.<sup>48</sup> The scale of these activities in conjunction with the technical complexity of cyber operations has exceeded the ability of states to understand, manage, and reach consensus on cyber norms to regulate acceptable state behavior in cyberspace.

Proponents of cyber persistence contend that the consistent employment of cyber operations below the threshold of armed conflict by both liberal and illiberal states demonstrates a process of normalization or agreed competition, whereby tacitly accepted cyber norms have gradually evolved through competitive interaction between states in cyberspace.<sup>49</sup> Through this process (which cyber persistence scholars call a “tacit bargaining” approach), cumulative and robust operational engagement with adversarial actors has the effect of developing mutual understanding of the boundaries of acceptable/unacceptable state behavior in cyberspace. Ergo, to shape behavior proactively, states must seize the initiative by actively operating and engaging with adversaries in cyberspace in order to tacitly reach informal understandings about the boundaries of accepted behavior.<sup>50</sup> As part of the tacit bargaining process, cyber persistence scholar Michael Fischerkeller suggests that states should coalesce around “focal points,” which he defines as “mutual understandings of acceptable/unacceptable behavior in agreed competition.”<sup>51</sup> These focal points, if well-established and continually reinforced, may provide some needed stability in cyberspace by enabling states to use them to predict how other states may interpret or respond to a cyber operation.<sup>52</sup> For traditional middle powers, these focal points might include malicious, state-sponsored cyber activities that undermine the rules-based international order or that seek to degrade public confidence in democratic institutions, subvert or sabotage critical infrastructure systems, or reduce the effectiveness of international and multilateral organizations.

Nevertheless, is the substantive nature of the “agreed competition” between states in cyberspace beneficial to the interests of traditional middle powers? The “maturity” of these cyber norms remains nascent and “differing perspectives, ambiguity or uncertainty” over the character of acceptable cyber operations short of armed conflict is likely to continue to cause uncertainty and present a risk for inadvertent escalation.<sup>53</sup> Essentially this means that the absence of explicitly accepted cyber norms and the current immaturity of tacitly accepted norms leaves room for malicious state actors to legitimize the use of significantly disruptive cyber operations short of armed conflict.<sup>54</sup>

In fact, tacit bargaining processes in cyberspace that are antithetical to liberal interest and values may already be occurring. For much of the previous decade, the United States’ restraint in responding to the continuous aggression in cyberspace from illiberal state actors such as Russia, China, and Iran has had a destabilizing effect by failing to disincentivize aggressors from operating with impunity. The result has been the gradual shaping and tacit acceptance of norms toward illiberal conceptualizations of cyberspace and the international order.<sup>55</sup> By failing to shape the development of cyber norms in their operational infancy, liberal states risk losing the initiative necessary to manage the emergence of norms that facilitate “massive theft of intellectual property, expanding control of internet content, attacks on data confidentiality and availability, violations of privacy, and interference in democratic debates and processes.”<sup>56</sup>

## SHAPING THE CYBERSPACE ENVIRONMENT THROUGH PERSISTENT ENGAGEMENT

In 2018 the U.S. Cyber Command (USCYBERCOM) reportedly undertook a series of cyber operations to respond to Russian disinformation efforts targeting US elections and institutions by publicly exposing individuals involved in disinformation efforts and disrupting the functions of the Internet Research Agency—the troll farm at the heart of Russian disinformation operations.<sup>57</sup> These activities formed part of the opening salvo of USCYBERCOM’s novel cyberspace strategic doctrine of “persistent engagement”—the most important development in US cyber doctrine in the 21st century. These persistent engagement attempts sought to address a perceived strategic deficit in cyberspace on the part of the United States relative to its adversaries by operating as close as possible to the origin of adversarial cyber activity, and persistently contesting adversarial actors to generate continuous tactical, operational, and strategic advantage.<sup>58</sup> To do so, USCYBERCOM expects to operate “seamlessly, globally and continuously” in cyberspace, using continuous engagement with adversaries to seize and maintain strategic and tactical initiative.<sup>59</sup> Since 2018, under the banner of persistent engagement and to challenge adversarial activities wherever they operate, USCYBERCOM has deployed at least 27 Cyber National Mission Force teams (called “hunt forward” operations by USCYBERCOM) to 15 separate countries as part of its efforts to track and disrupt specific nation-state actors in foreign cyberspace.<sup>60</sup> Reportedly, USCYBERCOM efforts to defend the 2020 US elections may have involved eleven hunt forward operations across nine different countries.<sup>61</sup> More recently, in February 2022, prior to the Russian invasion of Ukraine, hunt forward operations that partnered with Ukrainian network operators were credited with mitigating malware capable of disrupting Ukrainian railway networks, enabling millions of Ukrainians to escape to safety and ensuring the flow of Western assistance remained undisturbed.<sup>62</sup>

Persistent engagement aims to generate “continuous tactical, operational, and strategic advantage in cyberspace,” with the ultimate objective of cumulatively shaping the boundaries of acceptable adversarial behavior in cyberspace, through the aforementioned approach of tacit bargaining.<sup>63</sup> Therefore, cyber activities driven by persistent engagement are meant to function as a never-ending series of signals that will push adversaries toward a preferred set of cyberspace norms by continuously undermining their ability to succeed.<sup>64</sup> In 2018, USCYBERCOM operationalized a strategy of persistent engagement in its *Command Vision for U.S. Cyber Command: Achieve and Maintain Cyberspace Superiority*.<sup>65</sup> Through this strategy, USCYBERCOM aims to “secure US national interests in cyberspace and disrupt the cyber campaigns of US adversaries” by “defend[ing] forward as close as possible to the origin of adversary activity, and persistently contest[ing] malicious cyberspace actors to generate continuous tactical, operational, and strategic advantage.”<sup>66</sup> The ultimate objective of the strategy is to “influence the calculations of [US] adversaries, deter aggression, and clarify the

distinction between acceptable and unacceptable behavior in cyberspace.”<sup>67</sup> In essence, the strategic doctrine of persistent engagement necessitates a more active US posture in cyberspace, with the overall strategic objective of inhibiting an adversary’s attempts to intensify cyber operations against the US and its allies.

Proponents of persistent engagement contend that previous US approaches to cyberspace were overly reliant on multilateral initiatives to establish cyber norms explicitly, which in turn resulted in a restrained and reactive operational strategy in cyberspace.<sup>68</sup> By contrast, the very *raison d’être* of the persistent engagement strategy is as an operational complement to sole reliance on multilateral efforts to develop cyber norms, which is believed to have ceded the advantage in cyberspace to adversaries with an incentive to be more aggressive in their use of cyber operations.

Through persistent engagement, the US aims to “gain strategic advantage” in cyberspace by preserving a favorable distribution of power. This objective is ambitious, and global in scope, with an end state the US defines as acceptable or unacceptable behavior in cyberspace, but it is also somewhat ambiguous.<sup>69</sup> Critics of persistent engagement are also concerned about the lack of defined objectives and clarity regarding the strategy’s actual implementation, proposing that in its current form, persistent engagement appears to prescribe an endless deployment of cyber resources in pursuit of vague strategic objectives.<sup>70</sup> Other critics argue that the persistent deployment of US cyber capabilities against rivals is destabilizing and risks unintended consequences through inadvertent escalation, thereby exacerbating instability in cyberspace and accelerating an already hyper-competitive and unstable environment.<sup>71</sup> However, concerns about escalation in and through cyberspace have generally been overstated. Recent research suggests that cyber operations are only narrowly escalatory, and only within the context of broader geopolitical crises.<sup>72</sup>

## **FUNCTIONAL ENGAGEMENT FOR TRADITIONAL MIDDLE POWERS**

Traditional middle powers face significant threats in cyberspace and are vulnerable to adversarial cyber operations that undermine their national and global interests. Middle powers have largely responded to this growing threat by taking a passive approach: hardening their cyber defense capabilities and participating in multilateral initiatives to develop and diffuse transnational cyber norms. Middle powers may expect that the combination of these efforts will reduce the threats they face from malicious state actors in cyberspace. Since multilateral cyber diplomacy efforts have largely stalled, and given that the threats middle powers face in cyberspace are increasing exponentially, an alternative (or complementary) approach is necessary.

Cyber persistence theory and the concepts of tacit bargaining and normative shaping in cyberspace hold significant strategic utility for middle powers. The problem: cyber persistence theory has been formulated to guide the US approach to countering adversarial behavior in

cyberspace. The only known operationalization of cyber persistence theory—persistent engagement—specifically aims to alter the global balance of cyber power in the United States’ favor by continually contesting its adversaries around the clock.<sup>73</sup> These objectives are unattainable for middle powers, not only due to inadequate resources, but also because they are misaligned with the foreign policy ambitions and characteristics of middle powers. In contrast, foreign policy interests more characteristic of middle powers might include maintaining the status quo, ensuring security and order in the international system, upholding the integrity of international organizations and democratic institutions, and protecting economic security and prosperity.

This article posits the cyber-strategic concept of functional engagement as a variation on persistent engagement uniquely tailored for operationalization by traditional middle powers. Functional engagement seeks to harness the strategic utility of cyber persistence theory and persistent engagement by adapting it to align more closely with traditional middle powers that strive to influence international affairs selectively as a function of their relative capabilities, interests, and degree of involvement.<sup>74</sup> The key difference between functional engagement and persistent engagement is the scope and scale of their respective objectives. Functional engagement proscribes a narrower application of tacit bargaining and normative shaping in cyberspace that reflects the limited cyber capabilities and foreign policy ambitions of traditional middle powers. To this end, functional engagement is premised on establishing and reinforcing a limited set of focal points that are communicated unambiguously to set boundaries for acceptable and unacceptable behavior in cyberspace. Middle powers can then harness their limited cyber capabilities more effectively against adversarial cyber actors that transgress these specific focal points.

An initial set of focal points for unacceptable behavior could include malicious activities that subvert or degrade the integrity of electoral processes or critical infrastructure systems, actions that undermine economic security or competitiveness, and behavior that undermines the effective functioning of international institutions. Instead of continuously and globally employing cyber capabilities to change the overall balance of power in the international system, functional engagement calls for middle powers to deploy targeted cyber operations, specifically in instances when a malicious actor conducts cyber activity that is antithetical to tacitly accepted focal points. In turn, this strategy enables traditional middle powers to bolster focal points for cyber norms while upholding the rules-based international order.

## **CANADA: A CASE STUDY FOR EMPLOYING FUNCTIONAL ENGAGEMENT**

As a variant of the United States’ persistent engagement approach, we contend that functional engagement is better suited to states with limited resources but whose geopolitical ambitions render them targets of, and vulnerable to, adversarial state-sponsored cyber activity.

### *The Functional Principle and Its Application to Canada's Cyberspace Doctrine*

In the post-Second World War period and throughout the Cold War, Canada leveraged the “functional principle” (from which functional perspective of middle power identity and the proposed functional engagement doctrine derive their names) to pursue its interests, justify a disproportionate influence in the international system, and cement its post-1945 status as a leading “non-great power.”<sup>75</sup> First articulated by Canadian diplomat Hume Wrong, the functional principle stipulated that an individual small state’s involvement in international affairs should be based on (1) the relevance of the state’s interests, (2) the direct contribution of the state to the situation in question, and (3) the capacity of the state to participate.<sup>76</sup> Practically, the functional perspective holds that middle powers commit to maintaining the status quo, security, and order in the international system through leadership on specific global problems and foreign policy niches of their choosing.<sup>77</sup>

Indeed, growing instability and increasing strategic competition between states in cyberspace are both global problems and a foreign policy niche highly relevant to Canada’s national security and foreign policy interests. Owing to the resource constraints that characterize middle powers, for the past two decades Canada has been struggling to demonstrate effective international leadership and respond to a highly competitive cyberspace environment. At least three factors continue to coalesce to make Canada a low-risk, high-payoff target for malicious cyber activity. First, Canada has limited soft and hard power resources, which constrains its ability to combine instruments of power or retaliate unilaterally. Second, Canada’s economy is highly advanced, with a strong technology sector, high levels of digital connectivity, vast natural resource wealth, and cutting-edge research and development activities.<sup>78</sup> Third, Canada’s special relationship with the US and its membership in an array of coveted security alliances and multilateral institutions provide potential adversaries with an efficient means of targeting both Canada and its great power allies.<sup>79</sup>

Threats to Canada in cyberspace are escalating in sophistication, quantity, and complexity, and the country’s core national interests continue to be undermined by malicious, state-sponsored cyber actors. Canada’s national security and its international interests have long been assured by its geographic location, the security assurances of multilateral institutions, and the legal and normative frameworks of the rules-based international order.<sup>80</sup> Cyberspace represents a unique departure from these assurances: it allows Canada’s adversaries to bypass its geographic advantage entirely, while multilateral approaches to managing state behavior in cyberspace lack a foundation of stable laws, norms, and incentives to encourage malicious state actors to discipline their activities.

### *Threats to Canada in Cyberspace and Its Evolving Cyber Strength*

Canada’s tradition of liberal internationalism has reflexively inclined it toward supporting multilateral processes that attempt to establish explicitly (as opposed to tacitly) accepted



boundaries for state behavior in cyberspace. Since 2010, Canada has participated in at least forty-five multilateral statements, communiqués, and initiatives on cyber norms in the G7, G20, NATO, ASEAN, OAS, OSCE, the Commonwealth, and the UN.<sup>81</sup> Concerted cyber diplomacy efforts notwithstanding, the Canadian military unambiguously asserts that state actors are increasingly pursuing their agendas using hybrid methods below the threshold of armed conflict (including in cyberspace) to threaten Canada’s defense, security, and economic interests.<sup>82</sup> Moreover, the director of Canada’s domestic security service, the Canadian Security and Intelligence Service, has warned that Russian and Chinese state-sponsored commercial espionage remains the most significant threat to the Canadian economy and future economic growth.<sup>83</sup> According to Canada’s 2020 and 2022 National Cyber Threat Assessments, cyber operations by China, Russia, Iran, and North Korea posed the greatest threat to Canada’s national security and its strategic interests.<sup>84</sup> The assessments, which are the landmark documents by which the Government of Canada communicates updates about strategic cyber threats to the Canadian public, assert that state-sponsored cyber actors have carried out “large-scale, worldwide cyber campaigns” to influence the Canadian public and conduct espionage against Canadian industry, government, and academia, with intent to “advance foreign economic and national security interests while undermining the same within Canada.”<sup>85</sup>

Although inevitably limited by challenges in collecting measures of national cyber capabilities, the Harvard Belfer Center Cyber Power Index (CPI) is a comprehensive effort to evaluate and compare the objectives and capabilities of states in cyberspace. That makes it a useful tool to examine the status and evolution of Canada’s cyber capabilities. In the 2020 CPI ranking for overall comprehensive global cyber power, Canada ranked eighth (behind the United States, China, the United Kingdom, Russia, the Netherlands, France, and Germany, but ahead of Japan and Australia).<sup>86</sup> In the updated 2022 CPI, Canada dropped out of the top ten.<sup>87</sup> Ranked thirteenth, Canada not only ranked lower than all of its major adversaries (Russia, China and Iran), but also three of its Five Eyes partners (the US, UK, and Australia) and a handful of its other like-minded partners (the Netherlands, South Korea, France, Germany, and Ukraine).<sup>88</sup> Moreover, the 2022 CPI shows that, since 2020, Canada’s measures have declined across all of the cyber power objectives.<sup>89</sup> Canada now lags its major adversaries, middle power peers, and Five Eyes partners in key objectives including the intent and capability to: conduct cyber-enabled foreign intelligence, control and manipulate the information environment, and destroy or disable an adversary’s infrastructure and capabilities.<sup>90</sup> Since 2020, though, Canada moved also from a “high-intent, low-capability” cyber power, to a “high-intent, high-capability” cyber power, retaining notable strengths in cyber surveillance, cyber defense and cyber norms development initiatives.<sup>91</sup>

On the one hand, the CPI’s assessment of Canada reflects two decades of careful focus on implementing and communicating cyber defense and cyber security initiatives. On the other hand, the rankings may indicate a strategic deficit and thus the need for a cyberspace



doctrine to harness a range of more assertive cyber espionage, subversion, and sabotage capabilities in pursuit of national strategic objectives.

In recent years, Canadian policymakers have made deliberate efforts to develop institutional and legislative mechanisms to support a more assertive cyberspace posture. Canada's 2017 defense policy, *Strong, Secure, Engaged*, recognized that cyberspace is essential for the conduct of modern military operations and complemented a strong defensive cyber posture with more assertive cyber operations.<sup>92</sup> In 2019, passage of Bill C-59, *An Act Respecting National Security Matters*, bolstered the prospect for Canadian cyber operations. Bill C-59 expanded the role and impact Canada could have in cyberspace by authorizing the Communications Security Establishment (CSE) to conduct offensive cyber operations, which the legislation parses into "active cyber operations" and "defensive cyber operations"—to supplement CSE's traditional role of ensuring cryptographic security and collecting foreign signals intelligence.<sup>93</sup> The addition of these capabilities to CSE's mandate was hailed as a major step in aligning Canada's cyber operations authorities with its Five Eyes allies.<sup>94</sup> For the first time in its history, the combination of foreign intelligence, active cyber operations, and defensive cyber operations mandates may enable it to conduct the full spectrum of cyber espionage, sabotage, and subversion operations.

In summary, Canada may be an ideal candidate for functional engagement since it (1) has a legacy of restraining its influence on geopolitics to foreign policy niches of particular relevance (the functional principle); (2) faces significant threats to its national and international interests as a result of malicious state-sponsored cyber activities and lacks a cyber strategic doctrine to organize its response; and (3) may already have, or is otherwise well on the path toward developing, the requisite cyber capabilities and authorities to begin upholding its interests in the cyberspace environment.

### ***Functional Engagement in the Canadian Context***

Canada may have an opportunity to demonstrate independent international leadership to reduce instability and uncertainty in cyberspace. In doing so, it can uphold and extend its strategic interests. According to cyber persistence theory, helping to establish and strengthen tacitly accepted cyber norms by regularly employing cyber capabilities may be an effective way for Canada to reduce uncertainty in cyberspace and limit threats to its national interests. Due to Canada's resource constraints and limited foreign policy ambitions (in comparison to the US and other great powers), functional engagement prescribes that Canada employ the full range of its nascent cyber capabilities to establish and reinforce a focused set of clearly defined and communicated focal points that define what it deems acceptable and unacceptable behavior in cyberspace. Instead of continuously and globally employing cyber capabilities to change the overall balance of power in the international system, functional engagement calls for Canada to employ its cyber capabilities more narrowly, in specific instances when a malicious cyber actor conducts activity that is antithetical to those focal points.

An initial set of focal points for unacceptable state-sponsored behavior in cyberspace could include malicious activities that (1) directly degrade Canada's sovereignty and the security of its people (e.g., cyber operations that target civilian critical infrastructure and ICS/SCADA systems); (2) degrade or subvert international law and the integrity of international, electoral, or democratic institutions (e.g., cyber operations that target electronic voting systems or the functioning of international institutions); and (3) directly undermine Canada's economic security, competitiveness, and prosperity (e.g., cyber operations that target intellectual property). In turn, this approach remains true to the fundamentals of cyber persistence but is more aligned within the limited resources and unique character of Canada's geopolitical identity as a middle power.

## CONCLUSION

The volume and sophistication of state-sponsored activities in cyberspace has increased apace with deepening global dependence on the Internet and digital technologies. Twenty years of international interactions in cyberspace reinforce that cyber war is rare and that states prefer to employ cyber operations as tools of statecraft well below the threshold of armed conflict. While the immediate risk of cyber escalation appears to be low, campaigns of cumulative cyber operations aim to generate strategic effects over time, by degrading the integrity of international, democratic, and electoral institutions, undermining economic competitiveness, and/or generating strategic information advantage over an adversary. Meanwhile, multilateral initiatives to reduce instability in cyberspace and develop explicitly accepted cyber norms have failed to deliver significant advances in regulating the boundaries of state behavior in cyberspace.

Traditional middle powers, especially those with highly interconnected societies, advanced economies, world-renowned research institutions, and memberships in an array of multilateral and security institutions, face threats in cyberspace as acute as those faced by great powers, and possibly even more so given their limited economic and military capabilities and narrow influence in the international system. Traditional middle powers thus present a low-risk, high-payoff target for their adversaries in cyberspace, and consequently are accumulating a strategic deficit vis-à-vis other states that have more readily grasped such threats—and the opportunities of cyber operations as a tool of statecraft. By failing to shape adversarial behavior in cyberspace around tacitly accepted focal points cumulatively, Canada, the Netherlands, Australia, and other traditional middle powers are ceding the operational initiative to illiberal adversaries such as Russia and China, which will in turn seize that initiative to generate cyber norms that support their strategic interests.<sup>95</sup>

Faced with the prospects of a deleterious change to their environment as a result of growing instability and malicious activity in cyberspace, middle powers can *exit*, use *voice*, or demonstrate *loyalty*. Traditional middle powers such as Canada had hitherto pursued a *loyalty*

approach that prioritizes multilateral efforts and close partnerships with like-minded great powers to develop explicitly accepted cyber norms. These efforts have yet to yield significant payoff and have failed to stem the rising tide of adversarial activity that is sweeping traditional middle powers in cyberspace. As a variation on persistent engagement for the US, *functional engagement* for traditional middle powers is a *voice* approach that adapts cyber-strategic concepts of cyber persistence theory and persistent engagement to align with the limited resources and foreign policy ambitions of middle powers. Functional engagement in cyberspace seeks to harness the potential of tacit bargaining and normative shaping by focusing the limited cyber capabilities of traditional middle powers in pursuit of narrow strategic objectives. Traditional middle powers can leverage coalition cyber strategic campaigns to establish and reinforce a set of focal points that delineate acceptable from objectionable behavior by states in cyberspace.🛡️

## ACKNOWLEDGMENT

Research for this article was supported by the Social Sciences and Humanities Research Council of Canada Partnership Grant 895-2021-1007.

## NOTES

1. Leuprecht, C., Szeman, J., and Skillicorn, D.B. (2019), The Damoclean sword of offensive cyber: policy uncertainty and collective insecurity, *Contemporary Security Policy*, 40(3), 382-407, <https://doi.org/10.1080/13523260.2019.1590960>.
2. Council on Foreign Relations. (2022), Cyber Operations Tracker, Council on Foreign Relations, <https://www.cfr.org/cyber-operations/#OurMethodology>.
3. Maness, R. C., Valeriano, B., Jensen, B., Hedgecock, K., and Macias, J. (2022), The dyadic cyber incident and campaign dataset, version 2.0. Harvard Dataverse, <https://dataverse.harvard.edu/dataset.xhtml?persistentId=doi:10.7910/DVN/CQOMYV>.
4. Ibid
5. Ibid
6. Ibid
7. Ibid
8. Mitrany, D. (1933), The progress of international government. Yale University Press.
9. Shin, Dong-Min. (2015, 4 December), A critical review of the concept of middle power. E-International Relations. <https://www.e-ir.info/2015/12/04/a-critical-review-of-the-concept-of-middle-power/>.
10. Glazebrook, G. (1947). The middle powers in the United Nations system, *International Organization*, 1(2), 307-18, <https://doi.org/10.1017/S002081830000608.1>
11. Cooper, D. (2011). Challenging contemporary notions of middle power influence: Implications of the proliferation security initiative for middle power theory, *Foreign Policy Analysis*, 7(3), 317-36, <https://doi.org/10.1111/j.1743-8594.2011.00140>; Patience, A. (2014). Imagining middle powers, *Australian Journal of International Affairs*, 68(2), 210–24. <https://doi.org/10.1080/10357718.2013.840557>.
12. Chapnick, A. (1999). The middle power, *Canadian Foreign Policy Journal*, 7(2), 73-82. <https://doi.org/10.1080/11926422.1999.9673212>.
13. Ibid.
14. Holbraad, C. (1984), Middle powers in international politics, Macmillan. Shin, 2015.
15. Chapnick, A. (1999), The middle power, *Canadian Foreign Policy Journal*, 7(2), 73-82, <https://doi.org/10.1080/11926422.1999.9673212>.
16. Ibid.
17. Holbraad, C. (1971), The role of middle powers. *Cooperation and Conflict*, 6(1), 77-90, <https://doi.org/10.1177/001083677100600108>.
18. Cooper, A., Higgott, R., and Nossal, K. (1993), Relocating middle powers. University of British Columbia Press.
19. Ibid.
20. Ibid.
21. Lee, G., and Soeya, Y. (2014). The middle-power challenge in East Asia: An opportunity for co-operation between South Korea and Japan, *Global Asia*, 9(2), 85-91.
22. Jordaan, E. C. (2003). The concept of a middle power in international relations: Distinguishing between emerging and traditional middle powers, *Politikon South African Journal of Political Studies*, 30(2), 165-81.
23. Ibid.
24. Ibid.
25. Ibid.
26. Grigsby, A. (2017). The end of cyber norms. *Survival*, 59(6), 109-22. <https://doi.org/10.1080/00396338.2017.1399730>; Maurer, T. (2020). A dose of realism: The contestation and politics of cyber norms, *Hague Journal on the Rule of Law*, 12(2), 227-49, <https://doi.org/10.1007/s40803-019-00129-8>; Tikk-Ringas, E. (2017). International cyber norms dialogue as an exercise of normative power, *Georgetown Journal of International Affairs*, 17(3), 47-59, <https://www.jstor.org/stable/26395975>.
27. Jensen, E. (2017). The Tallinn Manual 2.0: Highlights and insights, *Georgetown Journal of International Law*, 48(1), <https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf>.
28. Ibid.

## NOTES

29. Stevens, T. (2012). A cyberwar of ideas? Deterrence and norms in cyberspace, *Contemporary Security Policy*, 33(1), 148–70. <https://doi.org/10.1080/13523260.2012.659597>.
30. Tikk-Ringas, 2017.
31. Hurwitz, R. (2014), The play of states: Norms and security in cyberspace. *American Foreign Policy Interests*, 36(5), 322–32, <https://doi.org/10.1080/10803920.2014.969180>, Maurer, 2020.
32. Grigsby, 2017. Maurer, 2020.
33. Sukumar, A. (2017). The UN GGE failed. Is international law in cyberspace doomed as well? *Lawfare*, <https://www.lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well>.
34. Ibid.
35. Corera, G. (2016). How France’s TV5 was almost destroyed by “Russian hackers.” BBC News. <https://www.bbc.com/news/technology-37590375>; Cyber Law Toolkit (2015, 23 December), Power grid cyberattack in Ukraine (2015). Cyber Law Toolkit, [https://cyberlaw.ccdcoe.org/wiki/Power\\_grid\\_cyberattack\\_in\\_Ukraine\\_\(2015\)](https://cyberlaw.ccdcoe.org/wiki/Power_grid_cyberattack_in_Ukraine_(2015)).
36. Greenberg, A. (2018), The untold story of NotPetya, the most devastating cyberattack in history, *Wired*, <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>.
37. United States of America. (2018b). Findings of the investigation into China’s acts, policies, and practices related to technology transfer, intellectual property, and innovation under section 301 of the Trade Act of 1974. Office of the United States Trade Representative Executive Office of the President, <https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF>.
38. United States of America. (2021, 19 July). The United States, joined by allies and partners, attributes malicious cyber activity and irresponsible state behavior to the People’s Republic of China. White House, <https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/>.
39. Maurer, 2020.
40. Ibid.
41. Goldman, E. (2022). Paradigm change requires persistence—a difficult lesson to learn. *The Cyber Defense Review*, 7(1), 113–18. <https://www.jstor.org/stable/48642031>.
42. Fischerkeller, M., and Harknett, R. (2018b). Persistent engagement and tacit bargaining: A path toward constructing norms in cyberspace. *Lawfare*, <https://www.lawfareblog.com/persistent-engagement-and-tacit-bargaining-path-toward-constructing-norms-cyberspace>.
43. Healey, J., and Jervis, R. (2020). The escalation inversion and other oddities of situational cyber stability, *Texas National Security Review*, 3(4), 30–53, <http://dx.doi.org/10.26153/tsw/10962>; Kreps S., and Schneider, J. (2019), Firebreaks in the cyber, conventional, and nuclear domains: Moving beyond effects-based logics, *Journal of Cybersecurity*, 5(1), 1–9, <https://doi.org/10.1093/cybsec/tyz007>.
44. Fischerkeller and Harknett, 2017. Harknett, R., and Goldman, E. (2016). The search for cyber fundamentals. *Journal of Information Warfare*, 15(2), 81–8. <https://www.jstor.org/stable/26487534>; Harknett, R., and Smeets, M. (2022). Cyber campaigns and strategic outcomes, *Journal of Strategic Studies*, 45(4), 534–67. <https://doi.org/10.1080/01402390.2020.1732354>.
45. Harknett and Goldman, 2016.
46. Harknett and Smeets, 2022.
47. Fischerkeller, M., and Harknett, R. (2018a), Cyber persistence theory, intelligence contests and strategic competition. Institute for Defense Analysis, <https://apps.dtic.mil/sti/pdfs/AD1118679.pdf>.
48. Harknett and Goldman, 2016. Fischerkeller and Harknett, 2017. Fischerkeller, M., and Harknett, R. (2019). Persistent engagement, agreed competition, and cyberspace interaction dynamics and escalation. *The Cyber Defense Review—Special Edition*. [https://cyberdefensereview.army.mil/Portals/6/CDR-SE\\_S5-P3-Fischerkeller.pdf](https://cyberdefensereview.army.mil/Portals/6/CDR-SE_S5-P3-Fischerkeller.pdf).
49. Fischerkeller and Harknett, 2018b. Goldman, E. (2020), From reaction to action: Adopting a competitive posture in cyber diplomacy, *Texas National Security Review*, 3(4), <https://repositories.lib.utexas.edu/bitstream/handle/2152/83957/TNSRVol3Iss4Goldman.pdf?sequence=2>.
50. Fischerkeller and Harknett, 2018b. Fischerkeller and Harknett, 2019. Goldman, 2022.
51. Fischerkeller and Harknett, 2019.

## NOTES

52. Farrell, H., Glaser, C. (2017). The role of effects, saliencies and norms in U.S. cyberwar doctrine, *Journal of Cybersecurity*, 3(1), 7-17, <https://doi.org/10.1093/cybsec/tyw015>.
53. Fischerkeller and Harknett, 2019.
54. Ibid.
55. Goldman, 2020.
56. Ibid.
57. Gallagher, S. (2019). Report: US cyber command took Russian trolls offline during midterms. *Ars Technica*, <https://arstechnica.com/information-technology/2019/02/report-us-cyber-command-took-russian-trolls-offline-during-midterms/>. Nakashima, E. (2019). U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms, *The Washington Post*, [https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9\\_story.html](https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html).
58. United States of America. (2018a). Command vision for U.S. Cyber Command: Achieve and maintain cyberspace superiority, United States Cyber Command.
59. Ibid.
60. Pomerleau, M. (2022). Cyber Command has deployed to nations 27 times to help partners improve cybersecurity. *Fedscoop*, <https://www.fedscoop.com/cyber-command-has-deployed-to-nations-27-times-to-help-partners-improve-cybersecurity/>.
61. Ibid.
62. Srivastava, M., Murgia, M., and Murphy, H. (2022). The secret US mission to bolster Ukraine's cyber defences ahead of Russia's invasion, *Financial Times*, <https://www.ft.com/content/1fb2f592-4806-42fd-a6d5-735578651471>.
63. Harknett and Goldman, 2016. Fischerkeller and Harknett, 2017. Fischerkeller and Harknett, 2019.
64. Healey, J., and Caudill, S. (2020). Success of persistent engagement in cyberspace. *Strategic Studies Quarterly*, 14(1), 9-14, [https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-14\\_Issue-1/Healey.pdf](https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-14_Issue-1/Healey.pdf).
65. United States of America, 2018a.
66. Ibid.
67. Ibid.
68. Fischerkeller and Harknett, 2017.
69. Smeets, M. (2019). There are too many red lines in cyberspace, *Lawfare*, <https://www.lawfareblog.com/there-are-too-many-red-lines-cyberspace>.
70. Lin, H., and Smeets, M. (2018). What is absent from the U.S. Cyber Command "vision," *Lawfare*, <https://www.lawfare-blog.com/what-absent-us-cyber-command-vision>; Lin, H., and Zegart, A. (2018). Bytes, bombs, and spies: The strategic dimensions of offensive cyber operations. Brookings University Press.
71. Healey, J. (2019). The implications of persistent (and permanent) engagement in cyberspace. *Journal of Cybersecurity*, 5(1), 1-15. <https://doi.org/10.1093/cybsec/tyz008>.
72. Healey and Jervis, 2020.
73. United States of America, 2018a.
74. Holbraad, 1971. Cooper et al., 1993. Chapnick, 1999.
75. Chapnick, 1999. Chapnick, A. (2000). The Canadian middle power myth, *International Journal*, 55(2), 188-206, <https://doi.org/10.2307/40203476>.
76. Chapnick, 2000.
77. Cooper et al., 1993.
78. Siebring, J. (2021). Choosing complicated: The Canadian approach to national security in cyberspace [Master's directed research paper, Royal Military College of Canada], Canadian Forces Digital Library.
79. Canadian Security Intelligence Service. (2021). CSIS public report 2020. Government of Canada, <https://www.canada.ca/content/dam/csis-scrs/documents/publications/2021/CSIS-Public-Report-2020.pdf>
80. Macnamara, D. (2012). Canada's national and international security interests. In D. McDonough (Ed.), *Canada's national security in the post-9/11 world: Strategy, Interests, and threats*, 45-56, University of Toronto Press.

## NOTES

81. Carnegie Endowment. (2022). Cyber norms index and timeline—Canada, Carnegie Endowment for International Peace, retrieved July 15, 2022, from <https://carnegieendowment.org/publications/interactive/cybernorms#timeline-section>.
82. Canada. (2017). Strong, secure, engaged: Canada's defence policy, Department of National Defence, <https://www.canada.ca/en/department-national-defence/corporate/policies-standards/canada-defence-policy.html>.
83. Vigneault, D. (December 8, 2018), Remarks by Director David Vigneault at the Economic Club of Canada. Government of Canada, [https://www.canada.ca/en/security-intelligence-service/news/2018/12/remarks-by-director-david-vigneault-at-the-economic-club-of-canada.html?fbclid=IwAR2VWCrDlF4aCznfNfeQrQoyZd\\_CMxAfCi8ihugtNmzjE\\_BrjFG4jPD-7Pag](https://www.canada.ca/en/security-intelligence-service/news/2018/12/remarks-by-director-david-vigneault-at-the-economic-club-of-canada.html?fbclid=IwAR2VWCrDlF4aCznfNfeQrQoyZd_CMxAfCi8ihugtNmzjE_BrjFG4jPD-7Pag).
84. Canada. (2020), National cyber threat assessment 2020, Canadian Centre for Cyber Security, <https://cyber.gc.ca/sites/default/files/publications/ncta-2020-e-web.pdf>; Canada. (2022), National Cyber Threat Assessment 2023-2024. Canadian Centre for Cyber Security, <https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024>.
85. Canada, 2020. Canada, 2022.
86. Voo, J., Hemani, I., Jones, S., DeSombre, W., Cassidy, D., and Schwarzenbach, A. (2020), National cyber power index 2020, Belfer Center for Science and International Affairs, [https://www.belfercenter.org/sites/default/files/2020-09/NCPI\\_2020.pdf](https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf).
87. Voo, J., Hemani, I., and Cassidy, D. (2022). National cyber power index 2022, *Belfer Center for Science and International Affairs*, <https://www.belfercenter.org/publication/national-cyber-power-index-2022>.
88. Ibid.
89. Voo et al., 2020. Voo et al., 2022.
90. Voo et al., 2022.
91. Ibid.
92. Canada, 2017.
93. Bill C-59, (2019). An Act respecting national security matters, 1st sess., 42nd Parliament, 2017, SC 2019, <https://www.parl.ca/LegisInfo/en/bill/42-1/c-59>.
94. Carvin, S. (2018). Zero D'Eh: Canada takes a bold step towards offensive cyber operations. Lawfare, <https://www.lawfare-blog.com/zero-deh-canada-takes-bold-step-towards-offensive-cyber-operations>.
95. Jordaan, 2003.





# Competitive Advantage in the Russo-Ukrainian War:

*Ukraine's  
Technological  
Potential Against  
a Kremlin Goliath*

---

Captain Melissa Vargas

## ABSTRACT

*This study explains the technological context and miscalculations that led to Russia's invasion of Ukraine and explores how public opinion shaped the technological factors that are helping Ukraine gain and maintain a competitive advantage. NATO overestimated Russia in information technology and did not account for collective hybrid efforts outside of Ukraine, emboldening Russia to push physical and ethical boundaries. However, Ukrainian forces and benefactors have been using information technology more efficiently than Russia, among other enablers, to gain a competitive advantage over its seemingly larger and more powerful adversary. Research must be conducted to understand the factors of Russia's shortfalls, properly integrate corporations using a common language, and establish rules of engagement among civilian and military agencies in the cyber domain. History and case study methodologies were used for this research. Russia's historical identity and impunity emboldened the Kremlin to invade Ukraine, underestimating the impact technological benefactors would have on Ukraine as a formidable competitor under Porter's five forces model. This conflict exposes implications for industry integration to cyber defense exercises (CDX). This research is significant because it promotes a common language and framework to integrate private organizations in applying collaborative solutions and boundaries in a domain without borders and limited regulation.*

**Keywords** – cyber defense, cyber domain, CEO, Kremlin, five forces model, hybrid warfare, multi-domain operations, Russia, Ukrainian invasion

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



CPT **Melissa Vargas** is an Infantry officer in the U.S. Army currently serving as an Observer Coach/Trainer in Europe at the Joint Multinational Readiness Center. She graduated from the United States Military Academy with a B.S. in Information Technology in 2014 and is earning her M.S. in Information Systems Management from Embry-Riddle Aeronautical University Worldwide. She originally branched into the Field Artillery in 2014 but has been an Infantry officer since 2016.

Professionally, she has held the positions of Assistant Battalion Fire Support Officer, Infantry Fire Support Officer, Fire Direction Officer, Paladin Platoon Leader, Infantry Executive Officer, Regimental Assistant Plans Officer, Squadron Assistant Operations Officer, and Infantry Troop Commander. Across all positions, particularly in the European theater, her primary scope of interest and independent research has been Russian Hybrid Warfare in Fires, Maneuver, and Multi-Domain Operations.

## **COMPETITIVE ADVANTAGE IN THE RUSSO-UKRAINIAN WAR**

**R**esearch before 2022 determined that Russia would dominate the cyber domain in a hybrid conflict and questioned civilian tech providers' ability to protect themselves under a cyber-attack.<sup>1</sup> The problem is that NATO and the EU overestimated Russia's information technology advantage and did not account for collective efforts outside of Ukraine. This research examines factors of Russia's shortfalls to integrate businesses properly using a common language. This research study aims to understand which technological factors Ukraine is leveraging against Russia.

Before Russia annexed Crimea in 2014, President Vladimir Putin alluded to Russia's imperialistic ideology that Ukraine is not a country and that its population is of "one people" with Russian roots and cultural identity, undermining the Ukrainian language and heritage.<sup>2</sup> Crimea's annexation developed speculation about Russian capabilities and the ways that it would leverage cyber warfare and information among other technologies that NATO refers to as "hybrid warfare,"<sup>3</sup> perpetuating Russia's misperceived strength, contributing to its traditional impunity, and emboldening Russian aggression against Ukraine prior to its invasion in February 2022.<sup>4</sup>

When countries overestimate Russia, they underestimate their abilities and become reluctant to act for fear of retaliation, emboldening Russia to push physical and ethical boundaries. Additionally, the by-product of civilian technology companies involving themselves blurs lines that differentiate between combatants and non-combatants, potentially endangering employees. Until recent events, research was limited by our inability to observe Russian hybrid tactics and its integration with conventional military tactics. Militarily and commercially, this domain has been contentious in terms of

discussing ethics and regulation. This research is important in understanding the commercial impacts of technology in hybrid warfare, an area that researchers have studied less than the military technological impacts. The research adds to the body of knowledge by evaluating this occurrence of hybrid warfare in the context of commercial business competitive advantage and how worldwide opinion and technological support undermined Russia. The research notes the value of military technology in conventional warfare but focuses on commercial factors for which case studies are limited. Additionally, the research supports recommendations for collaborative information systems training, governance, and legal ethical policy.

## **KREMLIN IDEOLOGY**

To fully appreciate how the public came to misperceive Russia's power, a review based on chronology articulated a contextual understanding of the research that further perpetuated its image. Recognizing the annexation of Crimea in 2014, the post-Ukrainian Russian invasion in 2022, and the period between them drew common threads and themes that spanned over 200 years. An assessment of the degree to which each theme has been examined then promoted continued exploration of pervasive knowledge gaps.

Well before Russia annexed Crimea, the Kremlin held beliefs about Russia's place in the world as an empire. Most literature concerning Russian identity and history points to evidence that it is imperialistic by nature and has made efforts to undermine Baltic and Slavic states since the 1900s.<sup>5</sup> Most sources neglected to address Russian imperialist patterns dating as far back as the 1700s. Research often minimized its historic pattern of expansion despite being a relatively weak global power. From the 1700s to the 1940s Peter the Great, Alexander I, and Stalin achieved victories that resulted in expansive land acquisitions but did not result in dramatically increased purchasing power or quality of life. At the height of three expansions, Russia proved to be brittle yet resilient in three embarrassing losses against Crimea in 1856, Japan in 1905, and the Cold War. It was large on land but relatively weak on paper and inaccurately presented itself as more powerful than it really was. Its imperialist behavior was expected.

The literature after Russia's annexation of Crimea was the most extensive, in which research and speculation of hybrid warfare further elevated perceptions of Russia as a military power. Its concept of subversion was already widely established before 2014 as a strategy to undermine Western political powers internally.<sup>6</sup> Though subversion and hybrid warfare are used almost interchangeably and have very similar characteristics, the key difference is that subversion includes actions that may be integrated with covert cyber and military assets but intends to keep Russia away from open conflict. When Russia is involved in a direct, open conflict, more aggressive hybrid warfare measures are synchronized, such as using cyber-attacks on infrastructure shortly before moving military assets prior to an invasion. Case studies of Crimea's annexation perpetuated Russia's powerful image and deterred impunity.

Since Russia invaded Ukraine in February 2022, academic and open-source discussions have focused on Russia's targeting of Ukrainian private and public information systems in hybrid warfare, but there is limited research on the civilian and commercial assets that are aiding Ukrainians. Research cites military and commercial agencies that aid Ukraine in collective efforts and allude to the ethical implications among government agencies, and very little concerning its civilian benefactors.<sup>7</sup> Due to the evolving nature of the conflict, research on public opinion impacts, the commercial business factors that helped Ukraine gain a competitive advantage, and the resulting ethical implications are limited.

## **HYBRID METHODOLOGY: A HISTORICAL AND CASE STUDY APPROACH**

The research questions, which required a comparative analysis across history and its application to current events, determined a hybrid historical and case study methodology. The purpose of the research was twofold – to better understand the historical context and patterns leading up to the Russo-Ukrainian war and to gain a deeper understanding of the recent events that contradicted researchers' predictions about Russia's skill in a hybrid war. "A history-informed agenda...allows us to develop more informed causal theories about achievement (or failure to achieve) of organizational outcomes such as growth, survival, or a sustainable competitive advantage."<sup>8</sup> The historical method established patterns that resulted in the widely accepted prediction that Russia would dominate in the cyber domain. Historical research methods and qualitative data are useful when studying changes in strategy as they unfold over time.<sup>9</sup> Case studies are most effective in investigating humans and interactions with technology, as well as determining and proposing ethical borders in a discipline.<sup>10</sup> A hybrid approach was the best method to address themes across history, recent events, and ethics. Both methods are innately descriptive and often absent experimental data.<sup>11</sup>

### ***Sampling Design***

Source sampling consisted of three chronological areas which later resulted in three key themes. The chronological areas were the periods before the annexation of Crimea, the dwell period between this annexation and the Russian invasion of Ukraine, and the period immediately after the invasion up to the present. Sampling from these periods was important because it established that deeply rooted Russian imperialism drove the inevitability of the invasion, that NATO and the EU perceived Russia as much stronger than it was, and that Russia proved to be not so formidable, contrary to historical predictions.<sup>12</sup> The themes that arose from sampling these distinct time frames and comparing them were that researchers misperceived Russia in terms of its hybrid prowess and that technological support from outside Ukraine played a significant role in its recent performance.<sup>13</sup> The sampling design was primarily chronological for a comparative measure but also ensured analysis of sources from opposite perspectives across the themes.

### ***Materials***

Qualitative data were gathered for this research, with limitations. First, the possibility of direct interviews with Ukrainian combat forces was considered. However, this method would have required lengthy legal reviews and unlikely bilateral approvals requiring more than nine weeks to conduct. Second, participant observation was neither applicable nor permissible within constructs of military duties and responsibilities. Therefore, the only applicable method was to analyze existing data from past predictions and current events as the war unfolds absent of retrospect.<sup>14</sup> The scope of materials excludes interviews and direct participation but includes observations and interactions from existing sources, experts, and current events.

The reliability and validity criteria of researching prioritized four main characteristics when selecting sources: proximity, focus, currency, and scholarliness. Proximity assessed the subjective value of each source in terms of its immediacy to the theme in question. The focus categorized data in terms of history, technological applications, and ethics; materials rarely addressed all three. The date that the research was published was assessed to capture accurately the perceptions surrounding Russia in each time frame without the context of the Ukrainian invasion in mind. Scholarliness was the most objective criterion that prioritized peer-reviewed, expert articles from scholarly journals. Materials used included books, scholarly articles, videos, news articles, and policy papers.

### ***Procedure***

Various research materials were considered and required differing degrees of each of the criteria depending on the themes being researched. Sources with the least proximity were those that observed Russian history as early as the 18th century. Russian imperial culture is not a groundbreaking concept and literature establishing these patterns by historical experts was widely available. It was not necessary to obtain primary sources when peer-reviewed articles established this concept. The most proximate sources consisted of current policies, regulations, and proposals published by key stakeholders in the Russo-Ukrainian war or research which used primary sources from the conflict such as Microsoft's proposed Digital Geneva Conventions<sup>15</sup> and data points on public opinion concerning the Russo-Ukrainian war made available by Chinese data scientists.<sup>16</sup>

Data focuses were organized chronologically but categorized to cover the topics of history, technological applications, and ethics. Materials that covered narrow scopes to capture more details among the focuses were of higher priority than materials that considered these subjects only on their periphery. If available, perspectives which argued contradicting positions on each focus provided valuable insight. Some of the articles that argued opposing views concerning Russian historical prowess and technological applications resulting in a competitive advantage greatly assisted in identifying the factors that contributed toward Russian and Ukrainian performance in the ongoing war.

The currency of the data did not hold objective value; more recent data were not always prioritized over other sources. When analyzing data from before the annexation of Crimea, after the invasion of Ukraine, and the period in between, it was important to prioritize data published within those respective periods to capture accurate perceptions and sentiments surrounding Russian hybrid warfare relative to NATO and the European Union.

Finally, scholarliness varied across periods and focuses. More proximate sources were inherently less scholarly but more current. However, more current sources did not always imply proximity or scholarliness. Despite scholarliness having a value that was lower relative to when it was applied to older time frames, it still retained a higher value over all other materials reflecting analysis and drew conclusions but were not peer-reviewed such as blogs and opinion news articles. Non-peer-reviewed news articles addressing the Russo-Ukrainian war retained value due to a large gap in the body of literature; there was significant value in scanning for data points and empirical statistics from that material. Additionally, policy papers and other such materials were inherently not scholarly but highly valuable in formulating ethical implications.

The outcomes of the procedures provided the basis for which the research was organized and identified the key themes and factors that required further research and analysis. Because the challenge in identifying themes is that they were abstract and difficult to identify,<sup>17</sup> selecting a historical approach identified the themes of perceived Russian strength and how history applied to the technological competitive advantage they have projected since the annexation of Crimea. The case study approach identified additional categories of Ukrainian technological advantage within the latter theme and delineated the ethical theme that uniquely applies to the Russo-Ukrainian war.

### ***Justification and Limitations***

To summarize methodology selection, a hybrid approach accurately captured NATO and EU perceptions of Russian strength in information warfare before and after the annexation of Crimea. The historical approach rendered the identification of two of the three key themes and helped formulate causal theories of the ways Ukraine may be gaining a technological competitive advantage in the war. The case study approach contributed to the technological competitive advantage theme of “the first major conflict involving large-scale cyber operations.”<sup>18</sup> These methodologies were best suited for typically qualitative data. However, both methods were limited in primary sources due to restrictions that prevent direct involvement in the conflict to study. Additionally, qualitative data analysis is inherently subject to human error in thematic abstraction as well as content interpretation.<sup>19</sup>

## **FINDINGS AND DISCUSSION**

Three themes stood out while conducting research. First, the perception of Russia’s power projection is not a phenomenon of recent history, i.e., within the last 100 years. Russia has an



established expansionist pattern and conducts strategic messaging to create the perception of strength and to bolster the notion that it is more powerful than it is. Every instance of a cyber-attack between 2014 and 2022 became a cause for significant concern, and Russia's impunity further inflated that image. Second, world powers did not anticipate Ukraine's collective technological benefactors resulting from public opinion, both commercially and militarily, that would affect the tide of war in their favor. Finally, the application of Porter's five forces model, one that is traditionally used to explain factors that contribute to competitive advantage in business,<sup>20</sup> adds clarity to understanding the factors contributing to competitive advantage and strategy.

### ***Perception of Russian Cyber Domain and Hybrid Prowess***

Research trends surrounding Russian cyber and information warfare established the notion that Russia could do whatever it wanted to other nations' systems without regard for common, yet unwritten, decency. Russia's perceived prowess before 2014 resulted in limited sanctions for its actions from NATO and the EU, further bolstering its impunity. Comparatively, its system of government and policies were more consolidated and unified than NATO's to execute offensive cyber operations and defend against attacks.<sup>21</sup> Adding to external misperceptions, Russia was transparent about how it prioritized the information sphere and non-military tactics. Not only did Russia seem better rehearsed in the cyber domain with more effective policies, but it also messaged proactivity, aggression, and impunity so that other countries would not interfere for fear of repercussion. The NATO unity of command in a ground attack is very clear<sup>22</sup> because it has a legal direction to act as one. Cyber-attacks are not covered in the same unified and tangible manner, leading NATO to perceive itself as weaker in this domain despite being wealthier and larger overall.<sup>23</sup> However, Swedish cyber defense exercises (CDXs)<sup>24</sup> may provide a blueprint for integrating industry allies into NATO's Cyber Coalition Exercises<sup>25</sup> to build unity of command and collaborative solutions against threats to the private sector. Russia's numerous transgressions, impunity, and overt messaging, plus NATO's limited cyber-unity, are the established factors that perpetuated Russia's image. Putin's actions proved counterproductive and entrenched Ukraine deeper in the West,<sup>26</sup> leading to Russia's miscalculation of Ukrainian identity and degree of support.

### ***Technological Aid and Support from Outside Ukraine***

The commercial technological support from outside Ukraine is well documented but poorly consolidated because the conflict is ongoing. The volume of financial and military aid has fluctuated with subjective popular opinion worldwide. This kind of collaborative global indirect support is unprecedented and largely unofficial. Leaders did not anticipate this situation due to the lack of official policies and procedures in effect regarding Ukraine as a non-NATO nation.<sup>27</sup> The cyber domain has no borders and limited governance in wartime conditions, yet Ukraine was able to gain and maintain a competitive advantage through technology and public opinion against Russia.

## COMPETITIVE ADVANTAGE: FIVE FORCES APPLIED

Though Porter's five forces model is traditionally used to explain factors that contribute to competitive advantage in business,<sup>28</sup> it can be reframed to describe and conceptualize the commercial technological factors that play a strategic supporting role in military efforts. The five forces discussed and renamed in this study are the bargaining power of suppliers, the threat of substitute products, the bargaining power of buyers, the threat of new entrants, and rivalry among existing competitors.<sup>29</sup> In this article they are applied to Russia and Ukraine as business competitors to account for the tangible and intangible factors that were attributed to Ukraine's unanticipated success. Benefactors to either country are considered suppliers and buyers depending on their type of support. The product each country provides in this hypothetical market is national security, interests, and ideologies for their domestic consumer populations and financial benefactors. Consider that each factor is bolstered by public opinion, and analogous to brand loyalty.

**1. Bargaining Power of Supporters.** In business, the bargaining power of suppliers refers to the number and size of suppliers, the uniqueness of each supplier's product, and the company's ability to substitute.<sup>30</sup> In the Russo-Ukrainian war, the number and size of suppliers are the tech supporters, whereas Russia has fewer suppliers in technological aid. Though the IT suppliers do not offer unique products, Ukraine enjoys exclusive IT and cyber defense support from larger commercial assets like Microsoft and Starlink that Russia does not.<sup>31</sup> Starlink support raised SpaceX valuation to \$127 billion in 2022, increasing its status among tech giants.<sup>32</sup> Conversely, China continues to maintain an openly neutral sentiment that advocates for peace and sending Chinese representatives to Russia, Ukraine, and many other countries to support conflict resolution.<sup>33</sup> In addition to actively supporting Ukraine with IT, many countries, primarily the U.S., have implemented restrictions on technology to undermine Russia's industries.<sup>34</sup> Where Ukraine reaps the benefits of various technological supporters, military and commercial, for a competitive advantage, Russia relies mostly on itself.

**2. Threat of Substitute Security Measures.** The threat of substitute products refers to the number of substitute products, the buyer's propensity to substitute, and relative price performance.<sup>35</sup> In the national security context, this is reframed as the threat of substitute security measures. There are no substitute national defense agencies for either country, short of the U.S. or China's militaries stepping in to defend either one in a higher-impact conflict if its forces are decimated. The buyer's propensity to substitute refers to the benefactor's propensity to substitute indirect financial and technological aid with direct combat support; the latter is not consistent with global interests to maintain physical national security.<sup>36</sup> The threat of global powers substituting indirect technological support for direct high-impact warfare as a national security measure is low.

**3. Bargaining Power of Benefactors.** The bargaining power of buyers is the number of customers, differences between competitors, and the buyer's information ability.<sup>37</sup> The buyers are the benefactors that are contributing monetary aid to Ukraine in exchange for their sovereignty, which represents Western democracies and the opportunity to stay out of direct combat. From January 23, 2022, to October 3, 2022, Western countries, Japan, and Taiwan sent Ukraine over 90 billion euros in financial, humanitarian, and military aid.<sup>38</sup> The difference between the competitors is defined by their views on sovereignty and their respective levels of positive public opinion. The buyer's information availability is characterized by open-source interpretations of the current events in Ukraine. Russian policies align better with its internal state media to control its internal messaging<sup>39</sup> but have little effect outside of its borders. "The COVID-19 pandemic promoted collaborative fact-checking on an international scale."<sup>40</sup> Lessons learned from the Russian cyber-attacks, along with COVID-19 and political misinformation efforts became case studies that allowed agencies to refine their practices. Ukraine holds a relative advantage in the number of supporters and benefactors to its national security and ideology. The collective effectiveness of commercial and government agencies fighting against Russian misinformation efforts in the cyber domain is evidence of their advantage.

**4. Threat of New Adversaries.** The threat of new entrants refers to cumulative experience, government policies, brand loyalty, and capital requirements.<sup>41</sup> Russia alone has more experience in hybrid warfare than Ukraine but, in a cyber war involving private and public supporters on either side of the cyber conflict, Russia is outmatched as well as any other potential adversary that has not already aligned itself with a side. Government policies do not exclude commercial IT supporters, which are encouraged by public opinion, from helping Ukraine. The predicted human, technological, and financial capital to join a high-impact war against Russia or Ukraine exceeds the capital to remain a peripheral supporter. The threat of new adversaries that would compromise Ukraine's sovereignty and undermine autonomy is low.

**5. Rivalry Among Existing Competitors.** Finally, rivalry among existing competitors is the central factor that is impacted by the other four. It refers to the number of competitors, brand loyalty, and quality differences.<sup>42</sup> Ukraine has only one country to compete against. Brand loyalty is comparable to the rates at which public opinion affects domestic support for each country's efforts, also heavily affecting external aid to their causes. The quality of Ukraine's and Russia's national security forces depends on the bargaining power of supporters, the threat of substitute security measures, the bargaining power of benefactors, and the threat of new adversaries. Russia's underwhelming cyber effects are attributed to Ukraine's benefactors, both commercial and military, protecting its cyber sovereignty.<sup>43</sup> So long as Ukraine leverages the five factors, it can gain and maintain a competitive advantage over Russia, despite its relatively smaller size and limited internal assets.

## **CONCLUSION**

Despite reluctance to act against Russian aggression that emboldened the Kremlin to overstep physical and ethical boundaries, formal and informal cyber-defense agencies worldwide were able to take advantage of Russian transgressions as case studies to analyze them and build effective defenses. Worldwide popular opinion reinforced Ukraine's ability to compete with Russia on the world stage despite its original disadvantages. While the unprecedented benefits of commercial IT benefactors significantly aided government efforts against Russian cyber-attacks and misinformation in a hybrid war, commercial IT support raises concern and urgency to establish international policies that define and protect non-combatants in cyberspace; though SpaceX restricted Starlink from being used in offensive operations as recently as February 2023, its involvement in the war continues to initiate debate and garner support for stronger public-private relationships with rising tech companies.<sup>44</sup>

### ***Future Direction***

As the war unfolds and someday concludes, a deeper study should be conducted with qualitative and quantitative feedback from those involved. In China, researchers applied a quantitative approach toward public opinion for or against the war. More research is required to understand the accuracy, feasibility, and ethics of applying business intelligence to international policy and decision-making. If NATO integrates private actors into CDXs with the five forces model used as a common language, researchers can assess the applicability and propose refinements to subcomponents from an empirical system dynamics perspective. Research providing a detailed approach toward rules of engagement must be conducted if private actors are formally introduced to cyber operations.🛡️

## **DISCLAIMER**

The views expressed in this work are those of the author 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.

APPENDIX



Figure 1: Reframed Five Forces Model.

## NOTES

1. Sascha Dov Bachmann and Hakan Gunneriusson, "Russia's hybrid warfare in the east: The integral nature of the information sphere." *Georgetown Journal of International Affairs* (Johns Hopkins University Press, 2015) 16: 198+. Accessed November 5, 2022, [https://go-gale-com.ezproxy.libproxy.db.erau.edu/ps/retrieve.do?tabID=T002&resultListType=RE-SULT\\_LIST&searchResultsType=SingleTab&hitCount=365&searchType=BasicSearchForm&currentPosition=17&docId=-GALE%7CA474768082&docType=Essay&sort=Relevance&contentSegmen](https://go-gale-com.ezproxy.libproxy.db.erau.edu/ps/retrieve.do?tabID=T002&resultListType=RE-SULT_LIST&searchResultsType=SingleTab&hitCount=365&searchType=BasicSearchForm&currentPosition=17&docId=-GALE%7CA474768082&docType=Essay&sort=Relevance&contentSegmen).
2. Jefferey Mankoff, *Russia's War in Ukraine: Identity, History, and Conflict*. Center for Strategic International Studies (2022). Accessed November 4, 2022, <https://www.jstor.org/stable/resrep40567>.
3. Joshua A. Sanborn, "RUSSIAN IMPERIALISM, 1914-2014: ANNEXATIONIST, ADVENTURIST, OR ANXIOUS?" *Revolutionary Russia* 27, no 5 (2014): 92-108, <https://doi.org/10.1080/09546545.2014.973677>.
4. Abishur Prakash, "How Technology Companies Are Shaping the Ukraine Conflict," last modified October 28, 2022, <https://www.scientificamerican.com/article/how-technology-companies-are-shaping-the-ukraine-conflict/>.
5. Jefferey Mankoff, *Russia's War in Ukraine: Identity, History, and Conflict*. Center for Strategic International Studies (2022). Accessed November 4, 2022, <https://www.jstor.org/stable/resrep40567>.
6. Andrew Radin, Alyssa Demus, and Krystyna Marcinek, *Understanding Russian Subversion: Patterns, Threats, and Responses*, RAND Corporation (2020): 6, <https://www.jstor.org/stable/resrep26519>.
7. Marcus Willet, "The Cyber Dimension of the Russia-Ukraine War," *Survival* 64, no.5 (2022): 7-26, <https://doi.org/10.1080/00396338.2022.2126193>.
8. Nicholas S. Argyres, Alfredo De Massis, Nicolai J. Foss, Federico Frattini, Geoffrey Jones, and Brian S. Silverman, "History informed strategy research: The promise of history and historical research methods in advancing strategy scholarship," *Strategic Management Journal* 41, no. 3 (2019): 343-368, <https://doi.org/10.1002/smj.3118>.
9. Ibid.
10. Emad Yaghmaei and Alexander Brem, "Case study research to reflect societal and ethical issues: Introduction of a research implementation plan for ICTs." *Computers & society*, 45 no. 3 (2016): 306-312, <https://doi.org/10.1145/2874239.2874284>.
11. Nova Allison, *Types Of Qualitative Research – Overview & Examples*, accessed December 2, 2022, <https://www.mypersfectwords.com/blog/research-paper-guide/types-of-qualitative-research>.
12. Stephen Kotkin, "Russia's Perpetual Geopolitics: Putin Returns to the Historical Pattern," *Foreign Affairs* 95, no. 3 (2016): 2-9.
13. Abishur Prakash, "How Technology Companies Are Shaping the Ukraine Conflict," last modified October 28, 2022, <https://www.scientificamerican.com/article/how-technology-companies-are-shaping-the-ukraine-conflict/>.
14. Nova Allison, *Types Of Qualitative Research – Overview & Examples*, accessed December 2, 2022, <https://www.mypersfectwords.com/blog/research-paper-guide/types-of-qualitative-research>.
15. "A Digital Geneva Convention to protect cyberspace, Microsoft Policy Papers," Microsoft, accessed November 20, 2022, <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH>.
16. Bingyang Chen, Xiao Wang, Weishan Zhang, Tao Chen, Chenyu Sun, Zhenqi Wang, and Fei-Yue Wang, "Public Opinion Dynamics in Cyberspace on Russia-Ukraine War: A Case Analysis With Chinese Weibo," *IEEE Transactions on Computational Social Systems* 9, no.3 (2022): 948-958, <https://doi.org/10.1109/TCSS.2022.3169332>.
17. Ulla H. Graneheim, Britt-Marie Lindgren, and Berit Lundman, "Methodological challenges in qualitative content analysis: A discussion paper," *Nurse Education Today* 56 (2017): 29-34, <https://doi.org/10.1016/j.nedt.2017.06.002>.
18. Lewis, A. J. (2022). *Cyber War and Ukraine*. Strategic Technologies Program. Washington D.C.: Center For Strategic & International Studies. Retrieved October 13, 2023, from <https://www.csis.org/analysis/cyber-war-and-ukraine>.
19. Ibid.
20. "The Five Competitive Forces That Shape Strategy," *Harvard Business Review*, filmed June 30 2008, video, accessed November 1, 2022, [https://www.youtube.com/watch?v=mYF2\\_FBCvXw](https://www.youtube.com/watch?v=mYF2_FBCvXw).
21. Kimberly Lukin, "Russian Cyberwarfare Taxonomy and Cybersecurity Contradictions between Russia and EU: An Analysis of Management, Strategies, Standards, and Legal Aspects." *Handbook of Research on Civil Society and National Security in the Era of Cyber Warfare*, (IGI Global, 2015), [https://search-credoreference-com.ezproxy.libproxy.db.erau.edu/content/entry/igitkws/russian\\_cyberwarfare\\_taxonomy\\_and\\_cybersecurity\\_contradictions\\_between\\_russia\\_and\\_eu\\_an\\_analysis\\_of\\_management\\_strategies\\_standards\\_and\\_legal\\_aspects/0](https://search-credoreference-com.ezproxy.libproxy.db.erau.edu/content/entry/igitkws/russian_cyberwarfare_taxonomy_and_cybersecurity_contradictions_between_russia_and_eu_an_analysis_of_management_strategies_standards_and_legal_aspects/0).
22. Marcus Willet, "The Cyber Dimension of the Russia-Ukraine War," *Survival* 64, no. 5 (2022): 7-26, <https://doi.org/10.1080/00396338.2022.2126193>.
23. Alba Iulia Catrinel Popescu, "OBSERVATIONS REGARDING THE ACTUALITY OF THE HYBRID WAR. CASE STUDY: UKRAINE," *Strategic Impact* 53 (2014): 124, <https://www.proquest.com/docview/1692921972?pq-origsite=primo>.

## NOTES

24. Catherine Stupp, "Sweden tests cyber defenses as war and NATO bid raise security risks; military, government and corporate cyber defense experts participated in an exercise focused on protecting the internet infrastructure," *WSJ Pro, Cyber Security* (2022), <http://ezproxy.libproxy.db.erau.edu/login?url=https://www.proquest.com/trade-journals/sweden-tests-cyber-defenses-as-war-nato-bid-raise/docview/2716865468/se-2>.
25. Allied Command Transformation, *Exercise Cyber Coalition 2022 Concludes in Estonia*, last modified December 2, 2022, <https://act.nato.int/articles/exercise-cyber-coalition-2022-concludes-estonia>.
26. Stephen Kotkin, "Russia's Perpetual Geopolitics: Putin Returns to the Historical Pattern," *Foreign Affairs* 95, no. 3 (2016): 2-9.
27. Kimberly Lukin, "Russian Cyberwarfare Taxonomy and Cybersecurity Contradictions between Russia and EU: An Analysis of Management, Strategies, Standards, and Legal Aspects." *Handbook of Research on Civil Society and National Security in the Era of Cyber Warfare* (IGI Global, 2015), [https://search-credoreference-com.ezproxy.libproxy.db.erau.edu/content/entry/igitkws/russian\\_cyberwarfare\\_taxonomy\\_and\\_cybersecurity\\_contradictions\\_between\\_russia\\_and\\_eu\\_an\\_analysis\\_of\\_management\\_strategies\\_standards\\_and\\_legal\\_aspects/0](https://search-credoreference-com.ezproxy.libproxy.db.erau.edu/content/entry/igitkws/russian_cyberwarfare_taxonomy_and_cybersecurity_contradictions_between_russia_and_eu_an_analysis_of_management_strategies_standards_and_legal_aspects/0).
28. "The Five Competitive Forces That Shape Strategy," *Harvard Business Review*, filmed June 30 2008, video, accessed November 1, 2022, [https://www.youtube.com/watch?v=mYF2\\_FBCvXw](https://www.youtube.com/watch?v=mYF2_FBCvXw).
29. Ibid.
30. Ibid.
31. Abishur Prakash, "How Technology Companies Are Shaping the Ukraine Conflict," last modified October 28, 2022, <https://www.scientificamerican.com/article/how-technology-companies-are-shaping-the-ukraine-conflict/>.
32. "Starlink and the Russia-Ukraine War: A Case of Commercial Technology and Public Purpose?." Belfer Center for Science and International Affairs, Harvard Kennedy School, March 9, 2023.
33. China's Position on Russia's Invasion of Ukraine. U.S.-China Economic and Security Review Commission. Washington D.C.: U.S.-China Commission. Retrieved October 13, 2023, from <https://www.uscc.gov/research/chinas-position-russias-invasion-ukraine>.
34. Kate O'Keeffe, "The Ukraine Crisis: U.S. Acts to Block Technology, Other Exports to Kremlin," *The Wall Street Journal*, April 8, 2022, Eastern Edition: A.8, <https://www.proquest.com/docview/2647961543?parentSessionId=nsxJeRlagjLJDe4fyEeR-6F3H4tCxHSV8e7fUlzP48KU%3D&pq-origsite=primo&accountid=27203>.
35. "The Five Competitive Forces That Shape Strategy," *Harvard Business Review*, filmed June 30, 2008, video, accessed November 1, 2022, [https://www.youtube.com/watch?v=mYF2\\_FBCvXw](https://www.youtube.com/watch?v=mYF2_FBCvXw).
36. Kate O'Keeffe, "The Ukraine Crisis: U.S. Acts to Block Technology, Other Exports to Kremlin," *The Wall Street Journal*, April 8 2022, Eastern Edition ed.: A.8, <https://www.proquest.com/docview/2647961543?parentSessionId=nsxJeRlagjLJDe4fyEeR6F3H4tCxHSV8e7fUlzP48KU%3D&pq-origsite=primo&accountid=27203>.
37. "The Five Competitive Forces That Shape Strategy," *Harvard Business Review*, filmed June 30 2008, video, accessed November 1, 2022, [https://www.youtube.com/watch?v=mYF2\\_FBCvXw](https://www.youtube.com/watch?v=mYF2_FBCvXw).
38. "Total bilateral aid commitments to Ukraine 2022, by country and type," *Statista*, Statista Research Department, last modified October 11, 2022, <https://www.statista.com/statistics/1303432/total-bilateral-aid-to-ukraine/>.
39. Kazimierz Pierzchala, "Information Warfare Between Russia and Ukraine: A Cause of War for the West?" *Polish Political Science* 48, no. 1 (2019): 103-111, <http://czasopisma.marszalek.com.pl/images/pliki/ppsy/48-1/ppsy2019106.pdf>.
40. Noemi Morejón-Llamas, Pablo Martín-Ramallal, and Juan-Pablo Micaletto-Belda, "Twitter content curation as an antidote to hybrid warfare during Russia's invasion of Ukraine," *Profesional de la información* 31 (2022): e310308, <https://doi.org/10.3145/epi.2022.may.08>.
41. "The Five Competitive Forces That Shape Strategy," *Harvard Business Review*, filmed June 30, 2008, video, accessed November 1, 2022, [https://www.youtube.com/watch?v=mYF2\\_FBCvXw](https://www.youtube.com/watch?v=mYF2_FBCvXw).
42. Ibid.
43. Marcus Willet, "The Cyber Dimension of the Russia-Ukraine War," *Survival* 64, no. 5 (2022): 19, <https://doi.org/10.1080/00396338.2022.2126193>.
44. "Starlink and the Russia-Ukraine War: A Case of Commercial Technology and Public Purpose?." Belfer Center for Science and International Affairs, Harvard Kennedy School, March 9, 2023.
45. Bingyang Chen, Xiao Wang, Weishan Zhang, Tao Chen, Chenyu Sun, Zhenqi Wang, and Fei-Yue Wang, "Public Opinion Dynamics in Cyberspace on Russia-Ukraine War: A Case Analysis With Chinese Weibo," *IEEE Transactions on Computational Social Systems* 9, no. 3 (2022): 948-958, <https://doi.org/10.1109/TCSS.2022.3169332>.





# Beyond “Bigger, Faster, Better:” Assessing Thinking About Artificial Intelligence and Cyber Conflict

---

Dr. Christopher Whyte

## ABSTRACT

*As cybersecurity researchers and scholars of cyber conflict studies turn to think about the impact that artificial intelligence (AI) technologies will have on patterns of digital insecurity, it is important that they learn from the record of recent technological transformation of the national security enterprise. This research note considers the challenge of forthcoming changes in the dynamics of global cyber conflict brought about by AI. It identifies a tendency in the way commentators frame the intersection of these technological areas with known technical or operational touchstones. Specifically, commentary along both lines often ignores the question of evolving strategic context in much the same way that early scholars of cyber conflict often did, reducing any conclusion about the impact of AI on cyber conflict to a simplistic “bigger, faster, smarter, better” bottom line. In place of these frames, I suggest a simple four-part typology that envisions cyber conflict dynamics in which interaction (1) employs AI, (2) is conducted against AI, (3) is undertaken entirely by AI, and (4) is shaped and attenuated by AI.*

**A**s cybersecurity researchers and scholars of cyber conflict assess the impact that artificial intelligence (AI) technologies will have on conditions of digital insecurity, it is important that they learn from the record of recent technological transformation of the national security enterprise. After all, early attempts to talk sensibly about the implications of new, revolutionary information and communications technologies (ICT) for national security often fail to consider the independent positive and negative effects of new ICT on society as a whole. With both the Internet and the social

© 2023 Dr. Christopher Whyte



**Dr. Christopher Whyte** is an assistant professor of homeland security and emergency preparedness in the Wilder School of Government and Public Affairs at Virginia Commonwealth University. His research presently focuses on the decision-making dynamics of cyber operations, the role of fringe virtual space in supporting influence campaigns, and the impact of artificial intelligence on cyber conflict dynamics. He is the author of nearly thirty peer-reviewed articles on these subjects and two books on cyber conflict. He is also coauthor of “Information in War,” a book on AI and military innovation published by Georgetown University Press in 2022, and author of “Subversion 2.0,” a book on fringe social movements and the Internet, to be published by Oxford University Press in 2024.

media/mobile device revolutions, for instance, an immense volume of public and expert discourse was dominated for many years by a curious disconnect between descriptions of possible insecurity at the lowest and highest levels of analysis. Many early scholarly works on cyber conflict nested their analyses in technical scenarios, attempting to forecast how denial of service attacks or use of malware might change the strategic calculus of political actors like terrorists or state militaries. Simultaneously, the first two decades of expert discourse on cyber conflict in the West was dominated by high-level depictions of widespread disruption and dysfunction made possible by digital means. Today, many analysts would likely describe the themes of these assessments as curiously contradictory, with acknowledgement of the limitations of cyber instruments not reflected in all-too-common portents of cyber doom.<sup>1</sup>

This tendency leads to an incomplete vision of strategic circumstances. Cyber instruments are in widespread use by criminals and all manner of security actors today – compared with the world in, say, 1990 – because every facet of social, economic, political and infrastructural function has been rewired by web technologies. The value in their use is only partly in the character, ease and reach of the technique and more so in the human correlates of technology usage. At the same time, the “cyberwar” envisioned by alarmists of years past is now recognized as unlikely in the extreme due to the lacking sociopolitical value in such an activity absent some additional conflict actions.<sup>2</sup>

This research note considers the challenge of addressing forthcoming changes in the dynamics of global cyber conflict brought about by AI. In place of conventional modes of thinking about the issue, I suggest a simple four-part framework that envisions cyber conflict dynamics in which interaction (1) employs AI, (2) is conducted against AI, (3) is undertaken entirely by AI, and (4) is shaped and attenuated by AI. Recasting conversations around these issues and away from

simplistic techno-strategic imaginings to a more holistic effort to tie the implications of AI employed at scale to the evolving cyber conflict today is critical if researchers in cybersecurity, international relations (IR) and other fields are to effectively address AI's relationship to evolving digital insecurity.

## **THINKING ABOUT ARTIFICIAL INTELLIGENCE AND CYBER CONFLICT**

Artificial intelligence is an umbrella term that covers a wide spectrum of techno-scientific-societal developments that span numerous disciplines.<sup>3,4</sup> Recent work has cast AI as a transformative influence that could shape cyber conflict dynamics in years to come. This extends to all areas of cyber operations, from offensive to defensive activities.<sup>5</sup> At this stage, however, empirical examination of the impact of AI on cyber conflict remains the purview of a small number of people, limited material and a relatively small number of examples. Explorations of AI's role in enhancing and changing patterns of cyber engagement remain hypothetical and often hyperbolic. As such, attempts to project areas of future opportunity and potential quagmire also remain mired in analysis absent from real world context. As has been argued elsewhere, it seems reasonable that the present tendency to "characterize most assessments of AI's potential impact on cybersecurity as the move towards more of the same, just 'faster, smarter, bigger, better'"<sup>6</sup> will persist. Both scholars and practitioners tend to center on the idea – and resultant alarm – that AI will likely lead to more sophisticated cyber threats that might achieve strategic effects as well as a more varied operational capacity. This upgrading of cyber conflict suggests a future in which the challenge of defense and deterrence of an immense, fragmented attack surface composed of organizations, sectors and entire nations, and ever more sophisticated malicious code becoming far harder to model, capture and neutralize than is presently the case.<sup>7</sup> On top of this, increasingly sophisticated AI (including employing machine learning) promises to make cyber tools more accessible among actors that might not presently be thought capable of sustaining persistent, sophisticated engagements. This is worrying particularly because the toolkit of advanced cyber techniques from which attackers select is therefore destined to diversify, forcing defenders to consider even more varied vectors, infrastructures and capabilities than is true today.<sup>8</sup>

### ***Existing Frameworks***

At present, thinking about AI and cyber conflict is often not conducted within a well-established framework that effectively organizes and coordinates the work of researchers. Most work to date discusses the impact of AI on cyber operations and digital insecurity in one of two fashions: (1) via the lens of AI subordinate technologies, or (2) by examining the tactical, operational and strategic impacts of cyber conflict.

In the first case, AI-driven threats are in line with the various technologies and sub-disciplinary areas that define the AI field itself (including robotics,<sup>9</sup> machine learning,<sup>10</sup> deep reasoning,<sup>11</sup> natural language processing (NLP)<sup>12</sup> and Big Data, among others). In this vein are

numerous studies that focus on technical developments that are likely to impact cybersecurity challenges. For instance, some studies have centered on AI and malware, demonstrating the manner in which enhanced capacity for attack surface analysis and toolkit selection can produce automated capabilities that exceed those developed and employed by human hackers. Work on the application of generative adversarial networks (GANs) has contributed to both the cyber conflict studies and broader digital security fields in demonstrating the use of adversarial learning techniques for activities as distinct as deepfake deployment (for social engineering purposes, for instance) to on-the-go malware upgrading. Other work has described the way enhanced facial recognition software has enabled identification employing unmanned platforms, a capacity that has clear potential applications for social engineering and other cyber-related activities. While these types of explorations are often interesting and frequently compelling, linking their findings and suggestions to the broader national security mission that is interested in modeling the holistic transformative effects of AI on cybersecurity and digital insecurity can be challenging.

In the second case, the framework defaults to conventional levels of analysis to the study of AI in cyber conflict. The (1) tactical, (2) operational and (3) strategic levels of security operation are especially common frameworks employed by researchers as they provide a more holistic analysis of the scope of the issue area.

The tactical level of analysis draws a line around the most direct forms of inter-adversary engagement. A lynchpin of these analyses is the argument that adaptivity produces new defensive challenges.<sup>13</sup> Malicious code written by AI demonstrate these concerns. Such code might equate to a capacity for selecting specific techniques without human input, which generally implies that the sophistication of malware at the baseline may be destined to rise.<sup>14</sup> Such code could also have the capacity for selecting strategies, some of which could deviate from human goals and objectives. This is different from simple technique selection in which a target is pre-selected by an operator and the minutia of the method is machine-determined.<sup>15</sup> As an example, AI-augmented malware might be able to update its understanding of the value of targeted information, infrastructure or network spaces on the fly. “Incoming data obtained via infection of machines,” may enable malicious programming “to probabilistically judge where and when further infection is likely to lead to some value return.”<sup>16</sup> This portends to help remedy a core limitation of offensive cyber operations (OCO) planning, namely that persistent cyber engagement demands immense commitment of operational resources that is often either unavailable or requiring of time to compile.<sup>17</sup>

The operational level of analysis encompasses human activities above the tactical space where direct engagement occurs. Here, AI stands to make the production of extremely robust techno-organizational and techno-political maps of both red and grey spaces increasingly possible.<sup>18</sup> As one analysis puts it, “the more information made available to competent cybersecurity stakeholders, the more capable the infrastructure and tools developed for preventing

malicious cyber activity are likely to be.”<sup>19</sup> For the defensive mission, the implications here are that (1) the already immense variety of tools produced by both criminal and legitimate cybersecurity endeavors will exponentially diversify,<sup>20</sup> and (2) benefits will increasingly come from indirect targeting (“i.e. access gained via indirect targeting of associated institutions, users or architecture”).<sup>21</sup>

Finally, the strategic level of analysis considers the impact of AI on the dynamics of global cyber conflict wherein it shapes the utility of digital instruments for projecting social, political or economic power. This is where many initial analyses also have the least specificity. Furthermore, the cumulative effect of tactical and operational analyses of AI’s impact strongly implies the “bigger, faster, better, smarter” conclusion<sup>22</sup> that the tempo of cyber engagement in international affairs is set to increase, perhaps exponentially.<sup>23</sup> This is also where discussions of the value of AI systems are often thrown, despite evidence that suggests significant advantages as a result of employing these technologies. Malicious actors may target AI development processes in several different ways, including through input attacks designed to mislead data collection so that algorithms are mis-trained or poisoning attacks that actively alter existing data or models to the same end.<sup>24</sup> Here, perhaps the most important takeaway for the strategic assessment is the idea that AI portends a further turn towards subversion as a key characteristic of cyber conflict, with the interference of AI development systems and the potential reevaluation of strategies. These could combine to make AI more valuable for increasing the volume and tempo of cyber activities in the future.<sup>25</sup>

### ***The Need for Frameworks Devoid of Subjective Assumption***

Early in their development, emergent fields of study require conceptual models and empirical statements that deal in common characteristics and eschew subjective conclusions. In this way, core statements about the interaction of relevant forces can be constructed, tested and established.<sup>26</sup>

Contrasting this approach to building knowledge in a new field, much of the early analysis on AI and cyber operations has remained highly technical (thus, preventing the assertion of general principles) or has centered on broad descriptions regarding the character of the technologies based on use cases such as warfighting or crime. This makes sense for AI from the practitioner standpoint—after all, as is often the case with emergent technological areas, the numerous stakeholders seek to ground their AI and cyber operations within a contemporary strategic context. However, this makes it challenging to break away from the prevailing narratives about AI and national security in order to proffer analysis that links more clearly to the evolving fundamentals of national power and strategy.

Cybersecurity experts may find this tendency somewhat familiar, as the growth of the cyber conflict field has suffered from similar dynamics. This is particularly true in the early stages of development where narrow discussion of cyber tools, actors and phenomena has often

been linked to such broad narratives as the threat of “cyberwar”<sup>27</sup> or the rise of “liberation technologies.”<sup>28</sup> At times, these original notions about the coming impact of a new technology are often found to have been inaccurate or incomplete in hindsight. And, of course, quite worryingly, such notions often organize and drive fields of study, preventing the emergence of new security concepts. Thus, there is great value in attempting to construct appropriate analytic typologies – meaning, those that avoid subjective categorizations and unfalsifiable assumptions – as early as possible in that research and development process so that artificially limiting the view of researchers, practitioners and technologists can be avoided and potentially lead to better security instrumentation in a world rapidly augmented by AI.

## **A FRAMEWORK OF ARTIFICIAL INTELLIGENCE IN CYBER CONFLICT**

An important initial step in considering the impact of AI on cyber conflict is the development of a framework describing the different manners of interaction between the two areas of technology development and function (which are, admittedly, multi-faceted and overlapping) in question. Such an approach to thinking about the interactions of artificial intelligence technologies and web technologies must encapsulate the independent effects on contemporary society of each. In thinking about the future dynamics of cyber conflict, this means accommodating a holistic perspective on AI as a transformative influence on society alongside an objective view of how AI will alter the contours of cyber processes that have already become baked into the core functions of global society.

Here, I propose a four-part framework that envisions cyber conflict dynamics in which interaction (1) employs AI, (2) is conducted against AI, (3) is undertaken entirely by AI, and (4) is shaped and attenuated by AI.

### ***Cyber Conflict Using AI***

Cyber conflict using AI reflects the most common image of AI as a transformative element of security processes for most commentators. Simply put, AI applications and tools have the potential to upgrade or augment the potential of existing cyber threats along several lines.<sup>29</sup>

As has already been alluded, malicious actors could turn to AI to improve the efficacy of malware and cyber defenders may use AI to generate faster response times and actionable analytics on incipient threats. In both cases, it is perhaps best to describe this novel capability brought about by the use of AI tools as a capacity for analyzing the attack surface of a targeted infrastructure at greatly enhanced scale and speed.<sup>30</sup> Malware might be utilized, for instance, to forecast when and where compromise might be best targeted in order to achieve either tactical or strategic gains. As an example, Trickbot—perhaps the most commonly discussed example of malware with a variable selection dimension to date—is a good example of such a capacity.<sup>31</sup> While malware functions quite similarly to contemporary examples of code at the point of initial compromise, its actions are not easy to predict once a beachhead has been established.



Instead, the targets of further compromise are selected without clear reference – at least, without analysis of the malware itself – to a static ruleset. The code attacks the defender’s infrastructure at great speed and employs a pre-programmed intelligence analysis and selection routine that mimics the functionality of AI techniques currently being developed.<sup>32</sup> This kind of tool portends significant challenges for cyber defenders that perennially rely on predictive capabilities anchored on historical patterns to maintain systems integrity. Defenders are increasingly turning to machine learning to develop counters,<sup>33</sup> but it’s easy to see how the adversarial nature of evolving smart AI tools will confound defender efforts and prove a persistent problem for security administrators.

Added to this enhanced capacity to understand attack surfaces is the evolution of AI programming that shifts between techniques and tactics to successfully perpetrate a targeted compromise.<sup>34</sup> Malware developed along such lines by researchers has already demonstrated propensity for not only selecting appropriate techniques based on environmental analyses, but also for altering the tempo and scope of an intrusion underway in response to defender actions. Generative adversarial networks (GANs), for instance, have already been utilized to rapidly develop new malware versions that are more likely to bypass antivirus scanners<sup>35</sup> In perhaps more worrying examples, machine learning applications have been employed to be capable of rapidly reconnoitering a target’s digital presence and then generating thousands of social engineering hooks tailored to dozens of different categories of social media profile.<sup>36</sup>

In more limited demonstrations, these efforts have included the use of deepfake media and text content that is so high quality that it achieved incredibly high rates of successful phishing returns.<sup>37</sup> Such features of malware are not uncommon as characteristics of advanced persistent threat (APT) tools have been seen in the wild for at least twenty years. These APT tools also facilitate offensive adaptability via the use of off-the-shelf malware which suggests immense defender-side challenges, particularly as building and procuring such tools gets more economical.

Perhaps the most notable real-world example of AI systems that might augment cyber operations capabilities along the lines described above is an impressive new white hat hacking tool called Mayhem. Mayhem is an incredibly powerful computing engine that combines contrasting statistical analysis methods to find software vulnerabilities at great speed and scale.<sup>38</sup> Developed at Carnegie Mellon, Mayhem leveraged its AI capabilities in internal testing to find software vulnerabilities at an extreme rate. What was most impressive, however, was that almost 2% of vulnerabilities found were zero-day exploits, although they were assessed to not be particularly useful ones. In the Cyber Grand Challenge hacking competition hosted by DARPA, Mayhem won by more than double the points scored by the next human expert competitor, despite having crashed less than halfway into the event. While Mayhem is intended as a white hat tool, it’s easy to see how such capacity leveraged for malicious use could prove to be an extreme threat and a transformative element for future cyber conflict.

AI provides other benefits in a cyber conflict. For example, the use of AI behind the scenes of cyber operations to plan tactical engagements or reconcile empirical realities with strategic imperatives delineated above the operational level also contribute to the evolution of cyber conflict dynamics. Recent research has pivoted on this point in applying experimental methods to understanding how decision-makers might react to different forms of AI-driven intelligence conducting planning for cyber operations.<sup>39</sup> Clearly, stakeholders in the cyber conflict decision-making loop – including operators, managers and policymakers – consider such reliance on AI to furnish and upgrade cyber conflict engagement to be something that needs to factor into threat intelligence activities and planning. Thus, while there may be a difference to be found in AI systems employed by national security apparatuses for non-operational tasks and analysis (discussed below), it is clear cyber conflict action is not impacted by AI solely at the level of code, but also by direct intervention of new tools and processes at the operational level.

### *Cyber Conflict Against AI*

The race to develop enhanced cyber capacities based around new AI instrumentation should not only be considered in terms of incremental advances in the abilities of attackers and defenders. For defenders, in particular, additional challenges are to be found in the need to defend against cyber artificial intelligence attacks (CAIA)<sup>40</sup> in which malicious attackers attempt to subvert and manipulate the functionality of new AI processes.<sup>41</sup> CAIA involves directed targeting AI processes that will increasingly come to underwrite the processes and fundamentals of cyber conflict—such activity might occur in the real world, as conventional intelligence assets are used to interfere with the operation of national cyber-fighting institutions or the cybersecurity setup of private organizations. But the fact that cyberspace is the primary avenue via which so much AI functionality could be realized dictates that cyber conflict actions taken *against* AI are likely to be substantial and to include new categories of cyber conflict behavior (focused on counter-AI actions).

One type of CAIA is the input attack, in which adversaries deceive the AI systems’ approach to classification of behavioral patterns.<sup>42</sup> The logic behind such attacks is straightforward – there are opportunities for advantageous action in future conflict situations if the expectations of models produced by learning AI systems can be misled in the present. The idea is not to attack the code of AI tools itself, but rather to influence the information being fed into a learner so that that system’s view of the world is either slightly or substantially divergent from reality.<sup>43</sup>

Many of these actions can be taken outside of cyberspace. Researchers and security practitioners have notably used mirrors, stickers, and other physical objects to trick AI systems in vehicles and sensors and alter their response to environmental stimuli.<sup>44</sup> This, however, does not entirely separate such actions from the purview of cybersecurity practitioners and decision-makers. After all, kinetic enabling actions undertaken via human intelligence (HUMINT) operations or military force have often played a role in for amplifying the effect of

cyber or information operations. Kinetic attacks on Iraqi telecommunications infrastructure during the First Gulf War, for instance, forced Saddam Hussein's forces to resort to hackable methods of communications open to compromise by Western intelligence forces. Likewise, sophisticated cyber-attacks – from Stuxnet to the various employments of the BlackEnergy malware – have likely relied on black baggers and other intelligence assets to facilitate the use of cyber instruments. And of course, the opportunities to manipulate sources of AI system inputs via the Internet are also immense, particularly given the surprising volumes of data used to train machine learning algorithms that are publicly accessible on repository sites like GitHub. Using these resources, an attacker might track how adversary AI systems are being trained and adapt their behavior to encourage erroneous conclusions or could employ malware to bait defender systems into an expected response pattern before proceeding along completely different tactical lines.

Of course, the many publicly accessible resources often used to train AI models might also be directly altered via hacking. This would be an example of a poisoning attack,<sup>45</sup> the other side of the CAIA coin. Poisoning the fundamentals of AI systems is an appealing outcome for many prospective malicious cyber actors, just as it might be for Western intelligence and military forces. Poisoning achieves a similar outcome to input attacks, namely “the manipulation of data that such [AI] systems are trained on so that the model learned by the target system does not accurately reflect reality.”<sup>46</sup> Unlike input attacks, however, the idea is typically not just to skew the worldview of the model in question but prospectively to train the target towards a favorable behavioral outcome. A system may be tailored to fail at some particular juncture or when it encounters a particular pattern of activity that would be known to the original attacker.

One notable example of such an attack type leading to intrusion occurred in a laboratory setting and was presented at the 2021 HITCon security conference in Taipei. Researchers showed that it would be possible to inject a back door into the defensive model employed by a competent cyber high bender at the training stage by poisoning a shockingly small amount of the training data. By altering only 0.7% of training data, the research team produced notable vulnerabilities in the machine learning model being used to buttress a fictitious organization's cyber defenses, thus showing that remarkably little malicious data is needed to bypass some security systems.<sup>47</sup>

Expectedly, defenses against poisoning are already being developed by defensively-minded researchers.<sup>48</sup> Running special checks on training data to make sure that labels are accurate, for instance, is one such defense. However, this kind of task gets costly and time-consuming to manage at scale and is not an option for those who are buying their security products rather than developing them. Likewise, the standard of secondary verification rises inverse to the volume of malicious data required to create compromise.<sup>49</sup> If the HITCon research presentation example is anything to go on, this means that the standard of reliability is extremely high.

Beyond defensive options, challenges in effectively conducting poisoning attacks towards particular effects should be considered. A clear issue with contemporary AI – at least that which is reliant on deep learning methods – is in the explainability of outcomes from a given model. Biases present in data can come in a variety of forms and can lead to AI systems that have substantially accurate reads across the domain they are focused on while also having the potential for arriving at occasionally inexplicable outcomes. Lack of data at sufficient scale can also produce such outcomes and the AlphaGo outcome<sup>50</sup> – only works for conditions with strict rulesets, like a game of AlphaGo. Added to this opportunity for bizarre, deviant outcomes is the black box challenge wherein machine learning systems are challenging or impossible to view in terms of their inner workings. While white boxing – the task of making AI that both works as intended and can be interpreted mechanically by human users – is possible, it’s a difficult task and one that could compromise the power of AI systems in some cases. Thus, the opportunity for deviant outcomes and no way to explain them poses as much a challenge for attackers as for users. Simply put, what should poison look like in order to achieve particular malicious outcomes?

This dimension of future AI-infused cyber conflict seems destined to be of substantial and persistent concern going forward. Specifically, low-level threat actors may simply see value in disruption of AI systems and persistent, dedicated attackers may take extreme steps to achieve exact results, such as simulating an AI system, building a poisoned training set and then using cyber attack to replace clean files. More broadly, defenders face many of the same challenges of defense at scale as contemporary cybersecurity.

### *Cyber Conflict by AI*

In the past half decade, we have seen a great number of examples of autonomous agents bringing about unforeseen circumstances.<sup>51</sup> In the criminal world, both researchers and less scrupulous actors have created software with the ability to autonomously make decisions in new and changing environments. As Hayward and Maas describe,<sup>52</sup> a group of artists created one such agent in 2015 in the form of a shopping bot that subsequently analyzed several online sales environments, decided to purchase narcotics and was subsequently interdicted by Swiss law enforcement authorities.<sup>53</sup> This threat of abnormal behavior conducted online by entirely autonomous decision agents has become so pronounced that some researchers and legal professionals have already argued that certain AI systems may already be approaching the definition of legal personhood or achieving sentience.<sup>54</sup> This distinction reflects two practical realities. First, that AI systems have agency that is both functionally independent from those of human operators. Second, they are not readily recognizable in their actions simply via a review of some ruleset (i.e. how a hacker has written a program to respond to different environmental stimuli or commands).

Microsoft's chief scientific officer, Eric Horvitz, made a set of statements in 2021 emphasizing the degree to which AI-driven attacks are a grave concern even today. He stated that "[t]he value of harnessing AI in cybersecurity applications is becoming increasingly clear. Amongst many capabilities, AI technologies can provide automated interpretation of signals generated during attacks, effective threat incident prioritization, and adaptive responses to address the speed and scale of adversarial actions. The methods show great promise for swiftly analyzing and correlating patterns across billions of data points to track down a wide variety of cyber threats of the order of seconds."<sup>55</sup> And while AI also promises some ability to scale defensive efforts, particularly in light of cybersecurity workforce shortages, the application of AI to all elements of sophisticated cyber campaigns – such as disinformation and phishing activities, which could rely on AI decision-making in the most sophisticated cases – makes the association of AI and offensive operations the more worrisome prospect by far.

Beyond cybersecurity, the reality of AI systems as autonomous agents in global cyber conflict is quite worrisome. The strategic utility of actions taken via cyberspace is quite arguably anchored on the assertion that attribution of intent and political agency is remarkably difficult.<sup>56</sup> Attacks should be extremely specific in their timing and targeting in order to convey particular messaging.<sup>57</sup> Even then, the chances that basic actions might be considered a prelude or element of some more severe attack vis-à-vis a more common and expected manifestation of persistent engagement in the domain is reasonably high. Said another way, an AI system could make decisions and conduct operations that are outside the bounds of what human decisionmakers would prefer and even lead to unwanted and uncontrollable escalation. And this dynamic is exacerbated by dynamics of institutional culture, strategic context and individual cognition, each of which has increasingly received immense scrutiny as determinants of cyber conflict activity by scholars in recent years.<sup>58</sup>

Autonomous agents that operate according to rulesets that are learned in unsupervised processes and are evolvable may behave in an unexpected fashion. Even where backstops in AI systems function as a sort of kill switch to prevent undesired runaway behavior, it seems entirely possible that interacting agents might rapidly create new insecurities and conflict spirals in spite of their designer's intentions (even assuming a degree of expected self-autonomy from the model).<sup>59</sup> If such agents are not only allowed to operate in support of cyber operations or defense, but also with attacking AI systems merely accessible by cyberspace, the potential for such spiraling events climbs yet further. An oft-cited example of such runaway behavior is the 2010 "flash crash" of the Dow Jones in which over 1,000 points were lost in just 36 minutes due to automated selling programs that reacted first to odd events in the market and then to the reactions of one another.<sup>60</sup> Though losses were quickly recouped, \$1 trillion disappeared as a result of autonomous agent activity without human intervention in an incredible short period of time. Clearly, opportunities for perverse outcomes and even cascade effects exist with the case of independent autonomous agent activities. These

unintended consequences extend beyond – but can have similarly disruptive impacts as – the simpler utilization of AI by cyber stakeholders or focus on AI by hackers outlined in the previous two sections.

### ***Cyber Conflict Shaped by AI***

Finally, artificial intelligence systems will quite naturally redistribute value – economic, political, social, security – throughout society in years to come. AI will also create new sources of value. More realistically – at least in the near term – the ongoing growth of the Internet of Things (IoT), the automation of global finance and other beneficiaries of AI developments all portend a shift in the fundamentals of national economies, social function and political participation. The information revolution itself has dictated the shifting character of foreign interference efforts, organized crime and more to emphasize specific types of infrastructure, sources of data, etc. In similar fashion, the AI revolution will likely shift the ticker yet further and drive new patterns of digital engagement. Perhaps the battlefield of the future will be dominated by military personnel equipped with advanced brain-machine interface (BMI) technologies that enable unprecedented efficiencies in maneuver, resource coordination and more.<sup>61</sup>

This category of future cyber conflict shaped by artificial intelligence is, in some ways, the hardest to envision. It might be tempting to think that cyber conflict shaped by AI in this way is synonymous with CAIA itself, as to some degree, the two do overlap. However, it is not just focusing on hacking AI systems, data, procedures, or development/operational cycles that will determine such future cyber aggression. It is also the institutional, material and social value that those things shape that will determine such patterns. After all, global cybercrime developed via reference to the tenets of digital platform capitalism has been a focus of researchers and security practitioners for years.<sup>62</sup> Simply put, malicious behavior follows the enriching effects of new technology just as much as it is shaped by the characteristics of technology itself. Just as the printing press redefined international conflict around societal advances in culture, education, and religion, so too will much future conflict be shaped by the transformations of society caused by AI.<sup>63</sup>

## **ASSUMING AN INCOMPLETE MAP OF DIGITAL INSECURITY**

Planning for future cyber conflict will not be a simple matter. Cyber conflict in the age of AI and other transformative web technologies implies far more than augmentation of what exists today. Rather, cyber conflict will morph to reflect novel evolutions in the value landscape of global society, economics and international security, driven by both human and – possibly – machine agency. This point is critical given the state of thinking and formal mission-setting on the part of the United States government and that of our partners. Many attempts have sought to define future AI and cyberspace within the context of basic cybersecurity practices. Several noteworthy reports<sup>64</sup> nested in this subspace of broader discussion about AI in national security, for instance, anchor their analysis in the traditional framework of incremental



improvements for defenders and attackers. They articulate both challenges and opportunities associated with the deep learning used in developing AI systems. These range from concerns about explainability and transparency issues to the upsides of relying on machine learning for identifying and addressing the innumerable exploits that human checkers are inherently disadvantaged at finding in software products. However, they do so without considering the simultaneous transformation in the context of AI's role in global cyber conflict.

For strategic planners and policymakers, the most critical step to be taken in forecasting future digital insecurity amidst so much techno-strategic ambiguity is to simply be clear today about the issues. This means identifying those that cannot or will not be easily addressed by existing authorities; whether normative, institutional, legal or political. As AI's impact on cyber futures are considered, war-gamed and negotiated, emphasis needs to be placed on understanding where they might fall outside of current conceptualizations of digital security. The Western experience with cyber-enabled political interference beginning in the 2010s provides examples of the pitfalls in assuming that existing structures constitute sufficient perspective to address all likely security developments.<sup>65</sup> Organized around the idea of the cyber "domain" concept as something distinct from foregoing notions of information operations or the more legalistic ideas of critical infrastructures protection, the institutions built from the late 2000s onwards – which include U.S. Cyber Command and elements of the Department of Homeland Security, in particular – were slow to react to foreign interference in democratic process via the targeting of discourse supported by major corporations. With AI, it is imperative that stakeholders recognize that connected technologies have produced novel challenges for national security which are likely to further evolve in the future.

## **CONCLUSION: THE NEED FOR A BETTER GLOSSARY OF DIGITAL CONFLICT**

Thinking effectively about emerging disruptive technologies like AI inevitably requires us to reconsider established assumptions about cyber conflict. Even the language involved in talking about these issues must evolve and become more dynamic. This means not only building better and more accessible techno-strategic dictionaries of relevant terminology. It also implies a substantial shift in the way in advanced technologies like AI are incorporated into the strategic, operational and tactical landscape. This would involve a recasting of conversation around these issues and away from simplistic techno-strategic imaginings – i.e., every individual development amounting to "bigger, faster, smarter, better" – to a more holistic effort to tie the implications of AI employed at scale to the evolving foundations of cyber conflict today.♥



## NOTES

1. Lawson, Sean. "Beyond cyber-doom: Assessing the limits of hypothetical scenarios in the framing of cyber-threats." *Journal of Information Technology & Politics* 10, no. 1 (2013): 86-103.
2. Gartzke, Erik. "The myth of cyberwar: bringing war in cyberspace back down to earth." *International Security* 38, no. 2 (2013): 41-73.
3. Jensen, Benjamin M., Christopher Whyte, and Scott Cuomo. "Algorithms at war: the promise, peril, and limits of artificial intelligence." *International Studies Review* 22, no. 3 (2020): 526-550.
4. For robust histories of the development of the AI field, see among others Nils J. Nilsson, *The Quest for Artificial Intelligence: A History of Ideas and Achievements* (New York: Cambridge University Press, 2010); and Herbert Simon, "Artificial Intelligence: An Empirical Science," *Artificial Intelligence* 77, no. 2 (1995): 95-127, <https://pdfs.semanticscholar.org/>.
5. See, for instance, Whyte, Christopher. "Poison, Persistence, and Cascade Effects." *Strategic Studies Quarterly* 14, no. 4 (2020): 18-46; Burton, Joe, and Simona R. Soare. "Understanding the strategic implications of the weaponization of artificial intelligence." In 2019 11th International Conference on Cyber Conflict (CyCon), vol. 900, 1-17, IEEE, 2019; and Davis, Zachary. "Artificial Intelligence on the Battlefield." *Prism* 8, no. 2 (2019): 114-131.
6. Whyte, Christopher, "Machine Expertise in the Loop: How Military Decision-Makers React to AI Intelligence Delivery in Crisis," in IEEE: Cyber Conflict, 14th International Conference (CyCon) Proceedings, May 2022.
7. Whyte (2020).
8. Ibid. Sharikov, Pavel. "Artificial intelligence, cyberattack, and nuclear weapons—A dangerous combination." *Bulletin of the Atomic Scientists* 74, no. 6 (2018): 368-373.
9. For instance, Rajan, Kanna, and Alessandro Saffiotti. "Towards a science of integrated AI and Robotics." *Artificial Intelligence* 247 (2017): 1-9.
10. Domingos, Pedro. *The master algorithm: How the quest for the ultimate learning machine will remake our world*. Basic Books, 2015.
11. Goodfellow, Ian, Yoshua Bengio, and Aaron Courville. *Deep learning*. MIT Press, 2016.
12. Chowdhary, KR1442. "Natural language processing." *Fundamentals of artificial intelligence* (2020): 603-649.
13. Whyte, Christopher. "Poison, Persistence, and Cascade Effects." *Strategic Studies Quarterly* 14, no. 4 (2020): 18-46.
14. Ibid, 24.
15. Ibid, 24-25.
16. Ibid, 24.
17. Whyte, Christopher, and Brian Mazanec. *Understanding cyber warfare: Politics, policy and strategy*. Routledge, 2018, Chapter 5.
18. Leenen, Louise, and Thomas Meyer. "Artificial intelligence and big data analytics in support of cyber defense." In *Research Anthology on Artificial Intelligence Applications in Security*, 1738-1753. IGI Global, 2021. Also see Jahankhani, Hamid, Stefan Kendzierskyj, Nishan Chelvachandran, and Jaime Ibarra, eds. *Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity*. Springer Nature, 2020.
19. Whyte, Christopher, "Machine Expertise in the Loop: How Military Decision-Makers React to AI Intelligence Delivery in Crisis," in IEEE: Cyber Conflict, 14th International Conference (CyCon) Proceedings, May 2022; also see Whyte (2020), 25-26.
20. Kantarcioglu, Murat, and Fahad Shaon. "Securing big data in the age of ai." In 2019 First IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), 218-220. IEEE, 2019.
21. Radanliev, Petar, David De Roure, Rob Walton, Max Van Kleek, Rafael Mantilla Montalvo, La'Treall Maddox, Omar Santos, Peter Burnap, and Eirini Anthi. "Artificial intelligence and machine learning in dynamic cyber risk analytics at the edge." *SN Applied Sciences* 2, no. 11 (2020): 1-8.
22. Whyte (2020).
23. Horowitz, Michael C. "Artificial intelligence, international competition, and the balance of power (May 2018)." *Texas National Security Review* (2018).
24. Comiter, Marcus. "Attacking artificial intelligence." Belfer Center Paper (2019): 2019-08. Also see Insua, David Rios, Roi Naveiro, Victor Gallego, and Jason Poulos. "Adversarial machine learning: Perspectives from adversarial risk analysis." *arXiv preprint arXiv:2003.03546*(2020); and Puthal, Deepak, and Saraju P. Mohanty. "Cybersecurity Issues in AI." *IEEE Consumer Electronics Magazine* (2021).

## NOTES

25. Whyte (2020), 26.
26. Kuhn, Thomas S. *The structure of scientific revolutions*. Vol. 111. University of Chicago Press: Chicago, 1970.
27. Arquilla, John, and David Ronfeldt. "Cyberwar is coming!" *Comparative Strategy* 12, no. 2 (1993): 141-165.
28. Diamond, Larry. "Liberation technology." *Journal of Democracy* 21, no. 3 (2010): 69-83.
29. Brundage, Miles, Shahar Avin, Jack Clark, Helen Toner, Peter Eckersley, Ben Garfinkel, Allan Dafoe et al. "The malicious use of artificial intelligence: Forecasting, prevention, and mitigation." *arXiv preprint arXiv:1802.07228* (2018).
30. Whyte, Christopher. "Problems of Poison: New Paradigms and" Agreed" Competition in the Era of AI-Enabled Cyber Operations." In 2020 12th International Conference on Cyber Conflict (CyCon), vol. 1300, 215-232. IEEE, 2020.
31. DarkTrace, *The Next Paradigm Shift: Cyber- Attacks, AI-Driven*, research white paper (San Francisco: DarkTrace, 2018), <https://www.oixio.ee/>.
32. Lior Keshet, "An Aggressive Launch: TrickBot Trojan Rises with Redirection Attacks in the UK," *Security Intelligence* (2016).
33. E.g. Leenen, Louise, and Thomas Meyer. "Artificial intelligence and big data analytics in support of cyber defense." In *Research Anthology on Artificial Intelligence Applications in Security*, 1738-1753. IGI Global, 2021.
34. Whyte (2020), 25.
35. Kolosnjaji, Bojan, Ambra Demontis, Battista Biggio, Davide Maiorca, Giorgio Giacinto, Claudia Eckert, and Fabio Roli. "Adversarial malware binaries: Evading deep learning for malware detection in executables." In 2018 26th European signal processing conference (EUSIPCO), 533-537. IEEE, 2018.
36. Bahnsen, Alejandro Correa, Ivan Torroledo, Luis David Camacho, and Sergio Villegas. "Deepphish: simulating malicious ai." In 2018 APWG symposium on electronic crime research (eCrime), 1-8. 2018.
37. de Rancourt-Raymond, Audrey, and Nadia Smaili. "The unethical use of deepfakes." *Journal of Financial Crime* 30, no. 4 (2023): 1066-1077.
38. Brumley, David. "Mayhem, the Machine That Finds Software Vulnerabilities, Then Patches Them." *IEEE Spectrum* (2019).
39. Whyte, Christopher. "Learning to trust Skynet: Interfacing with artificial intelligence in cyberspace." *Contemporary Security Policy* 44, no. 2 (2023): 308-344.
40. Whyte (2020), 26.
41. E.g. Kuppa, Aditya, and Nhien-An Le-Khac. "Black box attacks on explainable artificial intelligence (XAI) methods in cyber security." In 2020 International Joint Conference on Neural Networks (IJCNN), 1-8. IEEE, 2020.
42. Kuzlu, Murat, Corinne Fair, and Ozgur Guler. "Role of artificial intelligence in the Internet of Things (IoT) cybersecurity." *Discover Internet of things* 1, no. 1 (2021): 1-14.
43. Comiter, Marcus. "Attacking artificial intelligence." Belfer Center Paper (2019): 2019-08.
44. [https://keenlab.tencent.com/en/whitepapers/Experimental\\_Security\\_Research\\_of\\_Tesla\\_Autopilot.pdf](https://keenlab.tencent.com/en/whitepapers/Experimental_Security_Research_of_Tesla_Autopilot.pdf)
45. Comiter, Marcus. "Attacking artificial intelligence." Belfer Center Paper (2019): 2019-08.
46. Whyte (2020), 27.
47. S. Cheng and M. Tseng, "Analysis of invisible data poisoning backdoor attacks against malware classifiers", Proc. HIT-CON 2021 Taipei Taiwan, November 2021.
48. See, among others, Ali W. Shafahi et al., "Poison Frogs! Targeted Clean-Label Poisoning Attacks on Neural Networks," presented at the 32nd Conference on Neural Information Processing Systems (NIPS), Montréal, Canada, 2018, <https://arxiv.org/>; Pang Wei Koh, Jacob Steinhardt, and Percy Liang, "Stronger Data Poisoning Attacks Break Data Sanitization Defenses," arXiv preprint arXiv:1811.00741 (2018), <https://arxiv.org/>; and Matthew Jagielski et al., "Manipulating Machine Learning: Poisoning Attacks and Countermeasures for Regression Learning," in 2018 IEEE Symposium on Security and Privacy (SP) (New York: IEEE, 2018), 19-35, <https://arxiv.org/>.
49. Ibid.
50. The references the AlphaGo AI that beat world grandmasters without input data after simulating over 30 million games of Go to learn how best to play.
51. Hayward, Keith J., and Matthijs M. Maas. "Artificial intelligence and crime: A primer for criminologists." *Crime, Media, Culture* 17, no. 2 (2021): 209-233.
52. Ibid, 217.

## NOTES

53. Kasperkevic, Jana. "Swiss police release robot that bought ecstasy online." *The Guardian* 22 (2015): 2015.
54. Bayern, Shawn. "The implications of modern business–entity law for the regulation of autonomous systems." *European Journal of Risk Regulation* 7, no. 2 (2016): 297-309. Also see Williams, Rebecca. "Lords select committee, artificial intelligence committee, written evidence (AIC0206)." (2018).
55. <https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report>
56. See works like Mueller, Milton, Karl Grindal, Brenden Kuerbis, and Farzaneh Badiei. "Cyber attribution." *The Cyber Defense Review* 4, no. 1 (2019): 107-122; or Rid, Thomas, and Ben Buchanan. "Attributing cyber attacks." *Journal of Strategic Studies* 38, no. 1-2 (2015): 4-37, for instance.
57. This point is a core conversation piece in discourse on the validity of cyber deterrence strategies. See *inter alia* Fischer-keller, Michael P., and Richard J. Harknett. "Persistent engagement, agreed competition, and cyberspace interaction dynamics and escalation." *The Cyber Defense Review* (2019): 267-287; Healey, Jason, and Stuart Caudill. "Success of Persistent Engagement in Cyberspace." *Strategic Studies Quarterly* 14, no. 1 (2020): 9-15; and Healey, Jason. "The implications of persistent (and permanent) engagement in cyberspace." *Journal of Cybersecurity* 5, no. 1 (2019): tyz008.
58. See, for instance, Kari, Martti J., and Katri Pynnöniemi. "Theory of strategic culture: An analytical framework for Russian cyber threat perception." *Journal of Strategic Studies* (2019): 1-29; Adamsky, Dmitry. "From Moscow with coercion: Russian deterrence theory and strategic culture." *Journal of Strategic Studies* 41, no. 1-2 (2018): 33-60; Snider, Keren LG, Ryan Shandler, Shay Zandani, and Daphna Canetti. "Cyberattacks, cyber threats, and attitudes toward cybersecurity policies." *Journal of Cybersecurity* 7, no. 1 (2021): tyab019; Gomez, Miguel Alberto, and Christopher Whyte. "Cyber uncertainties: Observations from cross-national war games." In *Cyber Security Politics*, 111-127, Routledge, 2022; and Gomez, Miguel Alberto, and Christopher Whyte. "Breaking the myth of cyber doom: Securitization and normalization of novel threats." *International Studies Quarterly* 65, no. 4 (2021): 1137-1150.
59. Whyte (2020), 38.
60. Ibid, 38-39.
61. Silva, Gabriel A. "A new frontier: The convergence of nanotechnology, brain machine interfaces, and artificial intelligence." *Frontiers in neuroscience* (2018): 843.
62. Tzanetakis, Meropi, and Stefan A. Marx. "The Dark Side of Cryptomarkets: Towards a New Dialectic of Self-Exploitation Within Platform Capitalism." *Digital Transformations of Illicit Drug Markets* (2023): 141.
63. Anderson, Benedict. "Imagined communities: Reflections on the origin and spread of nationalism." In *The new social theory reader*, 282-288, Routledge, 2020.
64. For instance, the National Information Technology and Networking Research and Development (NITRD) Program's Artificial Intelligence Research and Development (R&D) and Cyber Security and Information Assurance Interagency Working Groups (IWG) 2019 workshop report, <https://www.nitrd.gov/pubs/AI-CS-Detailed-Technical-Workshop-Report-2020.pdf>.
65. For a primer on such campaigns, see Whyte, Christopher, A. Trevor Thrall, and Brian M. Mazanec, eds. *Information warfare in the age of cyber conflict*. Routledge, 2021.

# THE CYBER DEFENSE REVIEW

◆ PROFESSIONAL COMMENTARY ◆



# CISA – The Future of Cyber Weather Forecasting

---

Lieutenant Colonel John Childress

Cybersecurity is like the weather on a summer day; you can see out of your window—just like you can see into your network—but you can’t see the storm on the other side of the mountain without a network of stations reporting what they can see. This analogy could be useful in thinking about forecasting for cybersecurity. This approach to cybersecurity—developing a “cyber-weather forecaster”—would enable defenders to see, predict and deal with threats in the same way that the National Weather Service (NWS) forecast helps us decide whether to bring an umbrella or leave it at home. As CISA’s Joint Cyber Defense Collaborative (JCDC) matures, developing “cyber weather forecasters” would provide an important improvement in gaining visibility into our networks and conducting predictive analysis.<sup>1,2</sup>

CISA founded the Joint Cyber Defense Collaborative in 2019 to combine the “visibility, insight, and innovation of the private sector with the capabilities and authorities of the federal cyber ecosystem to collectively drive down cyber risk to the nation at scale.”<sup>3</sup> In 2021 alone, the JCDC and its 21 Alliance partners worked together on major issues including Log4Shell, Daxin and Russia-Ukraine.<sup>4,5</sup> These are major achievements and they represent major milestones; however the JCDC must dramatically improve to provide the U.S. with the tools necessary to deal with more than a fraction of the 847,376 attacks reported just to the FBI’s Internet Crime Complaint Center in 2021 alone.<sup>6,7</sup>

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



**John Childress** is an Army Lieutenant Colonel who has served in various capacities at U.S. Cyber Command, the Cybersecurity and Infrastructure Security Agency, the Department of Social Sciences at West Point, the Army staff and as a ground commander in Iraq and Afghanistan. LTC Childress currently teaches at the United States Naval Academy in the Departments of Political Science and Cyber Science.

### ***Why the JCDC Will Do for Cybersecurity What the NWS Does for the Weather***

The National Weather Service could point the way forward for maturing the JCDC. This opportunity exists as a result of the deep similarities between the missions and functions of the NWS and the JCDC. Both seek to provide a public good—weather forecasts and cyber defense insights—to empower public-private action on a truly national scale.

Both organizations go about their mission in similar ways by combining public and private data—the NWS gathers data from public satellites and private weather stations, and the JCDC gathers data network information from .gov and from private partners like Microsoft and Mandiant—to create comprehensive datasets.<sup>8</sup> Both organizations then use these datasets to develop insights for their public-private partners—weather forecasts from the NWS and threat trends from the JCDC—which serve as information source, trends and predictive analysis that can support their constituents in guiding preparedness and response actions.

Perhaps most importantly, both organizations seek symbiotic relationships with their private partners—the JCDC wants private cybersecurity companies to help disseminate and add value to its products in the same way that local weather forecasters partner with the NWS to distribute and supplement the weather forecast.

### ***Realizing the JCDC's Forecasting Potential***

The mature weather ecosystem—the NWS, public and private data sources, foreign weather services and a distribution system which includes the NWS website, the Weather Channel and local news stations—provide a fully-realized vision for a future cyber defense ecosystem.<sup>9</sup> The mature cyber defense ecosystem would include different actors—private cybersecurity firms, network operators, individual citizens, multinational



corporations, government agencies and foreign partners—operating for both their individual benefit and for the good of the nation as a whole.

To realize this vision, CISA should pay attention to four critical aspects of the weather ecosystem that enable forecasting to successfully function at a national scale. First and foremost, CISA should develop a prediction model that adds value to the data that the public-private partners provide. This requires having access to comprehensive cyber data. However, it also implies more than simply recycling cyber data. The ecosystem should be truly symbiotic with each data provider—such as a having access to the “forecast” so they can make decisions for themselves and something that can be used in the marketplace. A mature cyber defense ecosystem should also have cyber defense forecasts which enable private partners to both supply data and to benefit from a public good in the same way that the local television station both provides weather data and repackages, or supplements, the publicly available forecasts on their nightly newscast.

CISA’s cyber ecosystem should provide partners with a common framework for data exchange; in other words, data providers must know that CISA’s forecasting models depend upon a standardized set of data elements. In a mature cyber defense ecosystem, each stakeholder would know what relevant network data to provide and in what form. CISA’s system should be developed incorporating a variety of tools including zero-trust protocols, machine learning and AI-enabled systems to enable real-time, machine to machine, easy-to-use system for gathering data from public and private partners across the country.<sup>10</sup> CISA could then fuse that information with national assets owned by the U.S. government and with information from international partners.

Lastly, the development of cybersecurity ecosystem would require leadership, support and resources provided by the Federal Government to ensure the proper investments are provided to complement the private sector. This would likely include protocols for incorporating potentially sensitive, proprietary and classified data. A mature cyber defense ecosystem would also require the Federal government plan to provide such leadership, support and resources on a recurring basis, at least during the early years. This would be required to ensure a lasting national capacity for conducting cyber defense forecasting.

### ***The Critical “Programmatic Investments” to Create the Cyber “Forecaster” that We Need***

Cyber will need to be able to evolve over time to adapt to the new threats, ecosystem partner requirements, and the evolving environment. At the most obvious level, these forecasts will provide day-to-day information which will enable people to prioritize and allocate their cyber defense resources. Cyber defense companies would need to inform less sophisticated operators about the cyber forecasts and assist them in mitigating their risk; more sophisticated organizations and individuals would hire cyber defense companies to supplement the publicly available cyber forecasts.

However, these cyber forecasts would have long-term benefits which go beyond the day-to-day. Long-term cyber forecasts would assist regulators, insurers and organizations understand risk profiles and incentivize a proper response in the same way that the Federal Emergency Management Agency’s Flood Maps guide zoning, regulations and insurance rates.<sup>11</sup> When the cybersecurity ecosystem reaches maturity, then an insurance company would be able to set client rates against a known risk profile.

The second focus area which will help mature the cyber defense ecosystem is developing confidence and certainty about the data framework necessary to model the “weather in cyberspace.” In other words, a mature cyber defense ecosystem should allow all partners to understand which data elements are necessary to feed the cyber-weather forecast. The JCDC and its cybersecurity partners do not need to build this framework from scratch as it already operates security frameworks which provide a logical point of departure. Furthermore, a guiding framework would need a central governance authority to guide the evolution of the cyber-weather forecasting model. The National Institutes of Standards and Technology (NIST) would be the logical partner to help forge consensus around a framework.<sup>12</sup>

Thirdly, the Federal Government should build a real-time, simple, machine-readable system to receive and coordinate the public-private data necessary to build cyber forecasts. This system must be adaptable and expandable so that it can adjust to changing reporting technologies— over time this system could accept data from across the world. The Joint Collaborative Environment and other systems may provide this functionality and the technical tools may change over time.<sup>13,14</sup>

Lastly, the government must make the right investments and assist partners in developing their investment priorities. In cyberspace the equivalent to weather satellites and national observatories are the government’s telemetry from its own networks (.gov, .mil) and the insights from its intelligence community. In a sense, the governments .gov and .mil networks mirror thousands of individual weather stations placed at strategic points in the U.S. while the intelligence community provides the weather balloons that help identify the location of the jet stream.

Federal networks may not require major financial investments, as CISA has authority over the .gov and the intelligence community has a global mission to collect intelligence of this sort already. Instead, the government would likely do better to focus attention on creating fast, reliable processes for collecting, analyzing, and disseminating partner network and Intelligence Community (IC) data into the cyber forecasting model. The IC would also need to ensure that data sources and methods are protected. Inevitably, this may require some difficult decisions on whether to withhold important data which cannot be disclosed for national security reasons.

A practical example comes from the United Kingdom’s (UK) Government Communications Headquarters (GCHQ) public partnership with the National Cyber Security Centre (NCSC)—this is the UK equivalent of partnering the National Security Agency (NSA) with the JCDC.<sup>15</sup> In 2021, the NCSC and its partners “dismantled over 22,000 phishing campaigns hosted in UK IP space, linked to over 142,000, attacks.”<sup>16</sup>

The United States requires the ability to understand and anticipate the cyber “weather” in our nation’s cyber networks. The newly formed JCDC provides the opportunity—in concert with its cyber partners—to develop the national cyber forecasts of the future. This will be essential as we can be assured that cyber threats will not go away and that more needs to be done to develop a predictive capability.

These are exciting times in cybersecurity; cyber defenders certainly have adversaries worthy of their time. The next logical step in our national cyber defense is to develop a predictive capability that is up to the task.🛡️

## **DISCLAIMER**

The views expressed in this work are those of the author 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. CISA, 2020, “Homepage | CISA,” Cisa.gov. 2020, <https://www.cisa.gov/>.
2. “JCDC | CISA,” n.d. [www.cisa.gov/jcdc](https://www.cisa.gov/jcdc).
3. “CISA Expands the Joint Cyber Defense Collaborative to Include Industrial Control Systems Industry Expertise | CISA,” n.d., [www.cisa.gov](https://www.cisa.gov/news/2022/04/20/cisa-expands-joint-cyber-defense-collaborative-include-industrial-control-systems), accessed November 10, 2022, <https://www.cisa.gov/news/2022/04/20/cisa-expands-joint-cyber-defense-collaborative-include-industrial-control-systems>.
4. “JCDC | CISA,” n.d., [www.cisa.gov/jcdc](https://www.cisa.gov/jcdc).
5. Joint Cyber Defense Collaborative, 2022, Review of Changing the Cybersecurity Paradigm: A Unified Cyber Defense, February 2022, [https://www.cisa.gov/sites/default/files/publications/JCDC\\_Fact\\_Sheet.pdf](https://www.cisa.gov/sites/default/files/publications/JCDC_Fact_Sheet.pdf).
6. Internet Crime Complaint Center, 2021. Review of Internet Crime Report 2021. Internet Crime Complaint Center. Federal Bureau of Investigation. 2021, [https://www.ic3.gov/Media/PDF/AnnualReport/2021\\_IC3Report.pdf](https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf).
7. “Internet Crime Complaint Center (IC3) | Home Page,” n.d., [www.ic3.gov/](https://www.ic3.gov/).
8. Joint Cyber Defense Collaborative, 2022, Review of Changing the Cybersecurity Paradigm: A Unified Defense. Joint Cyber Defense Collaborative, Cybersecurity and Infrastructure Agency, March 2022, [https://www.cisa.gov/sites/default/files/publications/JCDC\\_Fact\\_Sheet.pdf](https://www.cisa.gov/sites/default/files/publications/JCDC_Fact_Sheet.pdf).
9. National Weather Service, 2018, “National Weather Service,” [Weather.gov](https://www.weather.gov/), 2018, <https://www.weather.gov/>.
10. U.S. Department of Commerce, NOAA. n.d., “Own a Weather Station? We Want Your Data!” [www.weather.gov](https://www.weather.gov/iln/cwop), <https://www.weather.gov/iln/cwop>.
11. “FEMA Flood Map Service Center | Welcome!” 2019, [Fema.gov](https://msc.fema.gov/portal/home), <https://msc.fema.gov/portal/home>.
12. paul.hernandez@nist.gov, 2016, “Cybersecurity,” NIST, June 30, 2016, <https://www.nist.gov/cybersecurity>.
13. @MarkCMontgomery, 2021, “Making the Joint Cyber Defense Collaborative Work” *Lawfare*, August 6, 2021, <https://www.lawfareblog.com/making-joint-cyber-defense-collaborative-work>.
14. “Daily News | InsideCyberSecurity.com,” n.d., [Insidecybersecurity.com](https://insidecybersecurity.com), accessed November 10, 2022, <https://insidecybersecurity.com/daily-news/cyber-solarium-leader-montgomery-cites-%E2%80%98joint-collaborative-environment%E2%80%99-key-piece>.
15. NCSC, 2019, “About the NCSC,” [ncsc.gov.uk](https://www.ncsc.gov.uk), 2019, <https://www.ncsc.gov.uk/section/about-ncsc/what-we-do>.
16. Phil Muncaster, 2019, “UK’s NCSC Hails Another Successful Year of Cyber Defense” *Infosecurity Magazine*, July 17, 2019, <https://www.infosecurity-magazine.com/news/ncsc-another-successful-year-cyber/>.

# THE CYBER DEFENSE REVIEW

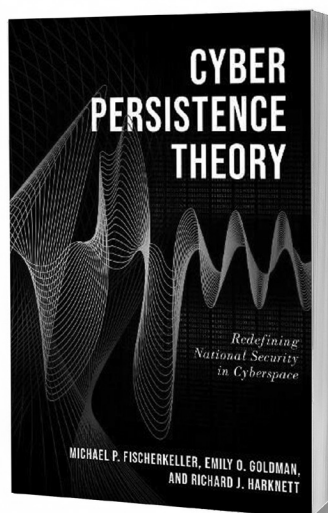
◆ BOOK REVIEW ◆



## Cyber Persistence Theory: Redefining National Security in Cyberspace

By Michael P. Fischerkeller,  
Emily O. Goldman,  
and Richard J. Harknett

Reviewed by  
Dr. Mark Grzegorzewski



### EXECUTIVE SUMMARY

*Cyber Persistence Theory* provides an important discussion of the structural shift in cyber strategy necessary for taking U.S. cybersecurity to the next level. No other work has made such a convincing case for this structural shift as the authors explain the current gap between cyber theory and observed cyber application. This alternative to the cyber deterrence paradigm provides an in-depth, academic analysis of the modern cyberspace environment. The main takeaway of this thesis is that cyberspace activity, especially exploitation, is the primarily form of strategic competition, and that exploitation should be interpreted as an alternative to war wherein states quickly capitalize on other state's cyberspace vulnerabilities rather than resorting to compellence. According to the authors, in cyberspace, states operate, at a low-cost, out of a structural need to persist and a strategic incentive to achieve short-term gains, without necessarily triggering an armed attack.

The book also emphasizes that the nature of cyberspace diminishes international cooperation, leading to a state of constant competition between countries. This structural feature, according to the authors, should encourage us to view cyberspace differently from the nuclear realm, while also emphasizing that strategic gains accumulate





Dr. Mark Grzegorzewski is an assistant professor of cybersecurity at Embry-Riddle Aeronautical University in the Security Studies and International Affairs Department. He is also an Army Cyber Institute Fellow. His recent publications include: “911? We Have an Emergency: Cyberattacks on Emergency Response Systems,” “In Search of Security: Understanding the Motives Behind Iran’s Cyber-Enabled Influence Campaigns,” and “Why the United States Must Win the Artificial Intelligence (AI) Race.” Dr. Grzegorzewski worked for over 11 years in the Department of Defense, seven of those years for U.S. Special Operations Command. He holds a Ph.D., M.A., and B.A. in Political Science/Government from the University of South Florida and a graduate certificate in Globalization Studies.

over time via successful tactical operations within campaigns. This suggests that by effectively conducting cyber operations, a state can enhance its relative power without resorting to traditional warfare.

## REVIEW

Martin Libicki’s “Cyberspace in Peace and War” (2nd edition) seminal work has been a must-read for anyone trying to understand the cyber domain and deterrence. However, in *Cyber Persistence Theory*, Fischerkeller, Goldman, and Harknett identify that, in practice, Libicki’s cyber deterrence formulation seems to be an imperfect fit for the future cyber strategic environment. In hindsight, the authors identify the cause of this mismatch as being obvious and rather simple: The U.S. government has been applying a 60-year-old nuclear deterrence paradigm to a completely unique strategic domain, cyberspace. In *Cyber Persistence Theory: Redefining National Security in Cyberspace*, the authors propose a new strategic concept for cyberspace that aligns closely with USCYBERCOM’s strategy of “Persistent Engagement.”

This alignment with USCYBERCOM’s strategy of “Persistent Engagement” is no coincidence, as the authors’ book serves as its unambiguous intellectual underpinning of the 2018 strategic-level strategy, which all had a hand in formulating. The authors possess impeccable credentials. Each of them has experience in strategy, cyber, and strategic studies. Fischerkeller is an Institute for Defense Analyses (IDA) researcher who has spent over 20 years supporting the Department of Defense (DoD). Goldman led the team that wrote the 2018 USCYBERCOM vision and currently serves as a USCYBERCOM strategist. And Harknett is the Director of the School of Public and International Affairs, Co-Director of the Ohio Cyber Range Institute, and Chair of the Center for Cyber Strategy and Policy

at the University of Cincinnati and was the inaugural USCYBERCOM Scholar-in-Residence. These authors' experiences complement each other well and add more to this compelling thesis together than either could do alone.

The book's initial focus is on this mismatch between cyber strategy and operations by examining previous literature, explaining how we got into our current predicament: We were too successful with our nuclear deterrence strategy. As the authors note, this presents a dilemma. Cyber strategy thinkers are boxed in by what they know and what was successful in the past. This causes cyber strategists to be anchored to the past, even though the old paradigm no longer quite fits and the old measures of success are no longer relevant. The authors conclude that in such circumstances, we must look for alternatives. In response to this imperfect fit, we've seen a new cyber paradigm emerge, at least within USCYBERCOM, "Persistent Engagement."

In developing the reasoning for the new persistent engagement paradigm, the authors advance the claim that there are three strategic domains, conventional, nuclear, and cyber, and that cyber is a domain of exploitation, unlike the conventional domain of conflict and the nuclear domain of coercion. As the authors assert, these three domains each have unique defining features. The conventional domain uses fighting and winning in war to achieve security conditioned by conflict. The nuclear domain uses the absence of war conditioned by offense dominance merely from the threat of use and a resulting no-win situation. The cyber domain presents an alternative, leading to war conditioned by competition.

In making this argument, the authors argue that the cyber strategic environment is novel since it is characterized by a dominant technology which poses unique challenges to international security. They further assert that the cyber domain has core exceptional features which make it mutable, interconnected, and macro-resilient while at the same time micro-vulnerable, due to an abundance of cyberspace vulnerabilities. Moreover, the constant contact is a permanent condition of cyberspace since all instruments of national power can engage other states and these states can engage right back due to the compression of space and time. The result is that in cyberspace, states are engaging each other constantly. This is in contrast to the conventional domain, where states also engage, yet their experience is episodic and characterized by having to cross physical space, or the nuclear domain whether the engagement tends to be more psychological by way of deterrence to have the intended effect.

The authors reason that in cyberspace, states are distinct entities like in the physical world, yet in the virtual domain states engage each other irrespective of physical geography. This condition impacts how states view their perception of security in cyberspace. The authors argue that states must persist in this virtual domain and achieve dominance by relentlessly engaging and taking advantage of adversaries' cyberspace vulnerabilities, while seeking to protect their own cyber networks, critical infrastructure, and national prerogatives as best

they can. In cyberspace, a vulnerability that is there one day, may be patched and closed-off the next. This is precisely why states must persistently engage and exploit opportunities in cyberspace. Clearly, the conceptualization of security in cyberspace is very different than that in the conventional domain.

To support these assertions, the authors employ the international relations concept of *fait accompli*. In cyberspace, a *fait accompli* is understood as a limited unilateral gain at a target's expense, where that gain is retained when the target chooses to relent rather than escalate in retaliation. The 2020 Russian Solar Winds hack provides such an example. The hack was treated, primarily, as an act of espionage, rather than an act of war, and the U.S. did not overtly respond in-kind to the Russian operation. The authors posit, this is often due to states learning about the intrusion long after it occurs. The logic is that since they have no recourse to get back what was stolen, they then have little incentive to respond long after the fact. While states could respond long after the fact, such actions could send a misguided signal to the adversary, thereby furthering misperceptions between the states and possibly destabilizing the environment. As a result, states often accept that a breach occurred and that a cyber incident impacted their information systems, and they reason that the intrusion likely does not warrant a response. As the authors note, ultimately by states not reacting to these incidents and thus accepting that adversary cyber exploitation will occur against them, they signal a tacit understanding and acceptance between states regarding cyberspace operations and activities.

In pressing this argument, *Cyber Persistence Theory* highlights that the world largely has not seen Russia, China, Iran, and North Korea holding targets at risk to destroy or disable in the event of hostilities, but rather taking advantage of cyberspace vulnerabilities they can exploit. An example is China's cyber economic espionage over the past 20 years. Individually, these actions might not appear connected, but taken as a whole, are indicative of a state-led campaign leading to strategic effects (i.e., growing Chinese economic dominance and diminishing American power). The authors assert these campaigns can achieve aims similar to war and can often lead to other strategic outcomes such as achieving economic aims. This description presents cyber as an "alternative to war" and highlights why the offense-defense rubric for cyberspace operations makes little sense in today's parlance and is unhelpful for discussions about cyber strategy.

Having laid the preparatory groundwork, the authors press the argument in support of their thesis. Cyber stability comes from the structure of the cyber domain that includes guardrails to constrain state behavior. These guardrails come in the form of tacit coordination and tacit bargaining. Tacit coordination arises when parties with common strategic interests align their actions implicitly without direct communication. Tacit bargaining involves informal agreements reached through actions and patterns, allowing both sides to perceive

and establish boundaries based on observed behaviors, fostering clarity, predictability, and stability. Ultimately, tacit coordination and bargaining produces mutually dependent actions, and regularity, in the cyberspace.

Given these theoretical underpinnings, cyber persistence theory was applied to the United States as a case study. The authors reiterate that the peace-war dichotomy did not work in cyberspace, and demonstrate that the moment a country pauses, they cede the operational initiative. An important outcome is that when this occurs, countries no longer hold targets at risk but rather are left to look for opportunities to what exploit cyber network insecurities when they find them. These instances demonstrated that the world was witnessing was not war, nor was it coercion. A new phenomenon had emerged that U.S. cyber strategy could not conceptually capture. This phenomenon reflected that adversarial countries were competing differently than the United States in cyberspace.

Realizing around 2013 that the Cold War nuclear deterrence paradigm had been misapplied and the “doctrine of restraint” had allowed offenders to operate without the consequence in U.S. networks, the United States needed a new approach. With this realization, the United States bought into the development of persistent engagement strategy in the cyber domain. The 2018 “defend forward” cyber strategy aimed to re-align U.S. cyber strategy with the cyber environment and provided the foundations for this new strategy. This strategy contains four pillars: (1) Defend the homeland by protecting networks, systems, functions, and data; (2) Promote American prosperity by nurturing a secure, thriving digital economy and fostering strong domestic innovation; (3) Preserve peace and security by strengthening the ability of the United States—in concert with allies and partners—to deter and, if necessary, punish those who use cyber tools for malicious purposes; and (4) Expand American influence abroad to extend the key tenets of an open, interoperable, reliable, and secure Internet. These pillars, particularly 1 and 4, incorporate aspects of persistent engagement, provide an alternative to the deterrence paradigm, and provide an alternative to war in achieving strategic outcomes.

## CONCLUSION

*Cyber Persistence Theory* makes an important contribution to and provides highly reasoned basis for understanding the evolution of U.S. cybersecurity strategy to “persistent engagement.” The lack of applicability of the deterrence paradigm to cyberspace was an open secret, and this work is an order of magnitude towards properly re-conceptualizing cyberspace operations in strategic studies. Using the familiar lexicon of international relations, this work both describes a more apt theory and prescribes a strategy that better aligns with the realities of cyberspace than traditional cyber deterrence.

While the authors properly note that cyberspace is primarily a space of exploitation, they leave open the possibility that it could deter in limited circumstances, in cases such as holding critical infrastructure at risk. They also note that there's a distinct secondary behavior observed, primarily among certain non-state actors. For instance, hacktivist groups often use distributed denial of service or DDOS attacks on government websites, aiming to coerce rather than merely exploit. For those actors, cyber deterrence is still an effective strategy, but it does not mean it cannot be complemented by cyber persistence.

Indeed, today, we still observe both strategies in play. Yet, as we navigate new strategic alternatives in cyberspace, there's an inherent reluctance to abandon previously effective strategies. Eventually, this profound paradigm shift will impact how we approach global cyber security.🛡️

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

Title:       ***Cyber Persistence Theory:  
Redefining National Security in Cyberspace***

Authors:   Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett

Publisher:  Oxford University Press

Paperback: 272 Pages

Price:       \$20.99 Paperback

              \$13.79 Kindle

# AVENGERCON

**AvengerCon VIII,**  
the 780th Military Intelligence (MI)  
Brigade's homegrown hacker con

**IS BACK &  
LOADED!**

A UNIQUE MULTI-OPTIONAL EXPERIENCE

- > **Presentations**
- > **Hacker Villages**
- > **Training Workshops**
- > **Additional Content provided by members of the AvengerCon community!**

AvengerCon welcomes



**U.S. ARMY  
CYBER COMMAND**

Open to all service members  
and employees of U.S. Cyber  
Command and Department of  
Defense personnel supporting  
cyberspace missions.

**We hope to see you there!**

**Visit [avengercon.org](https://avengercon.org)**

**February 28-29, 2024**

Georgia Cyber Innovation & Training Center  
Augusta, Georgia  
(or join remotely from anywhere!)



# THE CYBER DEFENSE REVIEW


CONTINUE THE CONVERSATION ONLINE

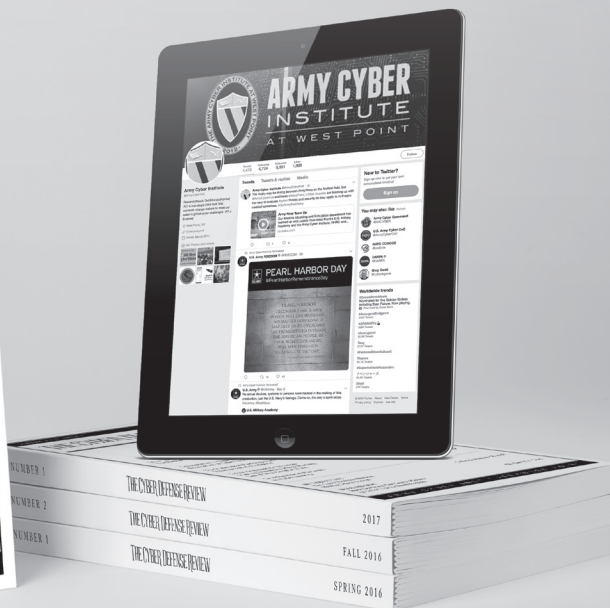
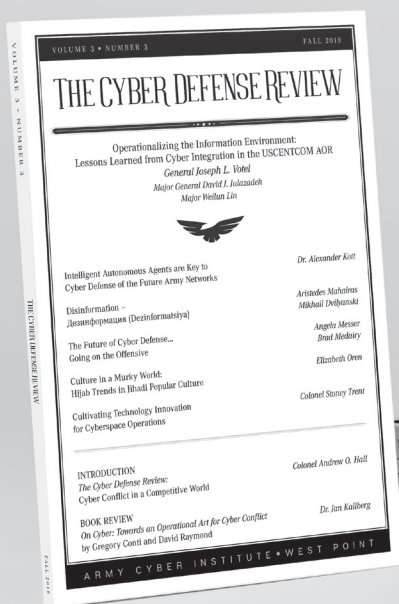
 [CyberDefenseReview.Army.mil](http://CyberDefenseReview.Army.mil)

AND THROUGH SOCIAL MEDIA

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

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

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



ARMY CYBER INSTITUTE ♦ WEST POINT PRESS







# 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.