VOLUME 5 ▪ NUMBER 3 FALL 2020

THE CYBER DEFENSE REVIEW

ARMY CYBER INSTITUTE ◆ WEST POINT

The Cyber Defense Review

Fall Edition

THE CYBER DEFENSE REVIEW

A DYNAMIC MULTIDISCIPLINARY DIALOGUE

CONTACT
Army Cyber Institute
Spellman Hall
2101 New South Post Road
West Point, New York 10996

SUBMISSIONS
The Cyber Defense Review
welcomes submissions at
mc04.manuscriptcentral.com/cyberdr

WEBSITE
cyberdefensereview.army.mil

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

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

INTRODUCTION

SENIOR LEADER PERSPECTIVE

PROFESSIONAL COMMENTARY

RESEARCH ARTICLES

RESEARCH ARTICLES

RESEARCH NOTES

BOOK REVIEW

The Cyber Defense Review

Introduction

VOL. 5 ◆ NO. 3

The Cyber Defense Review: Expanding the Cyber Discussion

Colonel Jeffrey M. Erickson

INTRODUCTION

Welcome to *The Cyber Defense Review* (CDR) Fall 2020 edition. As the new Director for the Army Cyber Institute (ACI), I am honored to be joining the CDR team and very excited about this most recent issue of the journal. The CDR plays a critical role in expanding the discussion within the cyber community, from tactical units to national leadership to industry partners to academia. The quality of articles from a diverse group of leaders and thinkers within the community, coupled with an extensive reach that includes foreign allies, partners, and international educational institutes, is a testament to the impact of this journal. The CDR is truly adding to the body of knowledge in the cyberspace domain.

Our Leadership Perspective portion provides unique perspectives with national impacts. Major General Robin Fontes (Deputy Command General (Operations), U.S. Army Cyber Command) and the ACI's Critical Infrastructure Team (Lieutenant Colonel Doug Fletcher, Lieutenant Colonel Erica Mitchell, Major Jason Hillman, Major Erik Korn, and Major Steven Whitham) address ways to increase the resiliency of public and private critical infrastructure through ACI's Jack Voltaic® project. Jack Voltaic®, which recently completed its third iteration involving the cities of Savannah, GA, and Charleston, SC, looked specifically at potential impacts on deploying forces as they utilize these key port cities.

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

We are honored to showcase two articles that tackle key issues from the Cyberspace Solarium Commission. The Honorable Patrick Murphy (former Under Secretary of the Army) and ACI's Dr. Erica Borghard discuss how the United States should adopt a whole-of-nation, defend forward strategy for information operations. From a legal perspective, the Honorable Joe Reeder (former Under Secretary of the Army) and ACI's Professor Rob Barnsby posit that the Cyberspace Solarium Commission may have broken through the public-private partnership roadblocks with respect to performing cybersecurity by reinforcing the necessity of a collaborative approach. The recommendations in both articles have a potential national-level impact on how the US organizes for success in the cyberspace domain.

Rick Howard (Chief Analyst, Chief Security Officer, and Senior Fellow at The CyberWire) and Ryan Olson (Vice President of Threat Intelligence for Palo Alto Networks) provide a Professional Commentary on the value of developing adversary playbooks as a framework to enable cyber defense and intelligence sharing. I think you will find their proposed approach moving beyond Lockheed Martin's white paper on Cyber (Intrusion) Kill Chain, an interesting solution.

Within our Research Articles, authors address a variety of topics to include a proposed operational framework, a look at the tendency to describe the complex cyber-threat environment through exaggerated terms, a method to analyze the ever-growing Smart City environment, and a proposed change to the Law of Armed Conflict concerning civilian data. First, Dr. Patrick Allen (Information Operations Specialist at the Johns Hopkins University Applied Physics Laboratory) articulates both the need and an approach for describing cyber maneuvers at the operational level. His article not only provides categories of maneuver, but also applicable examples that any maneuver commander could use to integrate cyber domain operations with more

conventional operations. Next, in "Beyond Hyperbole: The Evolving Subdiscipline of Cyber Conflict Studies," Dr. Aaron Brantley (Assistant Professor of Political Science at Virginia Tech and former Army Cyber Institute member) looks at scholarly works and argues for the need to move cyber conflict studies into the broader discipline of International Relations by shifting the discussion away from apocalyptic hyperbole to a focus on concrete, real-world examples.

Urban warfare has been a constant challenge for military forces. Considering the proliferation of Smart Cities, the increasing likelihood of future conflicts in these environments requires an understanding of the technologies and trends affecting the environment. Maxim Kovalsky (Senior Manager, Deloitte's Cyber Risk Advisory), Lieutenant Colonel Robert Ross (formerly ACI's Information Warfare Team Lead), and Greg Lindsay (non-resident fellow of the Atlantic Council) discuss the key trends in Smart Cities and propose a method for analyzing the ecosystems to inform intelligence preparation of the battlefield and enable military operations. Finally, the necessity to reclassify civilian data as an "object" is discussed in "Why the Laws of Armed Conflict Must Be Expanded to Cover Vital Civilian Data" by Colonel Beth Graboritz (Deputy Director, National Security Agency's Command, Control, Communications and Cyber Systems Directorate), Lieutenant Colonel James Morford (Deputy Director for Communications and Information at 7th Air Force), and Major Kelly Truax (Deputy Chief, Strategy and Policy Analysis Division, U.S. Transportation Command). This proposal would provide Laws of Armed Conflict protections for civilian data and allow for legal actions in response.

In the Research Notes section, First Lieutenant Hugh Harsono (Assistant Operations Officer in a Special Operations Task Force) discusses the challenges of digital threat financing, and the potential role Special Operations Forces could play in countering this growing challenge. Additionally, to address the current pandemic, Dr. Jan Kallberg, Dr. Rosemary Burk, and Dr. Bhavani Thuraisingham touch on some of the unknown second and third-order effects of the virus in "COVID-19: The Information Warfare Paradigm Shift." Looking ahead, we are accepting papers for a CDR COVID-19 themed issue in Spring 2021 related to the pandemic and the challenges related to cyberspace concerning security, technology, and policy. If you are interested in submitting a relevant article, please visit the CDR website for additional information: https://cyberdefensereview.army.mil/.

Finally, I would like to take a moment to recognize the departure of one of the ACI's team members, Dr. Erica Borghard. In her time with ACI, the impact of Erica's work has reached from the classroom to the halls of Congress. In addition to instructing at West Point, she served as a task force lead for the Cyberspace Solarium Commission, where she provided recommendations to the Nation's leadership on national policy and law related to cyberspace. She is departing to accept a position at the Atlantic Council, where she will continue to be a thought leader in the cyberspace realm. Good luck, Erica!

In conclusion, I am very honored to join *The Cyber Defense Review* team and excited about continuing the important dialogue with this august community. Let's move forward together!

The Cyber Defense Review

Senior Leader Perspective

To Defend Forward, US Cyber Strategy Demands a Cohesive Vision *for Information Operations*

The Honorable Patrick J. Murphy
Dr. Erica Borghard

INTRODUCTION

In 2018, the United States (US) Department of Defense (DoD) published the 2018 Cyber Strategy summary featuring a new strategic concept for the cyber domain: defend forward. It states DoD will, "defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict."[1] This reflects an important shift in DoD's strategic posture, compared to the 2015 Cyber Strategy, in two key ways.[2] First, defend forward rests on the premise that to deter and defeat adversary threats to national security, the US could not solely rely on responding to malicious behavior after the fact. Rather, the DoD should be proactive in maneuvering outside of US cyberspace to observe and understand evolving adversary organizations and, when authorized, conduct operations to disrupt, deny, or degrade their capabilities and infrastructure before they reach the intended targets. Implied, but not explicitly stated, in the 2018 strategy summary is the role of information operations, and the relationship between cyberspace and the information environment. According to US doctrine, the former is a subset of the latter.[3] This article builds on our work as members of the US Cyberspace Solarium Commission to offer a conceptual framework and policy recommendations for integrating information operations in the context of defend forward. Many of the Commission's 82 recommendations are slated to pass in the Fiscal Year 2021 National Defense Authorization Act (NDAA).

Although the field of information warfare and information operations is not new, there has been a recent resurgence in academic and practitioner interest within the US on the relationship between the information environment and cyberspace operations.[4]

The Honorable Patrick J. Murphy is America's first Iraq War veteran elected to the U.S. Congress and later served as the 32nd Under Secretary of the Army until January 2017. Secretary Murphy is currently a Senior Managing Director at Ankura, the Distinguished Chair of Innovation at the United States Military Academy at West Point, and a Commissioner on the U.S. Cyberspace Solarium Commission. Patrick serves as a director on several public and private-held companies and is a graduate of King's College Army ROTC Program and the Widener University Commonwealth School of Law. He has two young children, Maggie and Jack, and they reside in Pennsylvania.

In particular, Russia's use of cyber-enabled information operations to interfere in the 2016 US Presidential election, foment social strife, and undermine public faith in democratic institutions was a key event that shaped the framing of these more recent discussions.[5] Much of the conversation has rightly centered on (a) how the US can better defend itself and thwart such behavior in the future;[6] (b) concerns about how other adversaries and competitors, such as China,[7] may be taking a page out of Russian President Vladimir Putin's playbook; and (c) critiques of the US tendency—potentially stemming from differences in American and Russian strategic culture—to neglect the information environment. Arguably, the DoD is ahead of other departments and agencies within the Federal government and is best positioned in terms of resources, planning, and conceptualizing the optimal role of information operations in military strategy in general, and in cyberspace in particular.[8] For example, Army Cyber Command (ARCYBER) is pursuing an initiative to integrate information, electronic, and cyber warfare capabilities and has even considered changing the command's name to Army Information Warfare Operations Command.[9] Moreover, at the 2018 Cyberspace Strategy Symposium, U.S. Cyber Command (USCYBERCOM) grappled with the implications of "[s]ynchronizing and coordinating information-related capabilities together in a coherent strategy,...[to integrate] IO [information operations] and cyberspace capabilities."[10]

From a grand strategy perspective, it is imperative that the US considers how best to employ and integrate the full range of diplomacy, information, military, and economic instruments of power in furtherance of national objectives.[11] As to strategic objectives in cyberspace more specifically, the Fiscal Year 2019 NDAA established the Cyberspace Solarium Commission to develop a comprehensive strategy to defend the US against cyberattacks of significant consequences, as well as to promulgate a set of policies and legislation that would be required to implement the strategy.

Dr. Erica Borghard is a Senior Fellow in the Scowcroft Center's New American Engagement Initiative at the Atlantic Council. She is also a Senior Director on the Cyberspace Solarium Commission. Prior to that, Dr. Borghard was an Assistant Professor in the Army Cyber Institute. Previously, she was a Council on Foreign Relations International Affairs Fellow, with placement at JPMorgan Chase and U.S. Cyber Command. Dr. Borghard also served as an Assistant Professor and Executive Director of the Rupert H. Johnson Grand Strategy Program in the Department of Social Sciences at West Point. She received her Ph.D. in Political Science from Columbia University. Dr. Borghard has published in numerous academic journals and policy outlets on topics ranging from cyber policy to grand strategy. Dr. Borghard is a term member at the Council on Foreign Relations and a Research Fellow at the Saltzman Institute of War and Peace Studies at Columbia University.

Comprised of fourteen commissioners, including members of Congress, senior leaders in the executive branch, and subject matter experts from academia and the private sector, the Commission organized itself into three task forces to investigate distinct strategic approach for cyberspace—deterrence through active disruption and cost imposition; denial and resilience; and entanglement and norms—as well as a fourth directorate to explore cross-cutting issues. Following a rigorous research process that included interviews with subject-matter experts (SMEs), domestic and international engagements, a series of red team analyses, a multi-stakeholder simulation, and quantitative analysis, the Commission produced a report in March 2020 unveiling a novel strategic approach and recommendations.

Specifically, the Commission advocates for a strategy of layered cyber deterrence.[12] Rather than rejecting cyber deterrence, the Commission updates the concept for the modern era. Specifically, the Commission Report urges the US to adopt a whole-of-nation approach to deter malign behavior and cohesively leverage the full range of instruments of national power. Layered cyber deterrence also posits that the range of deterrence tools, such as promoting international norms to shape behavior, improving domestic defense and resilience, and imposing costs on adversaries for engaging in malicious behavior in cyberspace, have varying utilities in different strategic contexts against different types of threat actors. In particular, the Commission Report distinguishes between the deterrence challenges associated with preventing cyber-attacks above the level of war, versus those aimed at reducing the magnitude and frequency of malicious cyber campaigns below that threshold. Furthermore, defend forward is a key aspect of the Commission's strategy of layered cyber deterrence. The decision to feature defend forward as a core component of the Report's strategic approach reflects the Commission's mindset that the US should be more

proactive and biased toward action to address adversary threats in cyberspace.

Consistent with its statutory mandate, the Commission Report extensively addressed strategic challenges in cyberspace. However, one area with important implications for the cyber domain and for the implementation of the Commission's strategy and recommendations is the nexus of cyberspace and the information environment. Therefore, in this article we build on the Commission's strategy and recommendations to more fulsomely address how the US can improve its strategic approach in two respects as to the information domain.[13] First, the Commission Report makes the point that information operations should be incorporated into defend forward. Put simply, the US needs to be more proactive in thinking about the strategic employment of information operations. In this article, we lay out the strategic thinking that went behind this recommendation and explore how the US should conceptualize coupling cyber and information operations to shape adversary perceptions and, by extension, behavior, particularly below the level of armed conflict. More specifically, we provide a framework to guide strategic thought and policymaking on employing information operations as part of the defend forward strategy in cyberspace. Importantly, while the notion of being proactive—owning the narrative and deliberately using information for clearly defined purposes—is not inherently controversial, who "owns" this mission is not without controversy because there are many stakeholders with an interest in this space.

Second, this article also goes beyond the boundaries of the Commission's recommendations to urge that, in addition to incorporating information operations into defend forward, the US should consider developing a coherent approach to revitalizing the role of information as part of a national cyber strategy more broadly. While outside of the statutory scope of the Cyberspace Solarium Commission's mandate, this is a natural extension of the Commission's work and strategic vision. Therefore, we also explore how to extend the spirit of the Commission's recommendations to address ways the US can more strategically leverage information beyond the military instrument of power.

It is also important to note that the Commission's March 2020 Report delves into several recommendations to shore up domestic defenses against influence operations. Strengthening the ability of American society to better defend itself against adversary information operations is a critical task to preserve American democracy. Specific Commission Report recommendations that address this concern include advocating for programs that promote digital literacy, civics education, and public awareness at the societal level to inoculate the American public against foreign malign influence campaigns.[14] The Report also recommends defense of the US election system against adversary information operations, including improving the structure of and increasing resourcing for the Election Assistance Commission and promoting voter-verifiable, auditable, paper ballots.[15]

INCORPORATING INFORMATION OPERATIONS INTO DEFEND FORWARD

Beyond domestic defense, information operations also played an essential role in how the Commission addressed implementing the defend forward concept in cyberspace to favorably influence adversary behavior. The concept of defend forward was introduced in the 2018 DoD Cyber Strategy, which posits that DoD will "defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict."[16] It entails maneuvering where adversaries operate, sharing information with partners to enable their own defensive efforts, and, when authorized, delivering effects to disrupt, deny, and degrade adversary capabilities, infrastructure, and operations. Recognizing that defend forward is central to US cyber strategy, particularly in a context of strategic competition below the level of war, a key Cyberspace Solarium Commission recommendation is that the Executive Branch should issue an updated National Cyber Strategy to include defend forward as a key element.[17] Notably, the 2018 National Cyber Strategy lacks any reference to defend forward, even though this concept is the driving principle behind how DoD conceptualizes the nature of the strategic challenge in cyberspace, and how US military cyber forces should be organized and employed to counter adversary threats.[18]

Additionally, the Commission recommends that the defend forward concept should be expanded to encompass all of the instruments of national power—to include information as an instrument of power.[19] This concept is not explicitly discussed in the 2018 DoD Cyber Strategy summary or statements by leaders. Yet, the Commission recognized that the strategic employment of information is intertwined with conducting cyberspace operations to influence adversary decision-making and behavior.[20] Shaping behavior implicitly rests on affecting an adversary's perception of the strategic environment. Given this objective, integrating information operations into defend forward can assist in accomplishing the strategy's desired end state.

In Joint Publication 3-13, DoD defines information operations as "the integrated employment, during military operations, of IRCs [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."[21] The immediate locus of information operations is the mind of the adversary, although the ultimate objective is to manipulate adversary behavior in a desired direction. As Dr. Herbert Lin and Dr. Jaclyn Kerr describe, information warfare and influence operations entail "the deliberate use of information by one party on an adversary to confuse, mislead, and ultimately to influence the choices and decisions that the adversary makes."[22] Accordingly, "[t]he targets...are the adversary's perceptions, which reside in the cognitive dimension of the information environment," while the objective is to "[use] words and images to persuade, inform, mislead, and deceive so that the adversary does not use the (fully operational) military assets it does have, and the military outcome is the same as if those military assets had been destroyed."[23]

Importantly, we are not suggesting that the US government should replicate adversary campaigns that use cyberspace to conduct widespread disinformation against civilian populations.[24] To do so would be inconsistent with democratic values, especially when these types of campaigns take place outside of a context of active hostilities or conflict. Instead, we posit that *tailored* information operations conducted in conjunction with cyber operations against defined adversary military entities could enhance the effects of defend forward campaigns. Essentially, rather than conducting cyber-enabled information operations similar to those of US adversaries, in which disinformation is the objective and cyberspace is only one medium through which to achieve it, the US should consider how it could conduct "information-enabled cyber operations"—leveraging information to support the operational and strategic objectives of defend forward.

There are two notable examples of publicly disclosed efforts by the US to explore the nexus between cyber operations and the information space at the operational level. However, these have been almost wholly focused on employing cyber capabilities to disrupt adversary information activities—rather than integrating information into cyber capabilities for the purposes of shaping adversary behavior. The first, Operation GLOWING SYMPHONY in 2016, entailed countering the social media activities of the self-proclaimed Islamic State of Iraq and the Levant (ISIL).[25] In this example, cyber operations were reportedly used to undermine the adversary's ability to leverage social media to recruit, to spread propaganda, and for command and control purposes, specifically to "find and destroy the key nodes in ISIS online infrastructure and media operations."[26] Then-Deputy Secretary of Defense Robert Work described this effort as "dropping cyberbombs."[27] In the second example, in 2018 USCYBERCOM—replicating the task force model of the counter-ISIL campaign—worked with interagency partners to form the Russia Small Group. Among other measures, USCYBERCOM reportedly conducted cyber operations to disrupt adversary information operations targeting the 2018 midterm elections.[28] While these represent important efforts, the US should consider how it can move beyond cyber responses to adversary use of the information environment. Specifically, the US should improve its ability to incorporate information operations into cyber campaigns. This would require further maturation of thought about how to incorporate such operations into the defend forward strategic framework, and appropriate capabilities, authorities, and processes to enable its deliberate implementation at scale across multiple campaign plans.

STRATEGIC FRAMEWORK

Defend forward aims to address a central challenge for the US in cyberspace: how to change adversary behavior in cyberspace short of war to produce a more favorable status quo while mitigating potential escalation risks.[29] An improved status quo would be one in which the magnitude and effects of adversary campaigns targeting the US political system, critical infrastructure, and military capabilities are reduced. In the immediate term, defend forward

endeavors to do this by reducing the effectiveness and/or increasing the costs of adversary operations. Over time, the cumulative effect of defend forward operations and campaigns, in theory, is hypothesized to shift the adversary's perception of the environment; assessments of the relative costs, benefits, and risks of conducting malicious campaigns; and calculations about the likelihood of success, ultimately driving adversaries to divert resources to other efforts and reduce undesirable activities.

Conducting cyber operations to disrupt, deny, and degrade adversary operations and campaigns (which include, for example, their offensive cyber capabilities, infrastructure, and command and control) is a centerpiece of defend forward.[30] As a form of denial, these operations are directed at adversary offensive capabilities and strategies, and not at the broader civilian population.[31] However, given that the purpose of these operations is to affect an adversary's decision calculus, there is an opportunity for information operations—which, by definition, are directed at a target's perception—in tandem with cyber operations to enhance the latter's effects. Information operations that are aimed at shaping an adversary's decision calculus may be especially useful when conducted parallel to, or in support of, cyber operations. This is because academic research has demonstrated that cyber operations, in themselves, present challenges for discerning the intent behind them and, in some instances, may not always be immediately observed and understood by the intended target.[32]

US adversaries are conducting strategic cyber campaigns to subvert US interests, such as China's campaigns to steal intellectual property at scale from the defense industrial base and broader economy or Russia's campaigns to undermine US and other democratic elections.[33] These are not simple, one-off operations. Rather, they are long-term campaigns that rely on multiple organizations and entities within adversary military and intelligence services, as well as proxy groups.[34] Within the Russian government, for example, both its military and foreign intelligence (GRU and SVR) and internal state security (FSB) organizations are known to conduct cyber operations, in addition to external entities such as the Internet Research Agency that are affiliated with the government.[35] Successfully planning and conducting long-term cyber campaigns require some level of bureaucratic maturity and an organizational apparatus to support them.[36] Of particular concern, detailed in the recent DoD report, *Military and Security Development Involving the People's Republic of China*, is the threat posed by the Chinese Communist Party's (CCP) incorporation of cyberspace and information operations into its broader military strategy, specifically through its Military-Civilian Fusion (MCF) Development Strategy and its Strategic Support Forces (SSF).[37] China's investment in its warfighting capability and capacity is real and growing. Additionally, its continued cyber-enabled theft of American intellectual property at scale; the collection of personal data of hundreds of millions of Americans; and the development of information operations capabilities are essential to China's "whole of country" economic and military strategy. In this sense, it represents a greater threat to the US and its allies and partners than Russia.

In countering adversary cyber campaigns, cyber operations represent one element of this effort. However, beyond disrupting, denying, and degrading adversary cyber capabilities and operations via cyber means, information operations can have several complementary effects at various levels of analysis. At the strategic level, they can shape the adversary's perception of the environment. This would entail conducting information operations that target the broader military and intelligence agencies which provide the organizational capacity to carry out cyber campaigns, the locus of decision-making within the government, and the proxy groups that are known to operate on their behalf. These could be conducted for purposes such as peeling away critical stakeholders within the adversary's national security apparatus, generating competition or friction among different elements of the military or intelligence services, or otherwise undermining the bureaucratic politics that play out among governmental entities.[38]

At the operational level, information operations could be conducted to affect the command and control capabilities required to execute operations. This is particularly salient with respect to the proxy organizations that adversary governments rely on for cyber operations, because these often already depend on ambiguous command and control relationships and plausible deniability.[39] Finally, at the tactical level, information operations could influence the willingness of individual operatives to carry out their missions. For instance, these operations could be crafted to introduce uncertainty among operatives that they can continue to execute missions without admonishment or consequences, undermining their resolve. These operations could work even if they only produce shirking behavior, rather than defection (e.g., timeliness in following orders, willingness to carry out a specific objective, etc.). Because effects in cyberspace are difficult to observe and uncertain, the absence of a successful outcome could be blamed on the environment, rather than on an individual operator's propensity to shirk. In the aggregate, this could have strategic effects. Taken together across the strategic, operational, and tactical levels, coupling information operations with cyber operations can reduce adversary cyber capabilities writ large.

IMPLEMENTATION

The Cyberspace Solarium Commission Report recommends several specific authorities, capabilities, and processes that will improve USCYBERCOM's ability to integrate information operations in support of defend forward. Specifically, there are three recommendations essential for effective implementation. First, as part of DoD's next Cyber Posture Review, the Commission urges Congress to request analysis of the extent to which Title 10 cyber-related authorities should be further delegated down to USCYBERCOM.[40] In particular, the Report identifies authorities pertaining to "information operations (IO), which include authorities to create, procure, and deploy personas; military information support operations (MISO); military deception (MILDEC); and counterintelligence."[41] This would enable a rapid, cohesive, and seamless implementation of information operations against defined adversaries as part of approved cyber campaign plans. Section 1642 of the FY2019 NDAA stipulates that, if the

National Command Authority determines that Russia, China, Iran, and/or North Korea are engaged in "an active, systemic, and ongoing campaign of attacks...in cyberspace," then the Secretary of Defense, acting through the Commander of USCYBERCOM, may "take appropriate and proportionate action in foreign cyberspace to disrupt, defeat, and deter such attacks...to conduct cyber operations and information operations as traditional military activity."[42] DoD should assess the conditions under which these Secretary-level authorities should be delegated to USCYBERCOM to reduce the overall friction and aid in rapid execution of such cyber and information operations.

There are, of course, potential functional concerns with delegating certain types of information-related authorities to USCYBERCOM. For example, MISO (formerly Psychological Operations, or PSYOP) is currently defined as a core activity of U.S. Special Operations Command (USSOCOM).[43] This potentially means that content generated for proactive messaging would be implemented by USSOCOM personnel, even when cyberspace is the mechanism for delivering the message (versus, for instance, dropping leaflets from an aircraft). Additionally, there are important geographic concerns that should be considered. These operations seek to influence a target audience outside of cyberspace—actual human beings—into making a decision consistent with US objectives. This takes places in the physical world, in some geographic location. Therefore, regardless of which entity may produce the content (e.g., USSOCOM) or deliver it (e.g., USCYBERCOM), the message is ultimately targeting individuals in a geographic combatant command's area of responsibility. This adds an additional stakeholder involved in signing off on a single operation. Multiple combatant command approval of a given operation can create implementation challenges.

Therefore, this Commission recommendation seeks to streamline this process and reduce the friction—within defined circumstances and considering appropriate limits and restrictions—to enable USCYBERCOM to more proactively implement cyber campaigns as part of defend forward. Accepting this recommendation would empower DoD to weigh competing concerns of relevant stakeholders, including geographic and functional combatant commands. This recommendation seeks not to delegate information warfare authorities to USCYBERCOM writ large, but rather, to urge DoD to assess how it can improve and streamline decision-making processes to enable USCYBERCOM to better meet the strategic objectives of defend forward.

Beyond authorities, the Commission recommends DoD to consider the appropriate size, organization, resourcing, and manning of the Cyber Mission Forces (CMF) for the plethora of missions it supports. Specifically, the Commission recommends that Congress direct DoD to conduct a force structure assessment of the CMF, which is at the core of USCYBERCOM's operational capability.[44] As part of this assessment, the Commission urges evaluation of the requirements these missions create for relevant intelligence agencies in their combat support agency roles.[45] Additionally, for information operations to be incorporated into defend forward cyber campaigns, organizational and personnel requirements should be part of that force

structure assessment. For instance, information operations should be deliberately included in the campaign planning process, which would require increasing the planning staff within USCYBERCOM and relevant supporting commands. With regard to the Intelligence Community, there are additional requirements to provide strategic and tactical intelligence support to cyber campaigns—such as identifying centers of gravity, adversarial weak points, and other targetable entities to influence—that should also be assessed. Senior leaders have acknowledged there is room for improvement in this area. For instance, Admiral Michael Rogers, then-Commander of USCYBERCOM, testified in a 2017 House Armed Services Committee hearing that conducting information operations "is not right now in our defined set of responsibilities per se." He also noted the personnel shortage that has persisted since the end of the Cold War, stating that "[m]any of the individuals who had the skill sets are no longer with us.... I would be the first to admit it is not what our workforce is optimized for."[46]

Finally, the Commission urges Congress to create a Major Force Program (MFP) funding category for USCYBERCOM to enable it to acquire cyber-peculiar goods and services.[47] Congress granted limited acquisition authorities in the FY2016 NDAA to USCYBERCOM totaling $75 million, which sunset in December 2021.[48] However, a true MFP for USCYBERCOM would enable it to rapidly acquire the technical capabilities or requisite talent to conduct information operations (such as seasoned, credible personas) that are critically needed by operational enablers.

US policymakers should consider domestic and international issues in implementing these recommendations. First, from a domestic perspective, given that public trust in government institutions is at a historical low, it is important for policymakers to consider how to communicate with the American people about the military's role in these efforts. Recently, the government has taken positive steps to improve the transparency associated with cyber operations. While considering operational security, engaging the American people is essential to preserve public trust in the military. From an international perspective, perhaps the most significant comparative advantage the US enjoys relative to its adversaries is its deep and enduring constellation of allies and partners. The US should take care that, as it strives to improve its capabilities and processes to fully implement defend forward, it redoubles outreach efforts to allies and partners to (a) strengthen consensus on a shared vision for the defense of cyberspace, (b) clearly distinguish between acceptable and unacceptable behavior in cyberspace, and (c) collaborate whenever possible to achieve operational and strategic objectives.

LOOKING AHEAD

With the release of the Commission report and its consideration by Congress, the US is at a moment of strategic opportunity to capitalize on these efforts and significantly bolster its ability to counter adversary cyber campaigns. The Commission's findings also coincide with parallel DoD efforts to conceptualize and operationalize links between the cyber and information

environments. As the Commission's recommendations make their way into legislation, and as assessments and studies derived from the Commission Report surface, follow-up actions should be taken to ensure the successful, efficient implementation of defend forward, including integrating information operations into cyber campaigns.

Additionally, Congress should also consider how to extend the contributions of the Commission beyond the more tightly-scoped challenge of developing a strategy to defend the US in cyberspace. One core insight of the Commission's report, drawing inspiration from the Eisenhower Administration's original Project Solarium to develop a grand strategy to deter the Soviet Union, is that a single instrument of national power, in isolation, is insufficient to have decisive and sustainable strategic effects.[49] A consequence, likely unintended, of post-9/11 US strategy has been a preponderant focus on military solutions to address a diverse range of foreign policy challenges.[50] The Commission urged that policymakers should be wary of always turning to the military instrument of power. While crucially important, military capabilities hardly address the full scope of cybersecurity challenges.

There are further parallels between the Commission's efforts and the Eisenhower Administration's approach to Cold War grand strategy. In June 1953, six months before conducting Project Solarium, Eisenhower established the President's Committee on International Information Activities, also known as the Jackson Committee, to develop policies pertaining to the role of information and propaganda in US national security. Ultimately, the Committee's findings played a significant role in driving US grand strategy during the Cold War.[51] One important Committee outcome was establishment via Executive Order 10477 of the U.S. Information Agency (USIA) in 1953. USIA was the principal vehicle for US information and propaganda efforts during the Cold War, but was abolished in the Foreign Affairs Reform and Restructuring Act of 1998.[52]

Currently, there is no comparable, independent entity leading a US government information strategy. The State Department has a natural leadership role in this space. As the US seeks to be more proactive in defending forward against adversarial threats—to include information operations—diplomatic efforts must drive engagement. Of note, the Global Engagement Center (GEC) within the State Department, initially created in 2016 to coordinate US government communications to counter terrorist messaging and information campaigns, was given a broader mandate and increased funding in the FY2017 NDAA.[53] The 2017 NDAA defined its role as to "synchronize, and coordinate efforts of the Federal Government to recognize, understand, expose, and counter foreign state and non-state propaganda and disinformation efforts aimed at undermining United States national security interests."[54] Within DoD, a Principal Information Operations Advisor exists to "coordinate and deconflict its operations with the GEC, who is the lead."[55] However, it is unclear whether the GEC is sufficiently staffed or resourced to accomplish this important mission.[56] Moreover, a 2018 staff report prepared for the Senate Committee on Foreign Relations on Russia's information operations noted that, within the

GEC, "operations have been stymied by the Department's hiring freeze and unnecessarily long delays by its senior leadership in transferring authorized funds to the office."[57]

Given our nation's vulnerabilities posed by the ongoing weaponization of information by US adversaries, it is imperative that Congress and the executive branch take a bold stance toward not only implementing the recommendations in the Cyberspace Solarium Commission but also think more broadly about a whole-of-nation effort to promote US interests and values in the information space. While resurrecting a Cold War agency such as the USIA, or further empowering the GEC are not perfect solutions, the essential question of the role of information as an instrument of power in US grand strategy and the appropriate locus of these efforts within the executive branch are issues that Congress should not shy away from addressing.

NOTES

1. "Summary: Department of Defense Cyber Strategy," *U.S. Department of Defense*, January 2018, 1.
2. "The Department of Defense Cyber Strategy," *U.S. Department of Defense*, April 2015.
3. "Joint Publication 3-12: Cyberspace Operations," June 8, 2018, viii-ix.
4. For examples of early work, see John Arquilla and David Ronfeldt, *In Athena's Camp: Preparing for Conflict in the Information Age*, (Santa Monica, CA: RAND Corporation, 1997); Richard Harknett, "Information Warfare and Deterrence," *Parameters* 26, no. 3 (1996): 93-107.
5. David V. Gioe, "Cyber Operations and Useful Fools: The Approach of Russian Hybrid Intelligence," *Intelligence and National Security* 33, no. 7: 954-973.
6. Shawn Henry and Aaron Brantly, "Countering the Cyber Threats," *Cyber Defense Review* 3, no. 1 (Spring 2018): 47-56, Herbert Lin, "Developing Responses to Cyber-Enabled Information Warfare and Influence Operations," *Lawfare*, September 6, 2018, https://www.lawfareblog.com/developing-responses-cyber-enabled-information-warfare-and-influence-operations.
7. Elsa B. Kania and John K. Costello, "The Strategic Support Force and the Future of Chinese Information Operations," *Cyber Defense Review* 3, no. 1 (2018): 105-122.
8. "Defense Primer: Information Operations," *Congressional Research Service*, December 18, 2018. However, there are also important limitations on DoD's ability to conduct information operations, specifically stemming from concerns about operations that may have an impact on the American people.
9. Kimberly Underwood, "Army Cyber to Become Information Warfare Command," March 14, 2019, https://www.afcea.org/content/army-cyber-become-information-warfare-command. Kimberly Underwood, "Army CEMA Teams Advance Information, Electronic and Cyber Warfare," August 6, 2018, https://www.afcea.org/content/army-cema-teams-advance-information-electronic-and-cyber-warfare.
10. "USCYBERCOM 2018 Cyberspace Strategy Symposium Proceedings," *U.S. Cyber Command*, February 15, 2019, 2, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Cyberspace%20Strategy%20Symposium%20Proceedings%202018.pdf?ver=2018-07-11-092344-427.
11. For a comprehensive discussion of grand strategy, see Hal Brands, *What Good Is Grand Strategy? Power and Purpose in American Statecraft from Harry S. Truman to George W. Bush* (Ithaca NY: Cornell University Press, 2014).
12. "Cyberspace Solarium Commission Report," *Cyberspace Solarium Commission*, 11 March 2020, https://www.solarium.gov/report. For a discussion of the strategic approach, 23-30.
13. John S. McCain National Defense Authorization Act for Fiscal Year 2019, H.R. 5515, 115th Congress, 2018; "Cyberspace Solarium Commission Report," *Cyberspace Solarium Commission*, March 11, 2020, https://www.solarium.gov/report.
14. "Cyberspace Solarium Commission Report," 69-70.
15. Ibid., 66-67.
16. "Summary: Department of Defense Cyber Strategy," 2018, 1. There are references to the idea of defend forward in the 2018 Command Vision for U.S. Cyber Command, but the concept is not the central feature of that document.
17. "Cyberspace Solarium Commission Report," 2020, 32.
18. "National Cyber Strategy of the United States of America," *The White House*, September 2018, and "Summary: Department of Defense Cyber Strategy," 2018.
19. "Cyberspace Solarium Commission Report," 2020, 6; Erica D. Borghard and Mark Montgomery, "Defend Forward as a Whole-of-Nation Effort," *Lawfare*, March 11, 2020, https://www.lawfareblog.com/defend-forward-whole-nation-effort.
20. For example, when speaking on the topic of offensive cyber operations, former National Security Advisor John Bolton stated, "We're now opening the aperture, broadening the areas we're prepared to act in… Our response doesn't have to be only in cyberspace so we're really looking at the full range of things we can do." Kenneth Rapuano, Assistant Secretary of Defense for Homeland and Global Security, told the house Armed Force Committee that DoD's defend forward "strategy normalizes the department's efforts in the cyberspace domain, integrating cyberspace operations into military operations across all physical domains, and reinforces the need to prevent or degrade threats before they harm U.S. national interests." See Shannon Vavra, "U.S. Ramping up Offensive Cyber Measures to Stop Economic Attacks, Bolton Says," *CyberScoop*, June 11, 2019, https://www.cyberscoop.com/john-bolton-offensive-cybersecurity-not-limited-election-security/; Terri Moon Cronk, "DOD's Cyber Strategy of Past Year Outlined Before Congress," *U.S. Department of Defense News*, March 6, 2020, https://www.defense.gov/Explore/News/Article/Article/2103843/dods-cyber-strategy-of-past-year-outlined-before-congress/.

NOTES

21. Joint Publication 3-13 (November 27, 2012), ix.
22. Herbert Lin and Jaclyn Kerr, "On Cyber-Enabled Information Warfare and Information Operations," f*orthcoming, Oxford Handbook of Cybersecurity* (2019), 4.
23. Ibid., 5.
24. Herbert Lin, "The Existential Threat from Cyber-Enabled Information Warfare," *Bulletin of Atomic Scientists* 75, no. 4 (2019): 187-196.
25. For a discussion of recently declassified documents on Operation GLOWING SYMPHONY and Joint Task Force-ARES, obtained through Freedom of Information Act requests, see Cyber Vault project at the National Security Archive, "Joint Task Force ARES and Operation GLOWING SYMPHONY: Cyber Command's Internet War Against ISIL," https://nsarchive.gwu.edu/briefing-book/cyber-vault/2018-08-13/joint-task-force-ares-operation-glowing-symphony-cyber-commands-internet-war-against-isil.
26. "Statement of Admiral Michael S. Rogers, Commander, United States Cyber Command, Before the Senate Committee on Armed Services," February 27, 2018, 4. Also see, David E. Sanger, "U.S. Cyberattacks Target ISIS in a New Line of Combat," *The New York Times,* April 24, 2016, https://www.nytimes.com/2016/04/25/us/politics/us-directs-cyber-weapons-at-isis-for-first-time.html.
27. Ryan Browne and Barbara Starr, "Top Pentagon Official: 'Right now it sucks' to be ISIS," *CNN,* 14 April 2016, https://www.cnn.com/2016/04/13/politics/robert-work-cyber-bombs-isis-sucks/index.html.
28. "Statement of General Paul M. Nakasone, Commander, United States Cyber Command, Before the Senate Committee on Armed Services," February 14, 2019, 4. Dina Temple-Raston, "Task Force Takes on Russian Election Interference," *NPR,* August 14, 2019, https://www.npr.org/2019/08/14/751048230/new-nsa-task-force-takes-on-russian-election-interference; and Julian E. Barnes, "Cyber Command Operation Took Down Russian Troll Farm for Midterm Elections," *The New York Times,* February 26, 2019, https://www.nytimes.com/2019/02/26/us/politics/us-cyber-command-russia.html.
29. Brandon Valeriano, "Managing Escalation Under Layered Cyber Deterrence," *Lawfare,* April 1, 2020, https://www.lawfareblog.com/managing-escalation-under-layered-cyber-deterrence. For a general discussion of the risks of escalation in cyberspace, see Erica D. Borghard and Shawn W. Lonergan, "Cyber Operations as Imperfect Tools of Escalation," *Strategic Studies Quarterly* 13, no. 3 (2019): 122-145.
30. General Nakasone does note that information-sharing with partners and enabling others is also an important part of defend forward. *United States Special Operations Command and United States Cyber Command: Hearing Before the Senate Armed Services Committee,* 116th Congress, 2 (February 14, 2019) (statement of General Paul M. Nakasone, Commander United States Cyber Command); and William T. Eliason, "An Interview with Paul M. Nakasone," *Joint Force Quarterly* 92 (1st Quarter 2019), 6.
31. Daniel Byman and Matthew Waxman, *The Dynamics of coercion: An American Foreign Policy and the Limits of Military Might,* (Cambridge, UK: Cambridge University Press, 2002); and Glenn Snyder, *Deterrence and Defense,* (Princeton, NJ: Princeton University Press, 1961).
32. Erica D. Borghard and Shawn W. Lonergan, "The Logic of Coercion in Cyberspace," *Security Studies* 26, no. 3 (2017): 452-481; Borghard, "The 'Known Unknowns' of Russian Cyber Signaling," *Council on Foreign Relations-Net Politics Blog,* April 2, 2018, https://www.cfr.org/blog/known-unknowns-russian-cyber-signaling; Gartzke and Lindsay argue that cyber operations should be understood in the context of intelligence and covert operations capabilities and have utility in their role in aiding deception, precisely because of their ambiguity and problems associated with clear signaling. See Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies* 24, no. 2 (2015): 316-348.
33. The Solarium Commission Report describes adversarial campaigns in depth. See "Cyberspace Solarium Commission Report," 2020, 8-14; and Erica D. Borghard and Shawn W. Lonergan, "Public-Private Partnerships in Cyberspace in an Era of Great Power Competition," forthcoming.
34. Tim Maurer, *Cyber Mercenaries,* (Cambridge, UK: Cambridge University Press, 2018); and Erica D. Borghard and Shawn Lonergan, "Can States Calculate the Risks of Using Cyber Proxies?" *Orbis* 60, no 3 (2016): 395-416.
35. Michael Connell and Sarah Volger, "Russia's Approach to Cyber Warfare," Center for Naval Analyses, September 2016; "Grand Jury Indicts Thirteen Russian Individuals and Three Russian Companies for Scheme to Interfere in the United States Political System," The Department of Justice, February 16, 2018, https://www.justice.gov/opa/pr/grand-jury-indicts-thirteen-russian-individuals-and-three-russian-companies-scheme-interfere; Andrew Radin, Alyssa Demus, and Krystyna Marcinek, "Understanding Russian Subversion: Patterns, Threats, and Responses," RAND Corporation, February 2020.

NOTES

36. Rebecca Slayton, "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment," *International Security* 41, no. 3 (2017): 72-109; and Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," Security Studies 22, no. 3 (2013): 365-404.
37. Office of the Secretary of Defense, "Military and Security Developments Involving the People's Republic of China 2020: Annual Report to Congress, https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF. Also see Christian Brose, *The Kill Chain: Defending America in the Future of High-Tech Warfare* (New York: Hachette Books, 2020).
38. Barbara Geddes, Joseph Wright, and Erica Frantz, "Autocratic Breakdown and Regime Transitions: A New Data Set," *Perspectives on Politics* 12, no. 2 (2014): 313-331; Bruce Bueno De Mesquita, et al., "Testing Novel Implications from the Selectorate Theory of War," *World Politics* 56, no. 3 (2004): 363-388; and Jessica L. Weeks, "Autocratic Audience Costs: Regime Type and Signaling Resolve," *International Organization* 62, no. 1 (2008): 35-64.
39. Borghard and Lonergan, "Risks of Using Cyber Proxies."
40. For a discussion of the implications of the 2019 National Defense Authorization Act, which defined cyber operations as traditional military activity, see Robert Chesney, "The Law of Military Cyber Operations and the New NDAA," *Lawfare*, 26 July 2018, https://www.lawfareblog.com/law-military-cyber-operations-and-new-ndaa.
41. "Cyberspace Solarium Commission Report," 2020, 115.
42. John S. McCain National Defense Authorization Act for Fiscal Year 2019, H.R. 5515, 115th Congress, 2018, Section 1642.
43. "Core Activities," U.S. Special Operations Command, https://www.socom.mil/about/core-activities.
44. "Cyber Mission Force Achieves Full Operational Capability," *U.S. Department of Defense News*, May 17, 2018, https://www.defense.gov/Explore/News/Article/Article/1524747/cyber-mission-force-achieves-full-operational-capability/.
45. "Cyberspace Solarium Commission Report," 2020, 113.
46. HASC Hearing, "Hearing to Receive Testimony on United States Cyber Command, 9 May 2017, 20-21.
47. "Cyberspace Solarium Commission Report," 2020, 114.
48. Erica D. Borghard, "Cyber Command Needs New Acquisition Authorities," *Lawfare*, May 12, 2020, https://www.lawfareblog.com/cyber-command-needs-new-acquisition-authorities.
49. William B. Pickett, ed, *George F. Kennan and the Origins of Eisenhower's New Look: An Oral History of Project Solarium* (Princeton: Princeton Institute for International and Regional Studies, 2004).
50. See, for example, Rosa Brooks, *How Everything Became War and the Military Became Everything: Tales From the Pentagon* (New York: Simon & Schuster, 2016).
51. For further discussion, see Shawn J. Parry-Giles, "The Eisenhower Administration's Conceptualization of the USIA: The Development of Overt and Covert Propaganda Strategies," *Presidential Studies Quarterly* 24, no. 2 (Spring 1994), 263-276.
52. 105th Congress of the United States of America. H.R. 1757: Foreign Affairs Reform and Restructuring Act of 1998, (January 27, 1998).
53. Executive Order 13721: Developing an Integrated Global Engagement Center to Support Government-wide Counterterrorism Communications Activities Directed Abroad and Revoking Executive Order 13584, Section 1287, https://www.hsdl.org/?abstract&did=791347.
54. NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2017, Sec. 1287, https://www.congress.gov/114/plaws/publ328/PLAW-114publ328.pdf#page=548.
55. "Defense Primer: Information Operations," Congressional Research Service, January 14, 2020, 2.
56. Abigail Tracy, "A Different Kind of Propaganda: Has America Lost The Information War?" *Vanity Fair*, April 23, 2018.
57. "Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security," January 10, 2018, 3.

A Legal Framework for Enhancing Cybersecurity through Public-Private Partnership

The Honorable Joe R. Reeder
Professor Robert E. Barnsby

ABSTRACT

The Cyberspace Solarium Commission (CSC) published its report in March 2020 offering emphatic, far-reaching recommendations in the cybersecurity domain. This report highlights the rapidly growing importance of public-private partnership (P3) in this domain as a national security cornerstone, and significantly informs the debate over the public-private balance in the cybersecurity system of governance in the United States. While important questions remain as to the best ways to safeguard public law values, the report strongly supports arguments for informed P3 collaboration, and further discourages the notion that cybersecurity should exclusively be an inherently governmental function. A legal analysis of partnering in the cyber domain suggests the risks of violating existing inherently governmental function rules are low, and navigable. Indeed, the CSC's strong, bipartisan report accepts this as a given point of departure from the *ad hoc* P3 system we have today, and recommends concrete steps to advance national security and other public law values such as accountability, transparency, fairness, and privacy. Like legislation that set the stage for the NASA-SpaceX partnership, the CSC's unequivocal embrace of P3 in the cybersecurity realm has great potential to guide legislation and other steps to reshape and adapt "defense-of-nation" Cyber domain efforts.

The Honorable Joe Reeder, a West Point graduate (1970), served in the 82nd Airborne Division and was the Army's 14th Under Secretary and Chairman of the Panama Canal Commission (1993-97). A television commentator on national security and legal issues, he has published a number of articles and editorials, and represented nations, companies, law firms and entertainers as a partner at Greenberg Traurig, LLP, one of the world's largest international law firms with over 2,200 attorneys.

On March 11, 2020, the Cyberspace Solarium Commission (CSC),[1] a Congressionally-established bipartisan task force, released its final 174-page report, covering many pressing national security issues related to cybersecurity.[2] The CSC's "urgent call to action,"[3] recommends selection of a National Cyber Director, creation of a Cybersecurity Bureau within the State Department, and strengthening of the Cybersecurity and Infrastructure Security Agency (CISA). These are but three of the 82 recommendations organized along six policy pillars in the critical Cyber domain. [4] The importance of the issues addressed cannot be overstated, as emphasized by recent authors exploring the impacts of the CSC recommendations, with more commentary to follow.[5]

As lawyers, we appreciate the Commission's efforts to provide a definitive, coherent roadmap for future legislation, particularly iterations of the National Defense Authorization Act (NDAA) that likely will include provisions supporting many Commission recommendations. Although a complete "legal unpacking" of all aspects of the Commission's comprehensive report is an important task, our focus here centers exclusively on the fifth of the Commission's six pillars[6]—and its emphatic view that the United States Government (USG) should take a bold lead in working much more cohesively, collaboratively, and comprehensively with the private sector on national cybersecurity. Calling for significant steps forward in P3 law, the Commission makes strong, unequivocal P3-related recommendations, authored in consultation with several of the nation's brightest legal minds on this subject.[7] The CSC's bipartisan consensus on the heretofore contentious issue as to P3 boundaries will richly inform discussions on the appropriate balance in P3, and shift the debate from "whether" to "when" and "how" governmental actors should share cybersecurity functions with, or in some cases shift them to, the private sector. From a legal perspective, this consensus un-

Professor Rob Barnsby, also a West Point graduate (1996), is the Cyber Law Fellow for the Army Cyber Institute at West Point, where he teaches Cyber Law and Constitutional Law in the U.S. Military Academy's Department of Law. He recently served as a Visiting Assistant Professor at the University of California, Berkeley, School of Law, and has published several scholarly articles on a wide variety of cyber and legal subjects. In his twenty years of service as a U.S. Army officer, Rob led high-visibility legal teams in strategic locations throughout the United States and Afghanistan. Rob earned his J.D. from the William & Mary Law School, where he served as Executive Editor of the *William & Mary Law Review*.

derscores the importance of a successful P3 collaboration in optimizing the nation's cybersecurity, as we illuminate below with a "totality of circumstances" and public law values-based analysis.

Before the Commission's work, legal discussions on public-private partnerships in the cyber realm meandered among interesting but ultimately inconsequential cybersecurity P3 "cocktail party" conversations.[8] Some legal scholars voiced concern that cybersecurity partnerships in defense of the nation could violate longstanding rules that bar the outsourcing of "inherently governmental functions,"[9] and that fundamental "public law values [may be violated] when government functions are contracted out to private parties."[10] On the other hand, national-level cyber policy, along with unclassified Presidential and Department of Defense (DoD) strategy documents, increasingly have suggested otherwise and, over the course of several recent iterations, included policy pronouncements "incentiv[izing] cybersecurity investments ... [to] work with private ... sector entities to ... realize benefits from those investments,"[11] and urged DoD to "build trusted private sector partnerships."[12]

The bipartisan CSC team—including both public- and private-sector partners with executive and legislative, legal and non-legal members—resoundingly calls for lasting partnerships without even a mention of legal impediments. This should guide further debate as to USG partnering with the private sector in "defense of the nation" from a cybersecurity perspective.[13] "Totality of the circumstances" analysis amply supports the conclusion that national-level cybersecurity per se is not—and, essentially, cannot be—an inherently governmental function.[14] Rational analysis also confirms that our nation's current cybersecurity construct neither violates the law nor, with appropriate governance and CSC-recommended legislation, will it unduly risk undermining public law values going forward.

The recent SpaceX launch of the first-ever commercially built spacecraft provides a good example of a successful and highly functional public-private partnership executed at the highest levels of government and industry.[15] From a national and legislative perspective, this successful partnership would never have formed without passage of the NASA Transition Authorization Act of 2017, wherein Congress affirmed its "commitment to the use of a commercially developed, private sector launch and delivery system to the [International Space Station] for crew missions."[16] This Congressional language enabled NASA to work with the private SpaceX company to accomplish the historic space mission our nation witnessed this summer.[17]

Until quite recently, few believed space exploration would begin to include private sector competition for direct and large-scale work with the USG, yet SpaceX and its private competitors—with fulsome USG cooperation—changed that narrative. The USG has not abandoned its dominant Space domain role. Nor should or will it abandon its preeminent "defense-of-nation" role in the cybersecurity domain. Nevertheless, Congress must prioritize focus on the CSC recommendations and better enable the respective public and private cybersecurity actors to collaborate effectively, as occurred with public and private space actors in 2017.

The Pacific and Atlantic Oceans—7,000- and 4,000-mile geographical barriers that have militarily protected the United States for nearly 250 years—provide not even speed-bump protection from cyber devastation. Equally if not even more ominous is the ubiquitous nature of cyber "weapons," so easily accessible to the general public, unlike tanks, missiles, and military aircraft. These evolving circumstances mean certain P3 roles and missions in cybersecurity must be clarified, and even codified, given the pervasive private sector presence in, and ownership and/or control of, critical cyber infrastructure—in some estimates as high as 85% of the overall infrastructure.[18] CSC Recommendation 5.2 calls upon Congress to establish and fund a Joint Collaborative Environment, a common and interoperable environment for the sharing and fusing of threat information, insight, and other relevant data across the federal government and between the public and private sectors. CSC Recommendation 5.3 urges Congress to establish a public-private, integrated cyber center within CISA in support of the critical infrastructure security mission and to conduct a one-year, comprehensive review of federal cyber and cybersecurity centers, including plans to develop and improve integration.[19]

The Commission's Final Report also underscores the serious vulnerability of our nation's infrastructure, forewarning the threat not only to structures, (e.g., energy plants and power grids), but also to the US water supply. Typically, local municipalities oversee the water supply, with governance and security standards varying widely, sometimes falling well below our nation's lowest common denominator vis-à-vis "best practices." Cyber protection of our nation's water utilities and resources may lack the security alarm bells that accompany reportable metrics, and can be shortchanged by municipalities that face budgetary constraints.[20] These vulnerabilities illustrate that with or without enabling legislation, going forward, private security actors will play an increasingly larger role in the nation's cybersecurity. For the sake of US

national security, laws are urgently needed not only to empower P3 collaboration but also to provide clarity as to the lines and divisions of labor and authority between the public and private actors. Such clarity has become time-urgent, as some of our closest allies have recognized and already addressed.[21]

Despite decades of debate evolving on the role of private actors in "defense-of-nation" cybersecurity, official direction for the USG to partner with the private sector has consisted mostly of generic pleas to "work with the private sector."[22] Even the most recent DoD cyber strategy document contained only generic guidance to "expand DoD cyber cooperation with . . . industry," "work with the private sector," and "[b]uild trusted private sector partnerships."[23] Congress upgraded the conversation for the first time in the 2019 National Defense Authorization Act,[24] with its call for a formal commission to report on the nation's cybersecurity.

Following ten months of concentrated effort, the CSC proposed a P3 plan to "[o]perationalize cybersecurity collaboration with the private sector."[25] The CSC plan also urges the USG to unleash its "unique authorities, resources, and intelligence capabilities to support [private-sector entities]."[26] Its plan envisions an overall layered approach to deterrence. It also features "international engagement and cooperation," enforcement of already agreed norms in the cyber realm, and use of non-military tools (including information sharing). The CSC Report also urges "align[ment] of market forces" and "explor[ation of] legislation, regulation, executive action, and public- as well as private-sector investments," featuring "partner[ship] with the private sector and [an adjustment to] incentives to produce positive outcomes."[27] CSC Recommendation 5.2, calls for a "joint collaborative environment," and is further etched by CSC's Recommendation 5.3, which calls for the physical housing and ownership of this collaboration mission within the Department of Homeland Security's CISA. These recommendations are key to a culture of real-time P3 information sharing and joint analysis, and should be deemed essential.

We turn now to how CSC Report P3 recommendations help to illuminate the path toward an optimal design and governance of our nation's cybersecurity P3 relationships—whether through soft regulation, such as CSC's high-visibility recommendations, or with implementing regulations. One important requirement will be to avoid delegating missions to the private sector for which it is either unsuited, or hopelessly conflicted, for example, by profit considerations. Subpoena powers of the court, and other missions historically policed or performed by the government provide yet other examples of missions many believe are governmental per se and should stay there. Since 1983, such "contracting out" of functions to the private sector has been circumscribed by the Office of Management and Budget's (OMB) Circular Number A-76, which delineates those activities that private-sector entities are authorized to perform. Most recently revised in 2003, OMB Circular A-76 has consistently barred the USG from using commercial sources for functions "inherently Governmental in nature,"[28] which it describes as those functions "so intimately related to the public interest as to mandate per-

formance by Government employees."[28] Put another way, A-76 flagged certain activities as off limits for "contracting out" to the private sector, because the private sector's profit motive could undermine or otherwise conflict with the public's best interests. Under this reasoning, certain policy making decisions are quintessentially governmental in nature, and thus to be entrusted to and performed solely by the government. Examples include "act[s] of governing [which involve the] discretionary exercise of Government authority [e.g.,] criminal investigations, prosecutions and other judicial functions; . . . management and direction of the Armed Services . . . [and] direction of intelligence and counter-intelligence operations."[30] In recent armed conflicts, the inherently governmental nature of classic battlefield operations reserved to States under the Law of Armed Conflict, including detention and interrogation on the battlefield, has also been reinforced.[31]

Recent legal scholarship adds to the A-76 understanding in this area, particularly in the skillful analysis of cyber law scholars such as Kristen Eichensehr.[32] She suggests that—whether or not OMB Circular A-76 should bar privatizing certain aspects of cybersecurity—our existing cybersecurity system exposes to abuse certain fundamental public law values (e.g., privacy, fairness and transparency). In her 2017 *Texas Law Review* article, Professor Eichensehr advanced three basic reasons for not outsourcing cybersecurity to the private sector: (1) a well-functioning government should be capable of defending computer networks at the national level; (2) to do otherwise places the private sector in a quasi-governmental role, and otherwise compromises public law values with corporate profit motives; and (3) it is important to avoid undue private-sector corporate access to sensitive private individual information—despite Eichensehr's observation that "individuals . . . are typically more concerned about the government accessing their private information than about corporations accessing it."[33] Eichensehr essentially argues that "certain [cybersecurity] functions exist solely in the realm of government and within the expectations of the state."[34] While we would take issue with any blanket assertion that our government alone can ever be the sole, stand-alone guarantor of our nation's cybersecurity, Professor Eichensehr's analysis undoubtedly will and should inform further thought as to optimal legal ground rules for policing public-private partnerships in the cyber domain, and where lines should be drawn to prevent the privatizing of inherently governmental functions.

Unlike judicial activities and other conspicuously governmental functions,[35] computer network functions are neither obviously nor exclusively designed to be delivered by governmental elements. Such activities thus warrant further analysis under the OMB Circular's Supplemental Guidance and what it styles as "totality of the circumstances." The "determin[ation as to] whether a function is. . . inherently governmental. . . depends upon . . . a number of factors, and the presence or absence of any one is not in itself determinative of the issue."[36] OMB's guidance requires examination of many factors likely to impact any of the public law values alluded to above, and allows for the informed judgment of decision makers on a case-by-case basis. Such judgments will play a key role in the evolution of Cybersecurity P3. For example,

a most important question is whether defense of the nation's computer networks, in totality, should—or even could, as a practical matter—be exclusively regulated by the government, and hence beyond the purview of the CSC-envisioned public-private partnerships. Fortunately, this question, at least for now, has been resolved in favor of P3.

Another OMB factor in the proper division of labor between the government and private sectors is the "status quo ante." The OMB Circular's Supplemental Guidance observes that those functions already being performed by private parties are more likely to remain acceptable under P3 legal analysis.[37] It would be hard to overstate the pervasive extent to which the private sector already is deeply embedded in myriad aspects of our nation's cybersecurity, a subject others have described at length in this and many other publications.[38] While not by itself a dispositive factor, the private sector's long-standing performance of cybersecurity functions strongly supports the conclusion that continued private-sector participation should be considered "A-76 permitted," especially the P3 undertakings contemplated in the CSC Report. Similarly, the Supplemental Guidance allows for disclosure to the private sector of sensitive technical complexities, particularly where private actors possess as much, if not more, technical knowledge. Again, rudimentary knowledge of computer networks confirms that highly sophisticated cyber-sensitive technical expertise resides in the private sector—another factor under A-76 that supports fully integrated public-private partnerships and collaboration. For example, Eichensehr notes that the private sector, led by industry titan Microsoft, essentially pioneered the legal tactics (which necessarily utilize public-private collaboration) employed to take down operations of various cybercriminal-deployed botnets.[39]

Cost concerns also figure into analysis as to whether a particular function should be privatized. Redundant, expensive, and pre-existing national structures obviously are undesirable. Yet expensive and often sophisticated cybersecurity measures generally coexist wherever both private and public sector computer networks reside. Thus, from a cost perspective, requiring a uniquely governmental cybersecurity apparatus—parallel to a pre-existing private apparatus—essentially would call for a function falling outside A-76's "inherently governmental" scope.

Apart from her A-76 analysis, Professor Eichensehr eloquently explains why we also must ask whether privatization of cybersecurity violates public law values such as privacy, fairness, or transparency. Here, bipartisan operation and reporting of CSC, including its strong call for robust public-private partnerships, serves as a model of transparency.[40] As is true of accompanying Congressional oversight, enabling laws and regulations likely to implement CSC recommendations, by their nature, will be transparent in governing our public-private partnerships. New legislation combined with enforcement of existing Competition in Contracting Act (CICA) oversight should further mitigate fairness concerns, as CICA was enacted in order to even the playing field in competition for government contracts.[41] Actual awarding, administering, and terminating contracts are inherently governmental functions that generally are not outsourced.[42]

We are wary of urging blanket rules in the evolving governance of P3 cybersecurity partnerships, absent compelling exigencies, yet decision-making functions tainted or impaired by a competing profit motive should never be outsourced to a non-governmental authority. For example, much has been written about the Army's ill-fated Future Combat Systems that, but for a few spin-off technologies, had no fielded system and nothing else to show for the over $18 billion in taxpayer dollars expended.[43] This costly lesson traces directly to a procurement decision that empowered two companies, Boeing and SAIC, that were neither disinterested parties nor otherwise rendered so, and yet essentially made contract award decisions in selecting participating contractors. Privatizing this decision-making power of what many consider an "inherently governmental function" simply did not work.

A more workable example, we hope, is the ongoing Cybersecurity Maturity Model Certification (CMMC) requirement, wherein DoD is outsourcing a key function of this requirement. Specifically, DoD has empowered (a) Cybersecurity Maturity Model Certification Accreditation Body, Inc., an independent non-profit entity, to accredit CMMC Third Party Assessment Organizations (C3PAOs), and (b) individual evaluators to perform CMMC assessments of current and potential DoD contractors. A CMMC assessment and certification is now being required at one of several different levels as a prerequisite for doing business with DoD. This process includes a cadre of non-government auditors deciding which companies will, or will not, qualify for DoD contracts. No direct profit motive impairs the CMMC process, but we anticipate legislative concerns as to the oversight of this now delegated function, which potentially will influence tens of billions of dollars of DoD contract awards. Indeed, on September 16, 2020, it was reported that two members of CMMC's Advisory Board were forced off the Board, due to an alleged "pay for play" partner program, with charges as high as $500,000 "as a way to promote certain companies over others."[44]

Enforcement of existing legislation, accompanied by other policy changes and executive actions, must continuously include monitoring of the oversight of protections for delegated core public law values, and this should be integral to codification of the CSC's P3 recommendations described above. Properly monitored and protected with checks and balances, the proliferation of partnerships over time should reinforce a level of trust between public and private sector actors—a trust that must be nurtured and can never safely be taken for granted.[45]

In *The Cyber Defense Review*'s Spring 2020 issue, Professor Jim Chen underscores the importance of trust in effectively administering cyber security in the continuum of public-private interface, *i.e.*, in the spectrum running from "cooperation, to collaboration, to full integration, and explains why and how a sound framework for full-scale public-private collaboration can and ultimately should exist."[46] Moreover, with focus on laws designed to protect public-value interests, as discussed above, the CSC's strong endorsement of the technical and pragmatic reasons for expanding our P3 provides a major step forward. Realistic analysis of what are and are not "inherently governmental functions" should continue, but

more attention must focus on assuring a robust role for an empowered private sector which already is pervasively invested in the nation's cybersecurity. With thoughtful design, that role, consistent with public-value interests, can be greatly expanded and much better integrated. This discussion of A-76 and "totality of circumstance" analysis, to include the importance of "trust" Professor Chen highlights, all go to reinforce the CSC's strong argument in support of the P3 partnership.[47] For our national cybersecurity efforts to work optimally, the legal scales must tip to align better with broader and deeper private-sector participation.

NOTES

1. Established in the John S. McCain National Defense Authorization Act for Fiscal Year 2019, the Cyberspace Solarium Commission comprised fourteen commissioners, including four currently serving legislators, four executive branch leaders, and six experts with extensive backgrounds in industry, academia, and government service, (https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view.) The Commission's definition describing cybersecurity, adopted here, is the "prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication. This includes ensuring the availability, integrity, authentication, confidentiality, and nonrepudiation of the information contained therein, " (United States Cyberspace Solarium Commission, Final Report, March 2020, 132). The authors thank CSC members Professor Frank Cilluffo (Commissioner), RADM (Ret.) Mark Montgomery (Executive Director), and Professor Erica Borghard (Senior Director) for sharing valuable insights as to some of the critical aspects of the Commission's work. Thanks also go for suggestions provided by John Felker, former Director of the National Cybersecurity & Communications Integration Center (2015-19), and earlier, Deputy Commander of the U.S. Coast Guard Command (2010-12). The authors also thank Chip Leonard (USMA 1970) and Greenberg Traurig's Shomari Wade for their valuable editorial insights and suggestions. Views and shortcomings expressed here are exclusively the authors' responsibility, and do not necessarily reflect official policy or positions of the U.S. Military Academy or any DoD agency.
2. United States Cyberspace Solarium Commission, Final Report, March 2020, https://www.solarium.gov/report.
3. Ibid.
4. Ibid. *See also* Cyberspace Solarium Commission Testimony Before the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation of the Committee on Homeland Security, U.S. House of Representatives, July 17, 2020, 2.
5. *See, e.g.*, Kristen Eichensehr, "Public-Private Cybersecurity," *Texas Law Review,* 2017, further described throughout this work.
6. Ibid. Those six pillars are: (1) Reform USG's Structure and Organization for Cyberspace; (2) Strengthen Norms and non-military Tools; (3) Promote National Resilience; (4) Reshape the Cyber Ecosystem toward Greater Security; (5) Operationalize P3 Cybersecurity Collaboration; and (6) Preserve and Employ the Military Instrument of Power.
7. CSC Legal Advisors included Stefan Wolfe, General Counsel; Corey Bradley, Deputy General Counsel; Cody Cheek, Legal Advisor; David Simon, Chief Counsel for Cybersecurity and National Security; Veronica Glick, Deputy Chief Counsel for Cybersecurity and National Security; and Joshua Silverstein, Deputy Chief Counsel for Cybersecurity and National Security. U.S. Cyberspace Solarium Commission, Final Report, March 2020, *supra* note 2, 151.
8. *See infra* notes 11, 12, 22, 23, and accompanying text.
9. *See infra* notes 28-31 and accompanying text.
10. Kristen Eichensehr, "Public-Private Cybersecurity," *Texas Law Review,* 2017, *supra* note 5 (although Eichensehr describes an informal public-private *system*, not a partnership).
11. National Cyber Strategy of the United States of America, September 2018, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.
12. Department of Defense Cyber Strategy Summary, 2018, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF). *See also* H.R. McMaster, "Battlegrounds—The Fight to Defend the Free World," Harper-Collins (September 2020), 71-79. The General explains why today's battlefield goes far beyond kinetic military operations. And, pertinent here, in the context of Russian aggression, he concludes that, while no combination of P3 efforts to counter foreign cyberattacks will permanently resolve the threat, [p]rivate-sector effort can create a firehose of truth to counter [any] firehose of falsehoods." Ibid., 74.

NOTES

13. Law enforcement (e.g., power to issue subpoenas), and classified access/need to know considerations bring some aspects of the nation's cybersecurity closer to the ambit of "inherently governmental," and hence less susceptible to public-private partnering. The CSC Final Report itself discusses at least one specific example, wherein current laws impede victim companies from effectively "stalking" the cyber-stalker, or at least identifying such bad actors in defending their assets. United States Cyberspace Solarium Commission, Final Report, March 2020, *supra* note 2, 104 (https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkfl0MxIXJGT4yv/view). Notwithstanding the law enforcement and classification functions which fall closely if not squarely within the ambit of "inherently governmental," *Wired Magazine* flags another function many consider "inherently governmental," to include the collecting, counting, and recording of election votes. This article recounts the extraordinary collaborative efforts now and for more than a decade underway, in what may prove to be the most promising voting technology breakthrough since the late 19th century, when voter privacy was enshrined as a top priority, but at the cost of sacrificing another pivotal public interest value—transparency, and one's ability to confirm that his/her vote was actually counted. Harnessing Microsoft Research, a mammoth, private sector replica of DARPA, every American voter, using a homomorphically encrypted voting scheme, may soon be able to validate his/her vote without compromising the privacy of that vote. *See* "Lone Star—A More Perfect Election" *Wired Magazine*; (October 2020), https://www.wired.com/story/dana-debeauvoir-texas-county-clerk-voting-tech-revolution/.
14. Indeed, as we enter the eighth month of the COVID-19 pandemic, private sector assumption of aspects of cybersecurity have become more important than ever. As Committee Chairman Langevin noted in his July 17, 2020, opening statement during the House Hearing on the CSC, almost from the beginning "nearly half of employed adults became teleworkers, adding stresses on our infrastructure and creating new opportunities for hackers to wreak havoc." *See* Cyberspace Solarium Commission Testimony Before the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation of the Committee on Homeland Security of the U.S. House of Representatives, July 17, 2020, *supra* note 4.
15. *See also* Pulitzer-prize winning author Neil Sheenan's 2009 book *A Fiery Peace in a Cold War: Bernard Schriever and the Ultimate Weapon*, which provides an extraordinary account of the public-private development of the ICBM, under the general (sometimes even direct and personal) supervision of President Eisenhower, who many times spoke directly with then Colonel (and later 4-star Air Force General) Schriever.
16. NASA Transition Authorization Act, 2017, https://www.congress.gov/bill/115th-congress/senate-bill/442/text.
17. In particular, in Section 302, Congress reaffirms "its commitment to the use of a commercially developed, private sector launch and delivery system to the ISS for crew missions [and] the requirement that NASA shall make use of US commercially provided ISS crew transfer and crew rescue services. Section 702 of the same bill declares NASA "shall partner with ... private industry ... as appropriate," while in Section 825 it states, "NASA shall work across all (its) mission directorates to evaluate opportunities for the private sector to perform services." Ibid.
18. Kristen Eichensehr, "Public-Private Cybersecurity," *Texas Law Review*, 2017, *supra* note 5, 494.
19. U.S. Cyberspace Solarium Commission, Final Report, March 2020, *supra* note 2, 101 & 105.
20. Two very recent attacks by Iran against Israel underscore this vulnerability. On April 24 and 25, 2020, Iranian hackers were linked to attempted cyberattacks aimed to disrupt water supplies in at least two Israeli locations- attacks Israel Water Authority employees detected and quickly alerted Israel's cybersecurity agency, https://www.washingtonpost.com/national-security/intelligence-officials-say-attempted-cyberattack-on-israeli-water-utilities-linked-to-iran/2020/05/08/f9ab0d78-9157-11ea-9e23-6914ee410a5f_story.html. U.S. Cyberspace Solarium Commission, Final Report, *supra note 2*, 62, https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkfl0MxIXJGT4yv/edit.
21. The British government has already recognized the threat, establishing the National Cyber Security Centre in October 2016; the NCSC provides a single point of contact between industry and government to offer advice, guidance, and support on cybersecurity, including management of cybersecurity threats, https://www.ncsc.gov.uk. *See also* H.R. McMaster's "Battlefields," and the General's discussion of Finland's National Cyber Security Centre, and Estonia's cybersecurity initiatives following Russia's 2007 cyber attacks, "which now include high-functioning e-government infrastructure, digital identity, mandatory baselines, and a central system for identifying and responding to attacks." Ibid., 74-75.
22. Department of Defense Cyber Strategy Summary, 2018 (https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF), 4.

NOTES

23. Ibid., 3-5, committing DoD to "streamline [its] public-private information-sharing mechanisms and strengthen the resilience and cybersecurity of critical infrastructure networks and systems." Ibid. at 4. Interestingly, this Cyber Strategy pledges that the Department "will hold DoD personnel and our private sector partners accountable for their cybersecurity practices and choices." Ibid., 5.
24. John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232.
25. United States Cyberspace Solarium Commission, Final Report, March 2020, https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view, *supra* note 2, 105.
26. Ibid., 5.
27. Ibid., 4.
28. Executive Office of the President, Office of Management and Budget, *Circular No. A-76*, August 1983 (most recently revised 2003).
29. Kirsten Eichensehr, "Public-Private Cybersecurity" *Texas Law Review*, 2017, *supra* note 5 (emphasis added, *citing* OMB Circular No. A-76). *See* the Federal Activities Inventory Reform (FAIR) Act of 1998, P.L. 105-270. The FAIR Act directs Federal agencies to issue each year an inventory of all commercial activities performed by federal employees. The OMB reviews each agency's commercial activities inventory and consults with the agency regarding content. Upon the completion of this review and consultation, the agency is required to transmit a copy of the FAIR Act Inventory of Commercial Activities to the Congress and make it available to the public. The FAIR Act then establishes a limited administrative challenge and appeals process under which an interested party may challenge the omission or the inclusion of a particular activity on the inventory as a commercial activity. Inherently governmental functions are also codified in the Federal Acquisition Rules Subpart 7.5 ("Contracts shall not be used for the performance of inherently governmental functions").
30. *See* Executive Office of the President, Office of Management and Budget, *Circular No. A-76*, August 1983 (most recently revised 2003), *supra* note 28.
31. *See, e.g.*, "Inherently Governmental Functions and Department of Defense Operations: Background, Issues, and Options for Congress," Congressional Research Service, July 22, 2009, https://fas.org/sgp/crs/misc/R40641.pdf, *passim.*
32. Former University of California, Los Angeles, School of Law, now University of Virginia School of Law Professor who is cited throughout this paper.
33. Kristen Eichensehr, "Public-Private Cybersecurity," *Texas Law Review*, 2017, *supra* note 5, 519. While we do not disagree with these three important points, the infeasibility of the first suggestion, and the likely over-regulation inherent in the second suggestion give us some pause; the third—describing threats to individual privacy—should give all of us considerable pause. A cyber 9/11 event no doubt would revisit the nation's approach to these public law valuations like a bombshell.
34. Ibid.
35. Over time, even these governmental functions increasingly are becoming blurred -for example with the use of private security firms such as Blackwater and Triple Canopy, and extensive use of private arbitrators and mediators in lieu of court proceedings.
36. Executive Office of the President, Office of Management and Budget Circular No. A-76—Revised Supplemental Handbook, *Performance of Commercial Activities*, 1999, 57.
37. Ibid.
38. *See, e.g.*, Jim Chen, "A Framework of Partnership," *The Cyber Defense Review*, Spring 2020.
39. Kristen Eichensehr, "Public-Private Cybersecurity," *Texas Law Review,* 2017, *supra* note 5, 481-82.
40. While aspects of CSC's deliberations and reporting were classified, CSC's overriding effort was to provide an open and publicly accessible report, fully explaining its 82 recommendations.
41. The Competition in Contracting Act of 1984 (CICA), 41 U.S.C. 253, generally governs competition in federal procurement contracting by requiring eligible contracts to be entered into after "full and open competition through the use of competitive procedures."
42. "New Definition of 'Inherently Governmental Function' Affects Government Insourcing Decisions," *National Law Review*, September 24, 2011, https://www.natlawreview.com/article/new-definition-inherently-governmental-function-affects-government-insourcing-decisions.

NOTES

43. Sebastian Sprenger, "Defense News," https://www.defensenews.com/30th-annivesary/2016/10/25/30-years-future-combat-systems-acquisition-gone-wrong/.
44. Federal News Network, https://www.google.com/amp/s/federalnewsnetwork.com/cybersecurity/2020/09/turn-over-on-the-cmmc-advisory-board-continues/amp/.
45. Kristen Eichensehr, "Public-Private Cybersecurity," *Texas Law Review*, 2017, *supra* note 5.
46. Jim Chen, "A Framework of Partnership," *The Cyber Defense Review,* Spring 2020, *supra* note 38, 18.
47. U.S. Cyberspace Solarium Commission, Final Report, March 2020, https://www.solarium.gov/report.

Jack Voltaic®: Bolstering Critical Infrastructure Resilience

Major General Robin L. Fontes
Major Erik Korn
Lieutenant Colonel Doug Fletcher
Major Jason Hillman
Lieutenant Colonel Erica Mitchell
Major Steven Whitham

ABSTRACT

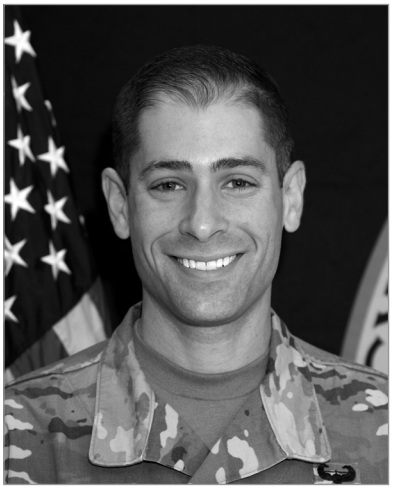
According to the Department of Homeland Security (DHS), municipal critical infrastructure has become an ideal target for a range of cyber threat actors including near-peer competitors seeking geopolitical gains and decentralized cyber criminals attempting to hold cities captive for monetary gain.[1] With municipalities predominantly partnering with the private sector for operation of national critical infrastructure as defined in Presidential Policy Directive (PPD) 21, cities, states, and industry entities find themselves on the front lines—possibly the first line of defense—against a perpetual barrage of attacks in cyberspace.[2] Accordingly, a dynamic shift from traditional conflict in the physical world to a homeland defense posture in cyberspace reveals several potential gaps with regard to handling emergency situations, coordinating response efforts, and restoring basic services for citizens.[3] This article seeks to highlight this dynamic environment, and the inherent gaps that exist in bolstering critical infrastructure resilience. Accordingly, the Jack Voltaic® (JV) research framework discussed in this article explores the interconnections among municipal, state, and federal response efforts during a cyber emergency scenario, with added emphasis on critical findings and themes from its Jack Voltaic® 2.5 workshop series. This effort brought together key regional stakeholders from across various levels of governance, the private sector, and academia to discuss the findings of previous JV exercises, lessons learned, and how similar efforts can strengthen critical infrastructure, community resilience, and a whole-of-nation approach to handling cyber threats.[4] This article will highlight common findings and themes from multiple exercises and workshops that further reinforce current JV research and the Jack Voltaic® 3.0 Legal and Policy Tabletop Exercise (TTX). Finally, this article concludes with a detailed discussion about JV 3.0, which is scheduled to execute in September 2020.

Keywords *– Jack Voltaic®, Resilience, Critical Infrastructure, Defense Support of Civil Authorities, Defense Support to Cyber Incident Response, Defender 2020, Multi-Domain Operations.*

Major General Robin L. Fontes has served as Deputy Commanding General (Operations), U.S. Army Cyber Command, since December 2019. She graduated from the U.S. Military Academy at West Point, N.Y., in May 1986 and commissioned as a second lieutenant in the Military Police Corps. During her career, she has served in a number of command, staff, and joint positions. She has commanded at all levels from a company to the Combined Security Transition Command-Afghanistan. Maj. Gen. Fontes has completed five operational assignments in Afghanistan, including four tours supporting OPERATION ENDURING FREEDOM and one tour in support of OPERATION FREEDOM'S SENTINEL. She has earned a Bachelor's degree from the U.S. Military Academy, Master's degrees in International Affairs from the University of Washington and National Security and Strategic Studies from the National Defense University.

SCENE SETTER

An international crisis in Europe prompts the U.S. President to order the rapid deployment of two brigade combat teams as a show of force in support of US allies. Tensions remain high at home and abroad as similar threats arise on both fronts. Forces are needed immediately, and any delay further harms US and NATO interests. US and NATO adversaries begin an immediate cyber assault on domestic critical civilian-owned infrastructure at first, but attacks quickly spread to critical NATO port cities as well. Gas pipelines rupture and transmission nodes are disrupted, causing interruption in fuel distribution.[5] *Widespread power outages lead to mass disruption of public utilities,*[6] *overloading of municipal medical systems, and civil unrest. Social media and news outlets report on these catastrophes, exacerbating negative public sentiment. Traffic systems become overloaded,*[7] *bringing vehicles to a standstill across strategic port cities and thus delaying access to the ports. Emergency operations centers at the municipal and state levels are unable to deal with this myriad of crises. Governors activate their state National Guard units in response to emergency declarations. Agency directors and Defense Coordination Officers become overrun with support requests from every region. Meanwhile, cargo manifests for rail and load plans at the ports are manipulated, causing incorrect heavy equipment loads. Some ships partially overturn in port*[8], [9]*; commercial and military shipping is blocked along the east coast.*[10] *Military equipment is delivered to the wrong destination and becomes significantly delayed. Garrison Commanders lose visibility of their personnel and equipment and cannot reach local authorities for resolution. Combatant Commanders around the world are faced with the responsibility of responding to adversaries, not knowing where their equipment is or when it will arrive. The Federal Bureau of Investigation and Department of Homeland Security commit teams to investigate and mitigate these local disasters. However, by the time it is understood that this is a coordinated cyberattack and force projection operations resume, the US has failed to respond in a timely manner, resulting in strategic disaster.*



Major Erik Korn is a U.S Army Cyber Officer serving as a Research Scientist at the Army Cyber Institute (ACI) at the United States Military Academy (USMA). Erik attained a B.S. in Comparative Politics from USMA in 2009, and an M.P.A. from Columbia University School of International and Public Affairs (SIPA) in 2018. MAJ Korn has previously served in a variety of operational Military Intelligence (MI) and Cyber assignments, including Brigade Collection Manager, ISR Platoon Leader, MI Company Executive Officer, Cyber Mission Commander, and Cyber Company Commander. He currently serves as a member of the ACI's Critical Infrastructure Key Resources (CIKR) Research Team, as well as the Jack Voltaic® 3.0 Data Collection and Analysis Lead. Erik also serves as a co-Course Director for the USMA Department of Electrical Engineering and Computer Science (EECS) IT460 Cyber Policy, Strategy, and Operations course, and faculty advisor for the cadet Cyber Policy Team.

INTRODUCTION

As outlined in the U.S. Cyber Command (USCYBERCOM) Command Vision, the globally interconnected digital nature of cyberspace and continuing proliferation of technology makes critical infrastructure a prime target for a multitude of persistent cyber threats.[11] With over 85% of US critical infrastructure owned and operated by the private sector, threats to the homeland are no longer across oceans or borders; they persistently reside within the domestic critical systems that American citizens depend on for basic services, safety, and security.[12] Cyberattacks in the form of denial of service, ransomware, and phishing are just some of the methods that can deliver debilitating effects against vulnerable critical domestic systems.[13] Increasingly sophisticated attack techniques and porous defenses within the US together make plausible a scenario in which a private company stands as the first line of defense against an attacking nation state. According to a recent December 2019 report, cyberattacks against local governments are reaching "critical" mass, citing as many as 948 municipalities, school systems, and health care providers reporting impacts by just ransomware alone.[14] Moreover, early decisions made by affected entities may set precedent for national response, and even in some ways constrain it. Recognizing the urgency of this growing threat, the Army Cyber Institute (ACI) at West Point launched the Jack Voltaic® (JV) research series aimed at studying critical infrastructure vulnerabilities in collaboration with industry and local government stakeholders to improve resiliency in interdependent systems from the bottom-up.

BACKGROUND

JV is the ACI's research project that focuses on the study of critical infrastructure resiliency and public-private partnerships, as well as municipal cyber incident response, recovery, and remediation efforts. In addition to supporting increased critical infrastructure

Lieutenant Colonel Doug Fletcher is a U.S. Army Operations Research Systems Analyst Officer currently serving as a Senior Research Scientist at the Army Cyber Institute at the United States Military Academy. Doug attained a B.S. in Applied Mathematics from the United States Military Academy in 1997, an M.S. in Applied Mathematics from the Naval Postgraduate School in 2007, and his Ph.D. in Statistics from Temple University in 2019. He is currently the project lead for Jack Voltaic® 3.0, a research event into how cyberattacks against commercial critical infrastructure impact Army force projection. Doug's current research interests include exercise design, statistical learning, and generalized linear modeling.

resiliency, this initiative also works to better inform our understanding of the nation's dependence on local governance and civilian critical infrastructure, specifically potential impacts on force projection capabilities in the event of local disruption. The JV concept grew from the energy sector's efforts in developing cyber mutual assistance, supporting sector coordination and resourced responses to major cyber incidents.[15] JV expands this concept across multiple sectors of critical infrastructure as a result of the interconnected nature of cyberspace, creating both sector-specific and multi-sector dependencies. Whereas most federal efforts aim at improving resiliency focus on regional or multi-state emergency response, JV takes a unique approach by focusing on the city level, where the density of both critical infrastructure and population is greatest. This bottom-up approach identifies key stakeholders and public-private partnerships, experimental design elements, governance hierarchies, exercise simulations, and relevant data collection points to elucidate critical insights regarding existing gaps, vulnerabilities, and successes of cyber incident response.[16] These unique bottom-up perspectives thus personify the critical need for integrating security considerations into incident response at all levels, and thereby helps to codify real-world cyber emergency response efforts to alleviate confusion during the heat of a real crisis.

The ACI began this effort in 2016 with Jack Voltaic® 1.0. In partnership with Citigroup, this event brought together private sector, federal, state, and local government stakeholders to simulate a "Cyber Worst Day" scenario in which key segments of New York City's critical infrastructure became severely degraded as a result of a cyber incident. This iteration of JV featured both adversary and friendly response network engagements in a simulated environment in parallel with a key leader tabletop exercise (TTX). The two-day event in New York City involved 25 organizations and 137 participants from 6 different critical infrastructure sectors: Financial Services, Emergency Services, Communications,

Major Jason Hillman is a Cyber Strategist and Research Scientist for the Army Cyber Institute at West Point. He also serves as an instructor in the U.S. Military Academy's Electrical Engineering and Computer Science Department. Jason graduated from West Point with a B.S. in Systems Engineering in 2005 and earned an M.S. in Cybersecurity from Webster University in 2018. His military service includes serving at increasing levels of responsibility starting at the tactical level as a platoon leader, up to and including Deputy Chief of Operations for Combined Security Transition Command - Afghanistan. Jason's primary research focus at ACI is critical infrastructure resilience. He maintains the following military skills and industry certification: Strategic Planner (6Z), Joint Planner (3H), Joint Cyber Operations Planner (3K), Space Enabler (3Y), Certified Information System Security Professional (CISSP).

Healthcare, Energy, and Transportation Systems.[17] In addition to establishing critical partnerships among the ACI, New York State, and New York City (NYC), it also helped NYC create a new cybersecurity agency, the New York City Cyber Command (NYC3).[18] The key findings from the first iteration emphasized the importance of a rehearsed city-level response plan nested within the state and federal response. While there are existing means at the federal and state level to enable cyber preparation, prevention, and response, it remains imperative that cities also develop, practice, and support their own cyber incident response.

The second iteration of JV took place with the city of Houston in partnership with infrastructure company Architecture Engineering Construction Operations and Management (AECOM) and Cybersecurity firm Circadence, again focusing closely on the study of potential gaps in resilience, emergency municipal coordination, and appropriate incident response. Jack Voltaic® 2.0 sought to expand on the previous iteration through exploration of a cyberattack following the occurrence of a devastating hurricane. Furthermore, by including elements in the scenario that affected the port of Beaumont, TX, this iteration of JV explored impacts on the Army's ability to deploy forces in defense of the nation due to a physical incident and cyberattack on a large American port city. JV 2.0 consequently assisted in establishing critical partnerships between government and industry, thereby enabling new Army public-private partnerships to take shape. JV 2.0 provided numerous findings and lessons learned, resulting in its inclusion in the 2019 National Defense Authorization Act Section 1649 as a method to assess and analyze critical infrastructure resiliency.[19] Two key findings of JV 2.0 furthered multi-level government cyber incident response. First, policy and legal authorities at the federal and state levels should be reviewed and adjusted to enable and complement cyber incident response at the city level.[20] Furthermore, current physical and cyber incident response frameworks require a review from

Lieutenant Colonel Erica Mitchell is the Critical Infrastructure and Key Resources (CIKR) Research Group Chief for the Army Cyber Institute and Assistant Professor in the Electrical Engineering and Computer Science Department at the United States Military Academy (USMA) at West Point. She graduated from West Point with a B.S. in American Legal Systems, was commissioned as a Signal Corps officer, and later transitioned to an Information Systems Management Officer (FA26B). She earned an M.S. in Information Systems Management, C.A.S. in Information Security Management, and Ph.D. in Information Science and Technology from Syracuse University. Her military service includes serving at increasing levels of responsibility, starting at the tactical level as a platoon leader, up to and including project management on DoD-level enterprise technology programs. Her main research focus at ACI is critical infrastructure resilience. She is a member of ACM and ISC2 and maintains the CISSP certification.

city to state to federal ("bottom-up") to allow the most flexibility in response to the rapidly evolving threat of cyberattacks.[21] In addition to these critical insights on cyber incident response, the second iteration of JV further illuminated the importance of civil and commercial critical infrastructure for the U.S. Army and helped guide additional research focus areas for Jack Voltaic® 3.0.[22]

While exercises in JV 1.0 and 2.0 produced findings and insights that support improved critical infrastructure resiliency, there are also other complementary events that contribute to achieving the overarching series objectives. These events highlight unique stakeholder insights on authorities, mitigation, and remediation that together identified a need for building municipal incident response frameworks capable of simultaneously addressing both cyber and physical incidents; this includes "cross-border and city-state-National Guard cooperation" that can further facilitate cyber personnel and capability resource sharing across existing structures.[23] In addition to planning workshops that support a specific exercise, a series of smaller one-day city-focused JV 2.5 workshops provided individual cities an opportunity to learn from the Jack Voltaic® research series, discuss how those findings apply to their environment, and improve partnerships across local sectors.

FINDINGS AND RECOMMENDATIONS

1. Crisis management and remediation is personality driven.

While the original research thesis centered around establishing structural lines of communication to mitigate personnel changeover, comments from participants and observations during Jack Voltaic® events have led to a contrary broader and somewhat different conclusion. Rather than just documenting lines of communication to draw upon during an actual crisis, it became apparent that individuals from disparate

Major Steven Whitham is a cyber warfare officer serving as a research scientist at the Army Cyber Institute. MAJ Whitham graduated with a B.S. in Computer Science from the United States Military Academy at West Point in 2009 and M.S. in Computer Science from the University of Washington in 2018. He is currently the lead scenario designer for the Jack Voltaic® research project. His research areas of interest include machine learning, artificial intelligence, cybersecurity, and exercise design.

organizations primarily rely on those they know. Rather than fight this tendency, organizations can better encourage familiarity among individuals and groups through regularly hosted events to build essential interpersonal and professional bonds for cyber incident response. Encouraging key personnel from distinct organizations, especially those in municipal emergency management, to attend these events is critical to improving communication across sectors and will ultimately lead to enhanced resilience. We recommend municipalities place strong emphasis on developing personal relationships and exchanging contact information during emergency preparedness drills in addition to practicing response actions and organizational responsibilities.

2. Individuals and organizations tend to lack experience with real cyber events and thus have difficulty visualizing second-, third-, and fourth-order effects; this inhibits a true understanding of interdependencies among organizations.

Municipalities, private companies, and other critical stakeholders typically conduct self-contained drills that unintentionally gloss over second-, third-, and fourth-order effects, ultimately detracting from a more complete understanding of the impacts to their organizations and subsequent interdependencies. During JV workshops, participants were able to identify the immediate impacts that cyber events would have on their organizations but generally lacked the ability to extend that impact to other interdependent entities. Full understanding of interdependencies is difficult to imagine in advance, but without exception participants in JV workshop events commented on learning about how much their organizations truly rely on other sectors, and how much other organizations relied on theirs. Participants from local government who participated in the planning for a full Jack Voltaic® scenario also remarked how the act of simply coming together for a planning workshop was a huge boon for them, raising interrelated

issues they had never thought to consider and introducing participants to key personalities, even within the local area. We recommend crisis management drills incorporate as broad a set of interested parties as possible from public and private sectors, at all levels of responsibility. Additionally, we recommend moderators for such drills allow time for participants to exercise creativity in considering how effects and responses to events may cause ripple effects, especially in prioritizing resources during incident response.

3. Municipalities and private entities tend to lack cyber policies, whether specific frameworks or as annexes to existing crisis management policies, and too often treat cyber incidents as information technology concerns.

Accordingly, when cyber incidents lead to physical events, existing crisis management documentation does not specify thresholds beyond the most extreme events and appear insufficient to handle situations wherein the causes of problems (cyber or mechanical) are not immediately known. Emergency management and incident response must therefore start including cyber as one of its critical components. Cyber intrusions are predominately considered an information technology (IT), not operational, problem at numerous levels of governance. Leaders often fail to recognize that the operation and maintenance of IT systems is a discipline and skill set unto itself. IT professionals may share underlying technical knowledge with IT security professionals, but their expertise and focus areas are dramatically different. This gap is further exacerbated with respect to operational technology (OT), the systems which undergird industrial infrastructure. Our JV workshops highlight a shortfall in understanding the full scope of threats to municipal critical infrastructure that currently exist with respect to building both IT and OT resilience. Leaders of organizations must stop treating cyber intrusion as a purely IT problem and begin treating it as an operational problem. Cities also tend to lack adequate cyber response policies in the form of specific documentation or as annexes to existing crisis management policies. This gap highlights the necessity of these critical stakeholders having these important conversations during events like JV in order to identify, discuss, and address previously siloed response actions that do not address important security considerations across sectors, community lifelines, and critical organizations. Additionally, even after including cyber events into existing crisis drills, incorporating effective measures, and resourcing them can take years for full maturation. We recommend organizations and municipalities incorporate scenario events into their regular drills designed to exploit gaps in current policy and force decision points that currently are not clearly defined.

4. Municipalities and organizations generally do not know what resources are available or who provides them during a cyber event; this results in hesitancy to declare a cyber incident.

Cyber incidents are by nature more difficult to identify than physical events, especially when a cyber intrusion causes a physical event. Federal and state resources are available across the country to assist with cyber incidents, but these resources may be slow to arrive if

it takes time to ascertain cyber intrusion as a cause. This can lead to a situation where those municipalities that have the greatest need for support lack the initial resources to determine what factors qualify them to request it. Exacerbated by the reality of our previous finding regarding policies, municipality emergency response personnel are often reluctant to claim a cyber incident is occurring, even at cyber resilience workshops, because their policies do not allow for such a declaration without higher approval. Local government and private sector participants at workshops were often surprised to learn that resources were available from entities like DHS, or that some states have extended their State Emergency Assistance Compacts to include cyber incident response. Federal-level cyber exercises tend to be held at state and regional levels, attempting to provide the greatest support to the biggest area. Unfortunately, this tends to leave municipality personnel unaware of available cyber resources. We recommend municipality drills include scenario events designed to exhaust locally available resources due to effects from cyber incidents, thus forcing participants to make resource requests and establish important lines of communication with supporting entities.

CONCLUSION AND WAY FORWARD WITH JACK VOLTAIC® 3.0 EXECUTION

The next full iteration of this research framework will occur with Jack Voltaic® 3.0, planned for September 2020. In concert with industry, municipal, and academia partners, the ACI will continue to study local response efforts during a multi-sector and multi-location cyber incident. This JV iteration will specifically focus on the cascading impacts of a cyberattack against municipal critical infrastructure, and how this affects the Army's ability to deploy and project forces. The third iteration of this study is currently finalizing plans and will occur as a completely distributed event in September 2020 with both the cities of Charleston, South Carolina, and Savannah, Georgia.

The JV3.0 exercise remains focused on examining and analyzing the impact of a cascading cyber incident delivering a range of effects against municipal critical infrastructure, the same critical infrastructure upon which the nation depends for its force projection capabilities. US port facilities exemplify one such critical infrastructure on which the Army depends on for force projection. A recent cyber incident in December 2019 resulted in 30 hours of degraded operations at a single maritime facility, demonstrating just how much damage can be inflicted with the occurrence of a similar cascading event occurring at multiple port facilities.[24] Accordingly, outlined research objectives for this iteration remain focused on building resiliency from the bottom-up, while also studying consequent impacts on the nation's ability to quickly move soldiers, equipment, and supplies to an active and potentially hostile area of operations (AO). As such, concerted efforts were made to nest earlier JV 3.0 events with the Army's DEFENDER-Europe 2020 exercise, the largest exercise covering deployment from the US to Europe in over 25 years.[25] This exercise will consequently bring together municipal, county, state, and federal stakeholders, along with critical members of industry and academia, to continue building comprehensive and holistic domestic critical

infrastructure resilience. Jack Voltaic® 3.0 will therefore focus on examining the following targeted research objectives:

- Exercise multiple cities in emergency cyber incident response, both for ensuring public services and safeguarding critical infrastructure.
- Reinforce a "whole-of-community" approach in response to cyber events through sustained multi-echelon partnerships across industry, academia, and government.
- Examine the coordination process for providing cyber protection capabilities in support of Defense Support of Civil Authorities (DSCA) requests.
- Develop a repeatable and adaptable framework that allows cities to exercise its response to multi-sector cyber incidents.
- Examine how cyberattacks on civilian critical infrastructure impact force projection.

Through these mutually supporting objectives, JV3.0 remains committed to building domestic critical infrastructure resiliency, facilitating partnerships, addressing gaps, codifying interdependencies, reinforcing holistic and comprehensive solutions to cyber incident response, and better enabling a whole-of-community approach. These factors not only ubiquitously affect force projection capabilities, but also directly impact the safety, security, and resilience of the American people. In a time characterized by Multi-Domain complexities within an emerging operational environment, defense of the homeland remains a paramount function of this effort.[26] The National Security Strategy (NSS) further reinforces this function, specifically highlighting the importance of critical infrastructure resiliency as a crucial facet of national protection, capabilities, and defense efforts; this includes deterring and disrupting malicious cyber threat actors from inflicting "catastrophic or cascading consequences."[27] Accordingly, the Jack Voltaic® Research Series seeks to facilitate comprehensive solutions, reinforce a whole-of-nation approach, and adequately address persistent challenges within this interdependent threat landscape that increasingly includes US homeland municipalities.

NOTES

1. "Secure Cyberspace and Critical Infrastructure," Department of Homeland Security, October 24, 2019, https://www.dhs.gov/secure-cyberspace-and-critical-infrastructure.
2. "Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience" (The White House, February 12, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.
3. Erica Mitchell, et al., "Jack Voltaic Critical Infrastructure and Public-Private Partnerships," *ACI Technical Reports*, July 18, 2019, 20-29, https://digitalcommons.usmalibrary.org/aci_rp/42.
4. "Jack Voltaic® 2.5: Cyber Workshop Series" (The Army Cyber Institute, 2019), https://cyber.army.mil/Portals/3/Documents/JackVoltaic/Jack%20Voltaic%202_5%20InfoSheet_v4.pdf?ver=2019-08-20-153840-620.
5. Kate O'Flaherty, "U.S. Government Issues Powerful Cyberattack Warning As Gas Pipeline Forced Into Two Day Shut Down," February 21, 2020, https://www.forbes.com/sites/kateoflahertyuk/2020/02/19/us-government-issues-powerful-cyberattack-warning-as-gas-pipeline-forced-into-two-day-shut-down/.
6. Brian Barrett, "An Unprecedented Cyberattack Hit US Power Utilities," *Wired* (Conde Nast, September 7, 2019), https://www.wired.com/story/power-grid-cyberattack-facebook-phone-numbers-security-news/.
7. Eduard Kovacs, "Critical Vulnerability Could Have Allowed Hackers to Disrupt Traffic Lights," *SecurityWeek*, June 5, 2020, https://www.securityweek.com/critical-vulnerability-could-have-allowed-hackers-disrupt-traffic-lights.
8. Ken Munro, "Sinking a Ship and Hiding the Evidence," Pen Test Partners RSS, February 18, 2019, https://www.pentestpartners.com/security-blog/sinking-a-ship-and-hiding-the-evidence/.
9. Tara Seals, "Researcher: Not Hard for a Hacker to Capsize a Ship at Sea," *Threatpost English Global,* threatpost.com, February 20, 2019, https://threatpost.com/hacker-capsize-ship-sea/142077/.
10. Alex Johnson, "After 'Pure Horror' of Rescue, Authorities Ponder What to Do with the Golden Ray," NBCNews.com (NBCUniversal News Group, September 11, 2019), https://www.nbcnews.com/news/us-news/after-pure-horror-rescue-authorities-ponder-what-do-golden-ray-n1052216.
11. "Command Vision for US Cyber Command: Achieve and Maintain Cyberspace Superiority" (U.S. Cyber Command, June 14, 2018), 6, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.
12. "Critical Infrastructure Protection, Information Sharing and Cyber Security," U.S. Chamber of Commerce, November 24, 2013, https://www.uschamber.com/issue-brief/critical-infrastructure-protection-information-sharing-and-cyber-security.
13. "The 16 Sectors of Critical Infrastructure Cybersecurity," *Cipher* (blog), October 10, 2017, https://cipher.com/blog/the-16-sectors-of-critical-infrastructure-cybersecurity/.
14. Sarah Nelson, "Report: Local Gov Cyberattacks Reach Critical Level," Government Technology, December 18, 2019, https://www.govtech.com/security/Report-Local-Gov-Cyberattacks-Reach-Critical-Level.html.
15. Jonathon Monken, Fernando Maymi, Dan Bennett, Dan Huynh, Blake Rhoades, Matt Hutchison, Judy Esquibel, Bill Lawrence, and Katie Stewart, Cyber Mutual Assistance Workshop Report, Pittsburgh, PA: Carnegie Mellon University Software Engineering Institute, 2018, available from https://resources.sei.cmu.edu/asset_files/SpecialReport/2018_003_001_513596.pdf.
16. Mitchell et al., 9.
17. Joseph W. Pfeifer, "Preparing for Cyber Incidents with Physical Effects," *The Cyber Defense Review* 3, no. 1 (2018): 28.
18. Charlie Mitchell, "'Jack Voltaic': Army Cyber Institute Initiative Seen Driving Security Improvements at City Level," *Inside Cybersecurity,* February 18, 2020, https://insidecybersecurity.com/share/10926.
19. Mitchell et al., 5.
20. Mitchell et al., 29.
21. Mitchell et al., 19.
22. Mitchell et al., 15.
23. Natasha Cohen, "Cyber Incident Response and Resiliency in Cities: How Partnerships Can Be a Force Multiplier," New America, Last Updated on February 21, 2019, 4, https://www.newamerica.org/cybersecurity-initiative/reports/cyber-incident-response-and-resiliency-cities/.
24. "Marine Safety Information Bulletin" (United States Coast Guard, December 16, 2019), 1, https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/MSIB/2019/MSIB_10_19.pdf.
25. "DEFENDER-Europe 20 Fact Sheet" (U.S. Army Europe, February 2, 2020), 1, https://www.eur.army.mil/Portals/19/documents/DEFENDEREurope/DEFENDEREurope20Factsheet200224.pdf.
26. "TRADOC Pamphlet 525-3-1: The US Army in Multi-Domain Operations 2028" (Training and Doctrine Command, 12/6/22018), vi-vii, https://www.tradoc.army.mil/Portals/14/Documents/MDO/TP525-3-1_30Nov2018.pdf.
27. "The National Security Strategy" (The White House, December 2017), 12, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

The Cyber Defense Review

Professional Commentary

Implementing Intrusion Kill Chain Strategies

by Creating Defensive Campaign Adversary Playbooks

Rick Howard | Ryan Olson

ABSTRACT

This paper extends the work of the Lockheed Martin research team on intrusion kill chains (the identification and prevention of cyber intrusions) in 2010. The theory has languished in the network defender community not because it is not the right idea, but because most InfoSec teams do not have the resources to implement it. What has prevented the success of the intrusion kill chain strategy is a standard framework to collect the intelligence associated with specific adversaries, to share and consume that standardized intelligence with trusted partners, and then to automatically process that intelligence and distribute new prevention controls to the network defender's security stack. The adversary playbook is that framework.

***Keywords and Concepts**: Adversary Playbooks, Adversary Campaigns, Adversary Playbook Visualizations, Automatic Intelligence Sharing, Cyber Strategic Defense Initiative (Automatic Deployment of Prevention Controls), Data Islands, Defensive Campaigns, DevSecOps Automation Layers, How Big is the Adversary Problem?, Intrusion Kill Chain Analysis, Sharing Technical and Tactical Attack Details vs Sharing Strategic Defensive Campaigns*

SETTING THE STAGE

Sometime in the early 1990s, the Internet became useful to commercial enterprises, academic institutions, and government operations. Soon after, criminals, spies, warriors, and troublemakers of all sorts discovered that it might be a useful avenue through which to pursue their activities. That was about the time when it became necessary to have network defenders within all organizations dedicated to protecting the enterprise. From the beginning, security practitioners installed their own systems designed to detect and prevent the use of malicious tools by cyber adversaries. Looking back, that was shortsighted. By focusing on individual attack tools and the indicators of compromise left in their wake, with no understanding the adversary's broader goals, the network defender community was left with no way to know if their defensive plans were working. We could tell if we stopped a specific malicious tool with our defensive systems but had no idea if we prevented the success of the cyber adversary's ultimate goal.

Rick Howard is the Chief Analyst, Chief Security Officer, and Senior Fellow at The CyberWire, a cybersecurity media network. His previous jobs include the Palo Alto Networks CSO, the TASC CISO, the iDefense GM, the Counterpane Global SOC Director, and the Commander of the U.S. Army's Computer Emergency Response Team. He was one of the founding players that created the Cyber Threat Alliance, and he also created the Cybersecurity Canon, a Rock & Roll Hall of Fame for cybersecurity books. Rick holds a Master of Computer Science degree from the Naval Postgraduate School and an engineering degree from the U.S. Military Academy. He also taught computer science at the Academy from 1993 to 1999. He has published many academic papers on technology, security, and risk, and has contributed as an executive editor for two books: *Cyber Fraud: Tactics, Techniques and Procedures* and *Cyber Security Essentials*.

When the research team at Lockheed Martin published their now-famous 2010 white paper on the Cyber (Intrusion) Kill Chain®,[1] the network defender community registered a new method to defeating the cyber adversary. Instead of installing one prevention control designed to defeat a single malicious tool, we could install prevention controls designed to defeat specific adversaries at each step of their attack sequence. Today, we know that hackers and hacker groups must string a series of actions across the intrusion kill chain in a campaign to achieve their purpose. Our aim should not be to stop the use of one technical tool with no context about what the adversary is trying to accomplish. It should be to stop the overall success of the attacker's entire campaign.

Unfortunately, the intrusion kill chain theory languished. Most network defenders understood the importance of the concept but could not muster the resources to deploy the tactics required to implement it. We needed to extend the theory and create a framework so that network defenders could build infrastructure to support it. The adversary playbook is one of those frameworks.

ADVERSARY PLAYBOOK DESCRIPTION

An adversary playbook collates all known intelligence on the hacker group's attack sequence: tactics, techniques, indicators of compromise, attack time frame, and context about motivation as well as attribution. It provides a standard framework designed to collect cyber adversary actions across the intrusion kill chain and eases the burden of sharing that collection with other network defenders. It further facilitates the automatic consumption of that intelligence on the other end, allows the receiver to write code to absorb it systematically, and provides the means to automatically deploy new and updated security controls to their already deployed defensive posture within their DevSecOps infrastructure.

Ryan Olson is the Vice President of Threat Intelligence for Palo Alto Networks. He leads Unit 42, a team responsible for the collection, analysis, and production of intelligence on adversaries targeting organizations around the world. His area of expertise is detecting and identifying actors and groups conducting cyber-crime and cyber-espionage operations. Ryan is a contributing author to *Cyber Fraud: Tactics, Techniques and Procedure*, and the primary author of *Cyber Security Essentials*. Before joining Palo Alto Networks, Ryan served as Senior Manager in Verisign's iDefense Threat Intelligence service. Ryan is a named inventor on two patents related to malware analysis and threat intelligence collection. Ryan holds a Bachelor of Science degree in Management Information Systems from Iowa State University and a Master of Science degree in Security Informatics from The Johns Hopkins University.

The five characteristics of an adversary playbook include the following:

1. Description of a hacker or hacker group's goals.
2. Timestamp of a hacker or hacker group's campaigns.
3. Collection of tactics and techniques they employed across the intrusion kill chain using the MITRE ATT&CK® framework.[2]
4. Aggregated indicators of compromise left behind as they execute their attack sequence.
5. Intelligence data set stored in a STIX™[3],[4] object designed to facilitate automatic intelligence consumption and deployment of security controls.

PLAYBOOKS VS. CAMPAIGNS

One adversary playbook might consist of several campaigns spread out over time. Network defenders describe campaigns in three ways: campaigns attempted in the past, campaigns currently running, and campaigns running in parallel. These descriptors are important because they create the opportunity to compare and contrast adversary behavior over time. When adversaries devise an attack sequence—a campaign—and run it against a victim, they may decide to change parts of the sequence for various reasons: efficiency, prevention control avoidance, new tools, etc. When they make those changes, however, they do not change the entire sequence. They only change the bits that need adjustment. The implication then is that the bulk of prevention controls that a network defender deploys against a specific campaign will likely apply to other campaigns run by the same adversary group. Even if the adversary leverages some new zero-day vulnerability somewhere in the attack sequence, with a vulnerability that nobody has ever heard about before, network defenders will have a good chance of preventing the adversary from being successful because of the other prevention controls already deployed against this playbook will still work.

Collecting all campaigns into an adversary playbook also facilitates the assessment of any new attack sequences. If the InfoSec team already knows which prevention controls it has in place for campaign one, when campaign two emerges, the task of evaluating whether the organization is vulnerable to the new campaign becomes easier. The team already knows what it has in place and can make decisions regarding how fast to respond to any new tactics. If the change in campaign two bypasses the already deployed defensive controls from campaign one, that is a higher priority than if the bulk of prevention controls are still valid.

How Many Active Playbook Campaigns Are Hackers Running on the Internet?

Since adversary playbooks contain every tactic and technique for specific attack sequences in various campaigns, network defenders can answer some important Critical Information Requirements (CIRs).[5] For example, one useful CIR asks how many tactics and techniques of all known adversaries are there? Another is how many adversary campaigns are hackers running on any given day? The InfoSec community already has a good answer to the former—and a decent estimate for the latter.

MITRE researchers have been collecting and documenting attacker tactics and techniques across the intrusion kill chain since 2013.[6] As of this writing, they are currently tracking 12 tactics and 330 techniques.[7] Of course, these numbers change over time as the researchers refine their collection mechanisms and develop insight into the problem space. The striking fact is how low the number is. Because of the volume of cyberattacks that are public knowledge these days, it seems like threat actors utilize millions of techniques to break into systems. In reality, hackers reuse a handful of tried and true techniques because network defenders have failed to deploy prevention controls against them. Malicious actors, therefore, do not need to create millions of new techniques. The old ones work just fine.

The answer to how many adversary campaigns hackers are running on the Internet on any given day is an estimate, and like the number of tactics and techniques out there, the number is likely smaller than expected. The Cyber Threat Alliance is a group of ~28 cybersecurity vendors who share adversary playbook information.[8] Their Algorithms and Intelligence Committee is staffed by some of the brightest intelligence minds in the commercial sector. For the past four years, their estimate of the volume of live adversary campaigns on the Internet on any given day has been under 250.[9] Unit 42 is Palo Alto Networks' Threat Intelligence Team, and for the last two years, it has been publishing adversary playbooks for public consumption. As of this writing, it has published ~22 adversary playbooks, which include ~50 campaigns. The observations by the Cyber Threat Alliance and Unit 42 estimate with 95% confidence that the number of active campaigns attackers are running on any given day is between 50 and 250.[10]

The InfoSec community has been treating the problem with the opposite assumption: that the volume of live attack sequences is so large, we cannot possibly keep up with it. If adversaries are running fewer than 250 campaigns every day that uses the same 330 techniques, then the conventional wisdom is completely wrong. It is possible for the community to keep up with ac-

tive attack campaigns. It is possible to deploy prevention controls more rapidly than the adversary can develop new tactics. The obstacles that prevent us from doing so are not about scale but about a willingness to share known adversary's attack sequences with our peers, along with the difficulty of automating the response once we have that intelligence. We designed adversary playbooks to facilitate the latter.

For the former, there are two schools of thought in the network defender community that mostly align with the policies of government cyber intelligence groups and everybody else. For government intelligence groups, their mission is more significant in that they are trying to help government leaders influence the international political and security environment. For everybody else, we are just trying to prevent material impact on our organizations. The differences between the two are stark. For the government side, some of the intelligence they collect comes from espionage operations. As such, they have a vested interest in protecting their sources and methods. For everybody else, most of the intelligence collected is from one's network and sharing partners, and it makes sense to share with trusted partners as efficiently as possible. For the government, it makes sense to support that sharing so that they do not have to give up their sources and methods.

One argument against sharing is that if adversaries discover what the network defenders know about them, then they will change their attack sequence, but that is the point of efficiently sharing threat intelligence. Instead of the network defender community scrambling to react to every newly discovered technical technique, we want to cause the adversaries to expend additional resources attempting to find new attack techniques that work. The key is agility in sharing new intelligence quickly and deploying new security controls to our infrastructure with speed and efficiency. The adversary playbook model supports that concept.

PLAYBOOK DATA ELEMENTS

Playbooks consist of two types of data: observables and context. Observables are digital objects or clues left behind by the adversary that give network defenders notice that there might be an intruder. We find them on all the data islands where our employees operate: on laptops and mobile devices inside the traditional perimeter and out in public, on servers within data centers, on SaaS (software as a service) supporting infrastructure, and on various public cloud infrastructures that provide PaaS (platform as a service) and IaaS (infrastructure as a service). Finding these observables on these data islands means that an attacker either executed an attack sequence in the past or is busy executing one currently. Context is intelligence derived from the observable. In other words, what do analysts know—or what can they assume—when they find an observable?

Consider the information included in Table 1. It lists the observables and derived context that one team of network defenders witnessed during an unsuccessful attack campaign by a hacker group we call DragonOK. By derived context, we mean that InfoSec analysts observed a malicious email arriving in an employee's inbox with the subject, "Your Purchase Order," and assumed that

the attackers used spear-phishing as their delivery mechanism. They found the malicious Word document with its unique hash, "020f5692b998...," and derived that the attackers leveraged a known vulnerability, "CVE-2015-1641," for their exploit code. They observed the portable executable file, "12d88fbd4960...," and derived its name, "Nflog," and its function, a remote access tool (RAT). Finally, the analysts recorded the command and control domain name, "www.dppline[.]org," and derived that the attackers used the standard HTTP communications protocol for command and control purposes.

Table 1. Adversary Playbook Data from a Single Attack by the DragonOK Threat

Intrusion Kill Chain Phase	Data
Delivery	Observable: "Email Subject: Your Purchase Order"
	Context: TTP: Spear Phishing
Exploitation	Observable: Sample – Word Document: 020f5692b998...
	Context: Exploited Vulnerability: CVE-2015-1641
Installation	Observable: Sample – Portable Executable: 12d88fbd4960...
	Context: Malware Name: Nflog
	Context: Malware Type: Remote Access Trojan
Command and Control	Observable: Domain Name: www.dppline[.]org
	TTP: Standard Application Layer Protocol – HTTP

Intrusion Kill Chain Analysis to Support a Defensive Campaign

A domain name that malware uses to support its command and control function is an observable. This kind of intelligence is valuable for blocking a specific attack technique and for "connecting the dots" between two separate attack sequences when adversaries reuse tools and infrastructure. Unfortunately, the time-to-live period of this observable is often short. Once the network defender community becomes aware of it, an attacker will stop using it. Alternatively, the higher-level "context" data elements within an adversary playbook are much longer lived, but they may not be as valuable to network defenders in defeating the attack or creating a defensive campaign.

Analyzing the data from the table above, network defenders might decide to block traffic destined to the associated command and control domain name, www.dppline[.]org, preventing malware already inside the network from communicating with the attacker. This is certainly a worthwhile action to take, but it will likely be a temporary solution. Once the attackers behind DragonOK notice that no traffic is coming into their server, they will probably change their command and control server to a different domain. Advanced adversaries change their command and control domains on a regular and automated cadence anyway to prevent this specific defensive measure. A longer-term action would be to deploy the Microsoft patch for

"CVE-2015-1641." This would prevent future attacks by DragonOK and other adversary groups who exploit the same vulnerability. Still, it would not prevent DragonOK from further actions along the intrusion kill chain spectrum if they were already inside. Neither of these defensive tactics offers a robust defensive campaign against DragonOK. This is the reason for intrusion kill chain analysis. The act allows network defenders to find gaps in their defensive posture against specific adversaries.

Let us examine the same data in another way. Figure 1 shows us the DragonOK attack techniques and their corresponding intrusion kill chain phases.

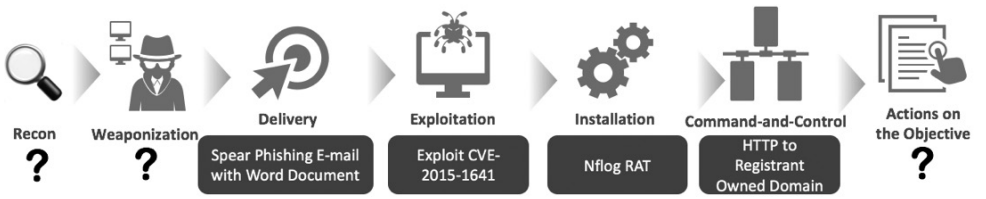


Figure 1. Intrusion kill chain view of a DragonOK attack

This view makes it more apparent that we are missing some elements of the attack. Based on our observations of a single attack, we only have information about four of the attack sequence phases. Of course, the goal of building an adversary playbook is not to look at a single attack, but at all the attacks attributed to the same adversary. The adversary playbook identifies past tactics and techniques and those likely to be used in the future. If other organizations that have observed attacks from DragonOK share additional data with us in the same format, we can build a complete picture (Figure 2).

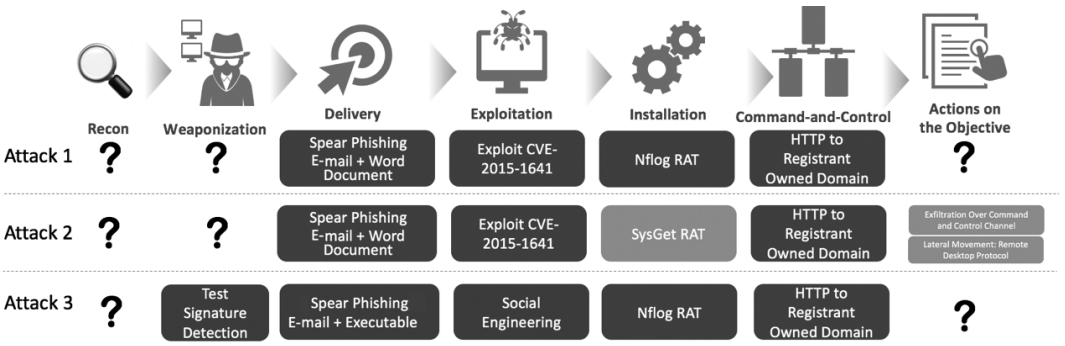


Figure 2. Attack sequence view of three DragonOK playbooks

This picture in Figure 2 remains incomplete, but now we know more about the DragonOK adversary playbook. Attack 2 indicates this attack sequence uses a different remote administration tool (RAT), called SysGet, during the installation phase, compared to Nflog in Attack 1 and tells us more information about what the attackers do once they breach a network. Attack 2 indicates, in the "Actions on the Objective" column, that the attackers exfiltrate data over a command and control channel and move laterally within the victim's network using the

Remote Desktop Protocol (RDP). Attack 3 shows us more ways the threat actor delivers its malware and how it might evade antivirus protection. In the "Delivery" column of Attack 3, the attackers use spear-phishing to deliver malicious code. Then, as shown in the "Exploitation" column, they use social engineering to trick the victim into running that code. Visualizations of other adversary playbooks can be found at the Unit 42 Playbook Viewer site.[11]

If a single group of network defenders, operating alone, observed Attack 1, its options for preventing the success of DragonOK in its networks would be limited and likely would not work. By combining and sharing the intelligence gathered by other network defender groups for other DragonOK campaigns, however, the entire InfoSec community could build a more robust defensive campaign specifically designed to thwart the DragonOK playbook.

We designed these visualizations for two purposes: we wanted to help analysts understand the value of grouping adversary intelligence into playbooks, but more importantly, we designed the playbooks to be readable by a machine to facilitate the network community's automatic sharing of this intelligence.

ADVERSARY PLAYBOOK DESIGN: THINGS TO CONSIDER

Table 2 shows a summary of the DragonOK attack information in a tabular form. This version of playbook information, boiled down to the essentials for automatic consumption, is not long

Table 2. Tabular Form of DragonOK Playbook

Adversary: DragonOK	
Recon	UNKNOWN
Weaponization	UNKNOWN
Delivery	• Spear Phishing with Word Attachment • Spear Phishing with EXE Attachment
Exploitation	• Exploit Known Vulnerability – CVE-2015-1641 • Social Engineering
Installation	• Tool: Nflog • Tool Type: Remote Administration Tool (RAT) • Tool: SysGet • Tool Type: Remote Administration Tool (RAT) • Tool: IsSpace • Tool Type: Remote Administration Tool (RAT) • Tool: TidePool • Tool Type: Remote Administration Tool (RAT)
Command and Control	• Standard Application Layer Protocol
Actions on Objectives	UNKNOWN

or particularly verbose. Human analysts who try to read this information will likely find it wanting. That is why it is essential to include reference material, which gives more detail on

named elements. For instance, intelligence analysts might like to share the discovered DragonOK remote administration tools: NFlog and SysGet. Providing reference links to this more detailed information is not essential to automatic intelligence sharing, but it is useful for developing a more robust picture of adversary behavior.

One of the significant barriers that has inhibited intelligence sharing from the beginning[12] is that the network defender community could not agree on a standard language or format to transfer the information. Common sense dictates that to facilitate information exchange, network defenders must agree on what to call things. If one person uses the term "Keylogging" to describe capturing keys pressed on a keyboard, but another uses the broader term "Input Capture," the entire network defender community could be talking about the same attack technique, but nobody would know.

This is where MITRE's Adversarial Tactics, Techniques, and Common Knowledge model and framework come in.[13],[14] MITRE ATT&CK includes hundreds of techniques in a Wiki-like format (Figure 3) to provide names, descriptions, and links to examples of adversaries using specific tactics inside an organization's networks.

Figure 3. ATT&CK description of the spear-phishing attachment technique

The tabular format of the playbook in Table 2 is closer to something a machine can read as compared to the intrusion kill chain diagram shown in Figures 1 and 2, but what we need to be able to exchange this information is a machine-readable format.

PLAYBOOKS IN STIX

There have been many efforts to build a common language to facilitate information sharing from both the open-source and commercial communities. In recent years, though, the network defender community seems to have embraced STIX™ (Structured Threat Information eXpression)

to be, at least, the common language to which all others must talk. This is evident by the fact that the most famous and well-respected information sharing organizations—like the Financial Sector Information Sharing and Analysis Center (FS-ISAC), the Cyber Threat Alliance, the Defense Industrial Base Information Sharing and Analysis Organization, IBM, and Palo Alto Networks, to name a few—have all adopted it.[15]

STIX allows for the exchange of many forms of threat intelligence, from a simple list of IP addresses to descriptions of assets involved in an incident. With an adversary playbook, our goal is associating adversaries with the tactics and techniques they employ at specific phases of the intrusion kill chain. Three core elements in STIX are necessary for encoding information for an adversary playbook.

The "Threat Actor" element is the characterization of a specific adversary. It does not need to include identifying information about individual actors, but it does need to include a consistent code name or identifier that one can associate with this adversary. The Threat Actor element is what lets the recipient know with which adversary the remaining elements should be associated.

"TTPs" (tactics, techniques, and procedures) are representations of what an adversary does when it conducts its attack. Does it scan the Internet looking for hosts that are vulnerable to an SSH, or does it send targeted spear-phishing email messages to your CFO? STIX allows broad descriptions of TTPs, but to be incorporated into a playbook, we suggest a predefined set of descriptions like those in MITRE ATT&CK be used.

STIX 1.2 does not have a mechanism to specifically reference MITRE ATT&CK TTPs, but they can be included by adding custom fields or by overloading the included Common Attack Pattern Enumeration and Classification (CAPEC) reference to point to MITRE ATT&CK TTP identifiers instead. MITRE has already created MITRE ATT&CK definitions for TTPs STIX 2.0. (see STIX 1.x vs 2.x box).

Indicators convey specific observable patterns in STIX. They tell us what to look for in our networks and on our endpoints when we are trying to identify an attack. STIX 1.x uses the CybOX (Cyber Observable eXpression) standard for defining specific types of observables, but STIX 2.x has incorporated these observables directly into the standard.

Whether STIX 1.x or 2.x is chosen to encode playbook data, the elements described above are the minimum you need to include when building a package for exchange. Details about the impact of an intrusion or the types of organizations targeted are valuable, but the Threat Actor, TTP, and Indicator data are critical.

Why Do We Need Adversary Playbooks?

We designed the adversary playbook to make it easier to share threat intelligence with trusted partners in a meaningful and efficient way. We also designed it to reduce the impediments of automatically processing that intelligence on the receiving end, allowing network defenders to make decisions faster than the hacker. By adopting the adversary playbook construct, cyber

intelligence practitioners can leverage actionable intelligence in a machine-readable format designed for the activities that follow.

Intelligence Collection and Capture. Generally, all intelligence teams are unique, regardless if they work in similar industries or government sectors. Team size, financial resources, organizational mission, and the boss's CIR (Commander Information Requirements)[16] all contribute to team uniqueness. This is one of the main reasons it has taken so long to develop a universal standard format for storing cyber intelligence. For cyber intelligence teams, the adversary playbook provides an industry-accepted format to store raw information on adversary behavior across the intrusion kill chain in a manner that is easily shared with other cyber intelligence teams.

Intelligence Distribution. To see a mostly complete view of the elephant (i.e., a comprehensive view of adversary activity), it is incumbent upon intelligence teams to swap information on adversary attack sequences in real time with trusted partners. Combining the intelligence with that of two or more trusted partners fills in the gaps of what one intelligence team knows. Distributing that intelligence to them in a machine-readable format allows those partners to process it automatically for their use without having to dedicate humans to the endeavor.

Intelligence Consumption. Intelligence teams consume threat intelligence products from trusted sharing partners in a format and language that facilitate automatic processing. The value of information sharing is thus realized because InfoSec teams can concentrate on more strategic tasks, like designing defensive campaigns or updating defensive campaigns for all known cyber adversaries, instead of manually crunching through written reports in documents, slide decks, spreadsheets, and emails.

DevSecOps Security Control Deployment. Network defenders understand the value of the DevSecOps infrastructure-as-code philosophy. They know it is imperative that whatever processes and procedures their DevOps teams pursue, they should go right along with them in a "shift left" kind of way. Security is one of the operational silos that the DevOps movement is designed to strike down. However, after years of advocating for a DevOps or DevSecOps vision, Gene Kim, author of several DevOps books, says:

> [I]ncredible problems still remain. In other words, someone could embrace fully all the principles and patterns espoused in *The Phoenix Project* (a book about the DevOps philosophy listed within the Cybersecurity Canon Hall of Fame[17]) … but I think one of the problems is that there is still all these … invisible structures required to make developers productive.[18]

For network defenders, one set of invisible structures prohibiting automatic response is unformatted intelligence products. They cannot very well automate their response to incoming intelligence if a human is required for each piece. Once intelligence products come into the organization in an understood and agreed-upon framework, it becomes possible to automatically deploy prevention controls to the organization's deployed security infrastructure. This goal has

been out of reach in the InfoSec community, but with the adoption of adversary playbooks as a best practice, the community can start to move toward achieving it. DevSecOps security control deployment becomes achievable now.

Defensive Campaign Design and Deployment. As intelligence teams share and consume more information on adversary campaigns over time, the operational picture of how the adversary operates on the Internet becomes more apparent. It is possible to design a comprehensive defensive campaign tailored to a specific adversary playbook within the network defender's DevSecOps infrastructure. InfoSec teams design these defensive campaigns to defeat the adversary's ultimate objective. In terms of material impact, there is a sizable difference between an adversary group compromising a single laptop on the victim's network as a key step in its attack sequence and that same group succeeding in exfiltrating customer data that might eventually materially impact the victim's organization. It is not enough to only try to stop the former. It is desired but insufficient. InfoSec teams must be successful at preventing the latter, and the design of all defensive campaigns must reflect that. The technology needed for network defenders to accomplish these goals is not yet ready. The first step is for all of us in the network defender community to adopt the adversary playbook concept as a common language to communicate what we know about the adversary's purpose.

Figure 4 shows a potential future model of cyber conflict represented by three color tones: light - security infrastructure and protected data, dark - network defender actions, and medium - adversary actions. The labeled arrows show in which direction information and action flow. The key on the right provides additional details.

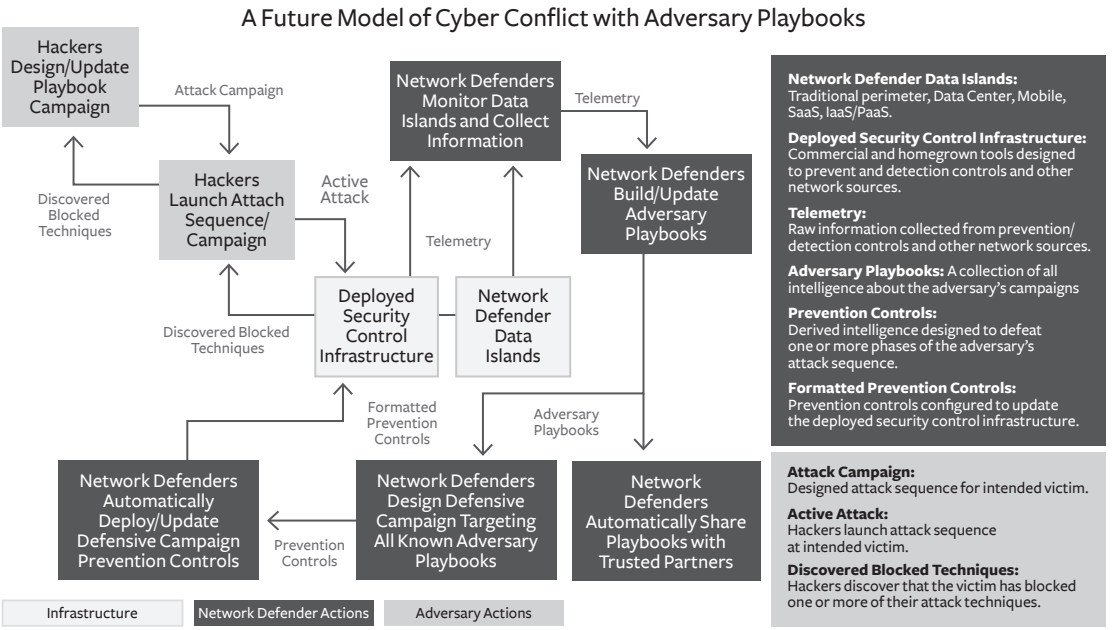


Figure 4. Model utilizing adversary playbooks in cyber conflict

The model shows that whichever side has the most agility will win. If hackers can deploy their attack campaigns more rapidly than network defenders can deploy their prevention controls, they will likely succeed. Conversely, if network defenders can collect telemetry, organize it into adversary playbooks, share those playbooks with their trusted partners, design defensive campaigns to thwart them, and deploy those defensive campaigns on their existing infrastructure faster than the hackers can act, then the network defender will likely succeed in preventing material impact to their organization due to cyberattacks. The network defender's only hope of being more agile than their cyber adversaries is to automate the deployment of prevention controls to the already-deployed security control infrastructure. To be specific, network defenders need four automation layers in their DevSecOps infrastructure:

1. **Adversary Playbook Consumption**—the ability to automatically consume adversary playbook intelligence products from their trusted sharing partners.
2. **Adversary Playbook Sharing**—the ability to share internally derived adversary playbook intelligence products automatically with their trusted sharing partners.
3. **Defensive Campaign Staging**—the decisions of the InfoSec team about how to thwart the adversary playbook efficiently at each phase of the intrusion kill chain and staging that information in a way that facilitates automatic deployment.
4. **Defensive Campaign Deployment**—leveraging the defensive campaign staging area by automating the deployment of security controls to the network defender's already-deployed security control infrastructure.

Building defensive campaigns and supporting automation layers has the added benefit of helping network defenders identify the gaps and redundancies in their prevention control toolset. If the intelligence team discovers that, after it completes its intrusion kill chain analysis, there is no way to stop the successful completion of the adversary's ultimate mission, this might indicate that the organization needs another prevention tool. Likewise, after the InfoSec team has deployed and maintained several defensive campaigns, it may discover some security tools within their DevSecOps arsenal that are not often used or are redundant controls for a specific phase of the attack sequence. That might be an indicator that the organization has too many tools deployed.

The industry-standard MITRE ATT&CK framework has shown us that the number of techniques used by hackers is under 400.[19] By collecting the techniques of all known hacker groups, intelligence teams can see which techniques are used most often. If the bulk of hacker groups mostly use the same handful of techniques repeatedly, the InfoSec teams could prioritize their defensive campaigns on those techniques first. For instance, the four adversary playbooks in Figure 5 identify the same hacker technique in the Exploitation phase of the attack sequence. Building defensive campaigns that prevent this exploit from working protects the organization from four different adversary groups at once.

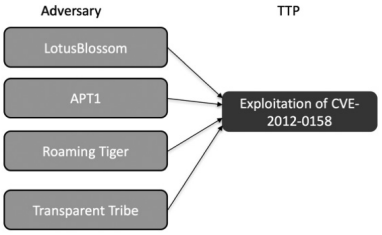


Figure 5. Multiple adversaries use the same TTP

Product managers behind many commercial security tools designed them to be successful against various adversary tactics and techniques. For example, security vendors created commercial off-the-shelf (COTS) spam tools to thwart adversaries from using email as a delivery tool. Others created anti-exploitation tools to prevent adversaries from using exploitation techniques on the endpoint. Deploying these commercial tools and updating them with the latest response based on new intelligence serves as the basis for all network defender prevention programs. Analyzing the aggregate hacker playbooks will provide network defenders insight into what kinds of tools they will need. Figure 7 demonstrates that all network defenders need some anti-exploitation tool.

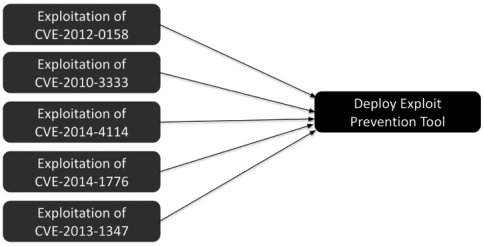


Figure 6. One defense may be effective against multiple TTPs

Additionally, by building playbooks for your top 10 (or more) adversaries and evaluating their tactics and techniques against your possible defenses, you can identify which technologies, processes, or policies will have the most impact on defending your organization from the significant threats you face. Figure 7 demonstrates that it might be possible for the InfoSec team to reduce the myriad of adversary tactics and techniques to a handful of generic defenses as an added layer to defensive campaign strategies.

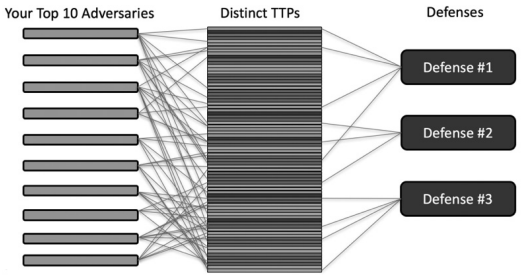


Figure 7. Identifying overlap between your top adversaries, their TTPs and your defenses

CURRENT STATE

Unit 42[20] did the initial work on adversary playbook development some five years ago. They brought that work to the Cyber Threat Alliance[21] when the security vendor intelligence-sharing group was just forming. The adversary playbook concept is baked into the Cyber Threat Alliance's DNA. Members share adversary playbook intelligence products so their common customers do not have to do it themselves. They have become a collection of trusted sharing partners. Because they are security vendors, when they receive the daily intelligence from the other vendors, they develop prevention controls for their own product sets and deliver them to their customer base. Aside from this handful of security vendors, no one else in the network defender community has adopted the adversary playbook concept as a best practice yet, and no one has come close to building defensive campaigns for all known adversary attack sequences. There is still much work to be done.

Figure 5 shows a potential future model of cyber conflict. To carry out this vision, the network defender community must transform its approach from manually responding to cyberattacks to embracing the philosophy of the DevSecOps model. The community has to get comfortable with automated responses to cyberattacks. It also must let go of the notion that InfoSec teams should respond to technical threats observed on their networks without consideration for the cyber adversaries' objectives.

NEXT STEPS

To achieve the vision of the DevSecOps model, the network defender community should pursue the following short-term activities:

- **Join the Cyber Threat Alliance.** Each of us in the network defender community already has a set of commercial security vendors we use to defend our data islands. The Cyber Threat Alliance is nonprofit organization working to improve the cybersecurity of the global digital ecosystems by enabling high-quality cyber threat sharing among companies and organizations. We must educate the network community regarding the benefits of the Cyber Threat Alliance. Even if our organization does not now have the resources to work toward this vision internally, using security vendors that do will spread the adversary playbook as a best practice within the community. The Cyber Threat Alliance has the added benefit of putting the burden on each security vendor to deploy prevention controls designed to defeat all known adversary attack sequences. This is one way we can promote and encourage the standard.
- **Encourage Government Organizations and Standards Bodies to Adopt the Adversary Playbook Model.** Whenever possible, urge government entities in charge of national cyber policy and government InfoSec teams to adopt adversary playbooks as a best practice.

- **Build and Share Adversary Playbooks with Trusted Partners.** If your organization is not sharing cyber intelligence with a trusted partner, find one. Make it your business to determine how your organization can make the adversary playbook model a reality in your organization. Find ways to share your internally developed adversary playbooks with your security vendors, especially if they are members of the Cyber Threat Alliance.
- **Encourage the Information Sharing and Analysis Centers (ISACs) to Adopt the Standard.** If you already belong to an information-sharing group, like the ISAC for your business sector, encourage the group's leadership to adopt the adversary playbook standard too. Find a way for your ISAC membership not only to share adversary playbooks with themselves but also to share their adversary playbook intelligence products with the Cyber Threat Alliance. In this way, the ISAC helps its members enhance their DevSecOps projects and helps vendors provide prevention controls to the products that their members already use.
- **Support and Adopt the MITRE ATT&CK Framework Standard.** For your intelligence efforts, use the MITRE ATT&CK framework to develop a universal standard for the community.[22],[23]
- **Support the Oasis Standards Group for STIX.** The Organization for the Advancement of Structured Information Standards (OASIS) is a nonprofit, international consortium that manages the open-source standards for STIX.[24] We believe the OASIS STIX standard is the way forward for future DevSecOps work.
- **DevSecOps Automation Layers.** Start building your own DevSecOps infrastructure to support these layers: Adversary Playbook Consumption, Adversary Playbook Sharing, Defensive Campaign Staging, and Defensive Campaign Deployment.

CONCLUSION

The network defender community began their work in the 1990s by trying to prevent, or at least, detect, the tools that cyber adversaries were using to penetrate their networks. That was short-sighted. Instead of trying to stop individual tools used with no context about what the adversary was trying to accomplish, we should have been trying to stop the success of the adversary's campaign. The famous 2010 Lockheed Martin white paper on the Cyber (Intrusion) Kill Chain® gave us the means. It advocated for the defeat of the entire adversary's campaign by deploying prevention and detection controls at every stage of the attack sequence. Currently, the commercial security vendor community believes there are fewer than 250 active campaigns at any one time, which is not a large problem space. What has prevented the success of the intrusion kill chain strategy is a standard framework to collect the intelligence associated with specific adversaries, to share and consume that standardized intelligence with trusted partners, and then to automatically process that intelligence and distribute new prevention controls to the network defender's security stack. The adversary playbook is that framework.

NOTES

1. Eric Hutchins, Michael Cloppert, and Rohan Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Lockheed Martin Corporation, 2010, accessed May 19, 2020, https://lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf.
2. "MITRE ATT&CK® Navigator," MITRE, accessed November 5, 2019, https://mitre-attack.github.io/attack-navigator/enterprise/.
3. John Wunder, "STIX 2.0 Finish Line," MITRE Blog, April 12, 2017, https://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-blog/stix-20-finish-line.
4. "Introduction to STIX," Oasis, accessed May 19, 2020, https://oasis-open.github.io/cti-documentation/stix/intro.
5. Major Michael Barefield, "Commander's Critical Information Requirements (CCIR): Reality Versus Perception," School of Advanced Military Studies, United States Army Command and General Staff College, Fort Leavenworth, Kansas, 1992-1993, https://apps.dtic.mil/dtic/tr/fulltext/u2/a264509.pdf.
6. Chris Brook, "What is the MITRE ATT&CK Framework?" Data Insider, DigitalGuardian, October 24, 2019, https://digitalguardian.com/blog/what-mitre-attck-framework.
7. "MITRE ATT&CK® Navigator," MITRE.
8. "Our Sharing Model," Cyber Threat Alliance, accessed October 7, 2020, https://www.cyberthreatalliance.org/our-sharing-model/.
9. Conversations with Cyber Threat Alliance (CTA) leadership from 2014 to 2019.
10. Ibid.
11. Playbook Viewer, Unit 42, Palo Alto Networks, accessed November 5, 2019, https://pan-unit42.github.io/playbook_viewer/.
12. "Sharing Timely, Relevant and Actionable Intelligence Since 1999," FS-ISAC, accessed November 5, 2019, https://www.fsisac.com/who-we-are.
13. "MITRE ATT&CK® Navigator," MITRE.
14. Brook, "What is the MITRE ATT&CK Framework?"
15. "Products," OASIS, accessed November 5, 2019, https://wiki.oasis-open.org/cti/Products.
16. Barefield, "Commander's Critical Information Requirements (CCIR).
17. "Cybersecurity Canon: A Rock and Roll Hall of Fame for Cybersecurity Books," sponsored by Palo Alto Networks, accessed December 20, 2019, https://cybercanon.paloaltonetworks.com/.
18. Mark Miller, "The Unicorn Project with Gene Kim—a transcription of the DevSecOps Podcast, recorded October 16, 2019," The DevSecOps Podcast Series, October 16, 2019, accessed December 20, 2019, https://cdn2.hubspot.net/hubfs/4132678/DSO%20Days%20-%20Transcriptions/The%20Unicorn%20Project%20with%20Gene%20Kim%20-%20DevSecOps%20Podcast%20Series%20Transcription.pdf.
19. "MITRE ATT&CK® Navigator," MITRE.
20. Conversations with CTA leadership, 2014–2019.
21. "Our Sharing Model," CTA.
22. "MITRE ATT&CK® Navigator," MITRE.
23. "MITRE ATT&CK®," MITRE, accessed December 20, 2019, https://attack.mitre.org/.
24. "OASIS Cyber Threat Intelligence (CTI) TC," by OASIS, accessed December 20, 2019, https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti.

The Cyber Defense Review

Research Articles

Cyber Maneuver and Schemes of Maneuver

Preliminary Concepts, Definitions, and Examples

Dr. Patrick D. Allen

ABSTRACT

This article is intended to stimulate discussion among cyber warriors and others about an approach to cyber maneuvers at the operational level. Cyberspace is one domain in what is commonly called "Multi-Domain Operations," while movement and maneuver is one of the warfighting functions in U.S. Army doctrine. This sets the context for a proposed approach to a concept for offensive and defensive cyber maneuver operations that starts with a goal or mission, and allows preparation of the commander's intent via a scheme of maneuver. The scheme of maneuver includes a sequence of *categories of maneuver*, which in turn are accomplished by specific cyber (or non-cyber) maneuver actions or fires, thereby connecting the mission to the scheme and categories of maneuver, and then to specific actions and fires. Effectiveness of specific cyber actions and fires will change over time, but the categories of maneuver and their intent are much more enduring. Commanders using this approach do not need to be "techies" to define a cyber scheme of maneuver. So long as the commander has, or has been provided, sufficient understanding of operational-level tradeoffs and effects of offensive and defensive cyber maneuvers, the staff can provide the technical details.

PURPOSE

Commanders currently provide an overarching intent to their operations orders. As cyberspace operations increase in frequency and importance, the commander's intent should consistently include cyber operations as part of their scheme of maneuver. This article will hopefully stimulate discussion among United States cyber warriors and others and provide preliminary examples that enhance operational-level cyber maneuver doctrine by

Dr. Patrick D. Allen (COL, Ret. USAR), currently an Information Operations Specialist at the Johns Hopkins University Applied Physics Laboratory, has a B.S. in Physics, an M.S. and Ph.D. in Operations Research, and a Master's in Strategic Studies. A graduate of both Army War College and Air War College, over his 40-year career, Dr. Allen has supported various organizations within the U.S. Defense and Intelligence Communities on topics including cyber, analysis, research and development, and modeling and simulation, as well as consulted internationally for Canada, the United Kingdom, and Sweden. A former Visiting Fellow at Cranfield University, UK Defence Academy, and a former Director of the Military Operations Research Society, he holds one patent and is author of two books, *Information Operations Planning*, and *Cloud Computing 101: A Primer for Project Managers*, five book chapters, and many journal articles. Readers should feel free to contact the author directly.

describing *cyber maneuvers at the operational level*, and connecting high-level doctrine to the lower-level tactics, techniques, and procedures (TTPs).

This article also seeks to explain why commanders do not need to know the technical details of specific cyber actions to create a commander's intent that includes cyber operations. All they need to do is select a principle or *category of maneuver* that accommodates the commander's intent and operational concept, as reflected in the *scheme of maneuver*. The staff then selects specific cyber and non-cyber maneuver actions or fires to accomplish the intent of each category of maneuver, and discusses any emergent issues with the commander. This helps bridge the gap between operational knowledge and objectives, and cyber knowledge and objectives, which also leads to better integration of cyber effects into operations.

CONTEXT SETTING

Commanders integrate warfighting functions into their operations. The U.S. Army defines six warfighting functions, which are suitable for the development of concepts for maneuver in cyberspace: "mission command, movement and maneuver, intelligence, fires, sustainment, and protection."[1] Maneuver, which is also one of nine principles of war,[2] is defined in Joint Publication (JP) 3-0 as "employment of forces in the operational area through movement in combination with fires to achieve a position of advantage in respect to the enemy."[3]

"Military doctrine aims at prescribing the manner in which an armed force will fight."[4] The U.S. Armed Forces are moving to multi-domain operations (MDO), which is doctrine that integrates the warfighting functions.

To summarize the main points of MDO, our adversaries are competing with the US short of conflict, using political, military, and economic means to separate the US from its partners. "The **central idea** in solving this problem is the ***rapid and continuous integration of***

all domains of warfare to deter and prevail as we compete short of armed conflict."[5] During conflict, our adversaries "will employ ***multiple layers of stand-off*** [attacks] in ***all domains—land, sea, air, space and cyberspace***—to separate U.S. forces and our allies in time, space and function in order to defeat us... ***The U.S. Army in Multi-Domain Operations 2028*** concept proposes a series of solutions to solve the problem of ***layered standoff.***"[6] "***Multi-domain formations*** possess the capacity, endurance and capability to access and employ capabilities across all domains to pose multiple and compounding dilemmas on the adversary."[7] [Text as highlighted in the original; cyberspace defined in JP 3-12.[8]]

Cyber maneuver is one proposed component of MDO, and focuses on the warfighting function of maneuver within and through cyberspace. Offensive and defensive cyber maneuvers support multi-domain operations outside of cyber, and vice versa, as part of MDO doctrine integrating the warfighting functions during both competition and conflict. This article proposes mental models and terminology to help insert operational-level cyber maneuvers into MDO.

The US and its allies devote substantial time and effort identifying and fixing their network vulnerabilities, and identifying and exploiting vulnerabilities on adversary networks.[9] While these efforts are necessary, the shifting nature of conflict requires the US to be more proactive. For example, rather than simply finding adversary vulnerabilities, offensive cyber maneuvers can be leveraged to create such vulnerabilities, and also to cause adversaries to respond in ways that create new exploitable vulnerabilities. This article explains how this in turn can support the U.S. Cyber Command's (USCYBERCOM) developing strategy that includes "persistent engagement" and "defend forward."[10]

Similarly, waiting to detect adversary activities on our own networks is reactive. More proactive cyber defensive maneuvers will allow US cyber warriors to take actions on the network that expose and act against otherwise undetected adversaries.

APPROACH

Technology by itself does not ensure victory in kinetic operations or in cyber conflict. *All conflict is primarily a battle of wits between opponents*—our minds against the minds of our adversaries. While technological advancements over an opponent are part of that competition of the minds, it is the continuous, ongoing operational application of *mental creativity and agility* over an opponent that leads to success in cyberspace.

Cyber maneuvers include the application of traditional military principles of maneuver to cyberspace and are also the actions that facilitate the achievement of maneuvering in cyberspace as described in JP 3-12. The following proposed definition of cyber maneuver will likely evolve over time based on feedback.

> Cyber maneuvers are actions taken within and through cyberspace to achieve physical, technical, and cognitive positional and temporal advantages over an adversary.

Physical advantages include physical access to friendly and adversary cyber capabilities, including through a supply chain. Technical advantages include having better cyber capabilities and methods of employment than the adversary. Cognitive advantages include, but are not limited to, having better information about a situation than the adversary, such as surprise, deception, and apparent invincibility; the ability to manipulate adversary thoughts and actions; and undermining adversary confidence. Cyber maneuvers can also help achieve non-cyber effects, while non-cyber maneuvers can help achieve cyber effects.

Physical and technical *positional* advantages include access where and when desired, thus allowing for unhindered use of cyberspace to prevail over adversaries. Cognitive *positional* advantages include gaining dominance over the minds of the adversary with respect to their views of their options, chances for success, confidence in their situation, and overall will to continue the conflict. Cognitive positional advantage superior to the adversary in cyberspace can be enhanced by coordinating Information Operations with cyber maneuvers, as described below. International public opinion, especially that of US allies, should always be factored into whether, when, and how we achieve cognitive positional advantage, to include how and when the adversary is *made aware* of the threats or results of US actions.

Cyber maneuver is much more than identifying and controlling "cyber key terrain," applying moving target defense technology, using decoys on a network, or performing lateral movement on an adversary's network. These techniques can all contribute to specific cyber maneuvers, but cyber maneuver is larger than any of these examples.

CONNECTING MISSION TO MANEUVERS

Military operations begin with a mission or goal. From the mission, commanders derive the "commander's intent," or prose description of sequential and parallel actions that will fulfill the mission. Thus, the commander's intent describes a "scheme of maneuver" for how the various types or categories of cyber maneuver will unfold.

- ***Schemes of maneuver*** define which *categories of maneuver* will be applied and in which sequence to achieve a specified mission (e.g., achieving a set of desired results).
- ***Categories of maneuver*** define the purpose, intent, and general mechanism for applying cyber capabilities, are more enduring than cyber maneuver actions or cyber fires, and are an abstraction of specific cyber actions that allows easy insertion and operational flexibility into maneuver narratives. Categories of maneuver are key to defining "mission type" orders, and are distinguished from maneuver actions and cyber fires because they include an intent that can be mapped back up to the mission's antecedent scheme of maneuver.
- ***Cyber maneuver*** actions achieve the intent of the category of maneuver they support. Maneuver actions are specific and less enduring than categories of maneuver because technology evolves, as do the countermeasures of cyberspace adversaries, who learn to

identify and counter specific maneuvers. (This article distinguishes "categories of maneuvers" from "maneuver actions" by using "maneuvers" to refer solely to the latter.)

- ***Fires*** may be cyber, physical, influence, or other actions designed to implement or facilitate cyber maneuvers. Note that physical actions and influence actions can support cyber maneuvers, just as cyber maneuvers can help achieve physical and influence actions. A specific fire may support multiple categories of maneuver, as described in the distributed denial of service (DDoS) example below.

Assembling these component definitions, the scheme of maneuver describes the commander's intent, and is constructed from categories of cyber maneuvers sequenced (or parallel) to accomplish that mission. Cyber maneuver actions and fires are then selected to fulfill the intent of each category of maneuver that supports the scheme of maneuver. Maneuver actions and fires may be cyber, physical, or influence actions taken to support a category of maneuver, as shown in the Figure below.

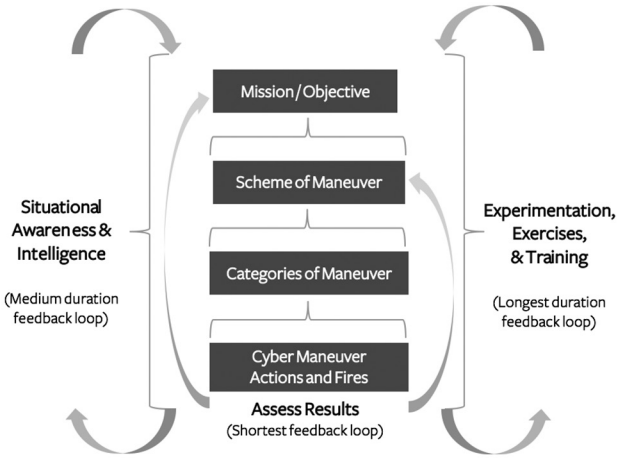


Figure 1: Components of Cyber Maneuver

As depicted above, the longest-duration feedback loop is the experimentation,[11] exercises, and training of the cyber maneuvers. The medium-duration feedback loop is driven by situational awareness and intelligence. The shortest feedback loop assesses the results of cyber maneuver actions and fires against the planned scheme of maneuver and/or the mission or objective. This Figure also highlights the dependence of cyber maneuver on sound situational awareness and intelligence, without which many maneuvers in cyberspace would be infeasible. Cyber actions are also useful in generating valuable intelligence or situational awareness to support other maneuvers.

This construct avoids many problems encountered in the cyber maneuver literature, which tends to be either too abstract or too detailed. For example, "deter" is an objective, not a maneuver, while DDoS is an action that could support, e.g., three different categories of maneuver: "delay," "distract," or "spoiling attack." An example of a "distract" intent occurred after the

series of large-scale Iranian DDoS attacks against US financial institutions. A later, much smaller, DDoS attack distracted financial institution defenders such that otherwise detectable fraudulent financial transactions actually succeeded.[12] An example of a spoiling attack is the alleged attack by USCYBERCOM against the Russian Internet Research Agency (IRA) in November 2018.[13] A single category of maneuver can include multiple cyber actions. Of these actions, any one at other times could be used for various categories of maneuver. Moreover, one category of maneuver can be used to help achieve the objectives of another category of maneuver, as described below (see section on Schemes of Maneuver).

CATEGORIES OF MANEUVER WITH EXAMPLES

This article lists twenty-one categories of maneuver in cyberspace, which will likely evolve over time. The first eleven are similar to principles of kinetic operations; the next five are similar to psychological operations (PSYOP—now called Military Information Support Operation, or MISO) principles; the last five are common hacking and counter-hacking principles. Nearly all apply to offensive cyber operations (OCO), two apply exclusively to defensive cyber operations (DCO), and more than half apply to both.

Similar to Kinetic Principles

- Ambush: Attract an adversary into a hidden "kill zone" (OCO, DCO)
- Herd: Push or Turn an adversary into a hidden "kill zone" (OCO, DCO)
- Stimulate a Response (DCO)
- Probe Adversary (OCO)
- Distract (OCO, DCO)
- Delay Adversary (OCO, DCO)
- Launch Spoiling Attack (OCO, DCO)
- Launch Supporting Attack (OCO)
- Counterattack (OCO, DCO)
- Counter Asymmetric Advantage (OCO, DCO)
- Leverage Deception (OCO, DCO)

Similar to Psychological Operations (PSYOP) Principles

- Appear Invincible (OCO, DCO)
- Undermine Adversary Confidence (OCO, DCO)
- Create False Sense of Security (OCO)
- Leverage Shifting Allegiances (OCO, DCO)
- Employ Influence Messaging (OCO, DCO)

Common Cyber Hacking and Counter-Hacking Principles

- Ensure Persistence (OCO)
- Vary Launch Points (OCO)
- Apply Social Engineering (OCO)
- Change the Terrain (or Manipulate the Network) (OCO, DCO)
- Leverage Perishability (DCO)

These categories can be used for offensive operations on adversary networks (Red space), defensive operations on friendly networks (Blue space), or in support of offensive or defensive operations in other networks not owned by us or the adversary (Gray space).[14],[15]

No single technique will work in all scenarios. No matter how successful a given technique, a countermeasure inevitably appears soon thereafter. The timing (simultaneous or sequential, and when) and flexibility of cyber maneuver schemes (if this does not work, do that instead) is what makes cyber maneuvers succeed. Similarly, no cyber maneuver technique *has* to work all the time. Sometimes, even using an unsuccessful technique can sow doubt in the minds of the target populace. For example, ineffectual Russian hacking attacks against voter registration systems in late 2018 caused substantial consternation in the US even though no Russian hacking attempt appears to have succeeded.[16]

This section provides examples of most of the twenty-one listed categories of maneuver. Again, individual maneuver actions and techniques will become more or less effective over time as cyber technologies evolve. *Categories of maneuver* and *principles of maneuver* are more enduring.

Ambush maneuvers seek to *lure* an adversary into an unforeseen "kill zone."[17] For an offensive cyber example, our forces infect both a branch and a leaf node in an adversary network. The leaf node then announces it is infected, bringing forth the adversary's network defenders, which access the infected leaf node via the branch node. Our forces infect the adversary responders' toolkit, thereby converting the toolkit into an access vector and unwitting agent of future infection. This ambush example need not always work, but its existence may distract or cause hesitation by the adversary defender, which can be the ultimate goal of the maneuver.

Herding seeks to push or turn adversary actions in a direction more desirable to the US. For example, if the US infects the less active of two "hot swap" routers, and then DDoS the more active one, the result is to *push* or *turn* the adversaries into the kill zone of an already infected router. Herding can also be applied to DCO, attempting to force adversaries away from more lucrative targets on U.S. networks.

Stimulating a response can involve a network defender changing passwords for a network segment, and watching for a previously undetected adversary seek to regain lost access—one of many actions defender can take to expose or "out" as-yet-undetected adversaries.

Probing an adversary is the offensive version of stimulating a response. The results of probing actions can provide valuable information about how an adversary defender will likely react, which can significantly contribute to achieving reflexive control[18] over the defender.

Distract and **delay** are two categories of maneuver that encompass many specific maneuver actions. As mentioned above, for example, a DDoS attack can help achieve a delay, a distraction, or a spoiling attack. Decoys can also distract or delay adversaries.

"A **spoiling attack** is a tactical maneuver that can cripple a hostile attack at the very outset, while the enemy is assembling for an attack."[19] A spoiling attack seeks to disrupt adversary momentum or preparations, which buys time, gains initiative, or disrupts adversary effectiveness.

As a cyber example, USCYBERCOM allegedly performed a form of spoiling attack against Russian influence operations days before for the 2018 elections by launching attacks against the Russian Internet Research Agency (IRA) that, according to one source, "basically took the IRA offline...They shut them down..."[20]

Cyber **supporting attack**s are designed to achieve an effect outside of cyberspace, e.g., taking down an adversary's electric power grid. Cyber warriors often operate in and through cyberspace to affect physical systems and adversary minds. Similarly, physical actions outside of cyberspace can support cyberspace maneuvers.

In the kinetic world, **counterattacks** typically are launched when the adversary is reaching its culminating point, i.e., when the attacker has extended itself geographically and expended its resources, such as ammunition, fuel, human energy and other combat resources.[21],[22] The counterattack seeks to time its attack to coincide with the adversary's most vulnerable moment, roll back any gains, and perhaps destroy its forces, and otherwise create and exploit follow-on opportunities. Identifying an adversary's culminating point in cyberspace is quite challenging. For example, bots do not get tired or run out of energy. One can "hack back" at a remote intruder, or send infected files as part of the stolen materials being exfiltrated by an adversary, but timing these actions is independent of any identifiable culminating point. Counterattack is one of our proposed categories of cyber maneuver, yet its meaning is quite different from the kinetic principle of the same name. Joint Cyberspace Operations doctrine for Defensive Cyberspace Operations-Response Actions already includes the cyber counterattack maneuver.[23]

In **countering an asymmetric advantage**, history is replete with examples of one side having an advantage (e.g., in range or firepower), yet the other side invariably adopted tactics and/or maneuvers that countered those advantages. The side with limited range and/or maneuverability chooses to fight in close-in terrain, such as urban areas (like Stalingrad in World War II), forests (like Teutoburg Forest in 9 A.D.), or mountainous terrain (like Afghanistan throughout history). Countermeasures in cyberspace follow the martial arts technique of leveraging an adversary's strength against it. For example, botnets are large and difficult to identify and

eradicate. Rather than trying to reduce the size of a botnet, render it unmanageably large, or at least so large as to make its command and control channels obvious. One potentially useful technique is to place a copy of the botnet malware on 100,000 nodes in a virtual private cloud with Internet access we control. The bots all duly report back to their C2 network, potentially swamping the C2 nodes. At the very least, the C2 node locations can be identified by the huge traffic generated by 100,000 simultaneously reporting new bots. Once the C2 nodes are exposed or overwhelmed, all nodes in the cloud can be shut down by our side, which owns them, thereby barring adversary access to a new 100,000-node botnet.

Cyberspace offers myriad ways to **leverage deception,** such as deploying decoy assets (e.g., hosts, routers, or servers), decoy users, decoy credentials, decoy traffic, and decoy content. Many commercial deception-for-cyber-defense tools are now available. For example, multi-fidelity decoy assets can effectively keep adversary intruders guessing as to what is real. Having very low-fidelity decoy nodes on the network may cause intruders to think they know what decoys look like. Learning the decoy was actually a higher-fidelity decoy should give adversaries pause. Repeats with increasingly high-fidelity decoys can cause the adversary to wonder whether a real network asset is actually authentic.

Projecting **invincibility** can seriously degrade adversary morale. In some cases, the adversary is truly helpless, such as when the Operation DESERT STORM (ODS) Coalition had air superiority over Iraqi ground forces and could bomb them at will.[24] In other cases, the invincibility may merely be an illusion. The following cyberspace example dates from when "Anonymous," in its heyday, would announce that on a certain date in the following week, nothing could be done to stop the hacking of a given target. The author is not sure if the following is what Anonymous did, but it is likely that Anonymous would have already hacked the target and planted several back doors. They could also have already downloaded materials unique to the target to prove the target was hacked, even if the target disconnected itself from the Internet. Sure enough, whenever Anonymous declared a target would be hacked, it was. Whether Anonymous really could hack any target or had already hacked the target was irrelevant, as either way, *it gave the impression of invincibility*.

Similar cyber maneuvers can be performed against our adversaries. After our forces hack a target, they let that target know it will be hacked at a specified future time, creating a "horns of a dilemma"[25] for the target. Either the adversary shuts off all outside connections, constituting a self-denial-of-service, or it maintains normal operations with increased vigilance, and risks proof of vulnerability to penetration, as forewarned.

Undermining adversary confidence shakes the adversary's confidence in its resources. During ODS, coalition forces would come up on the Iraqi military radio nets and announce coalition presence on the Iraqi nets, thereby proving it was literally operating within the Iraqi communications space.[26] These on-net announcements had a devastating effect on Iraqi morale, with lost confidence in the confidentiality, integrity, and even availability of working communications.

A similar set of cyber maneuvers can be performed, for example, by leaving messages on adversary computer screens, confirming your access to its network, along with five changes you made to that network, with each change flagged with a calling card, each confirming one of your five actions. If in reality, you made only four changes, imagine the untold consternation to the adversary, who devotes untold time trying to find and fix the phantom fifth change!

Conversely, **creating a false sense of security** gives the adversary wholly unfounded confidence in its network. For example, if we stop sending messages on adversary networks that had undermined its confidence, at the same time it took *unsuccessful* steps to end our intrusions, and it mistakenly believed its actions stopped our messages, with our forces still on its network, that adversary would have a false sense of security about its network. Note that the use of maneuvers to cause the adversary to lose confidence in its resources, followed by a false sense of security maneuver, is a good combination to employ as a pair within a scheme of maneuver. Similarly, once our forces are on the adversary's network, our forces could pretend that they have not gotten in by making obvious access attempts designed to be readily blocked.

Shifting allegiances can be leveraged at the individual, group, and national levels. In addition to causing someone to switch sides, shifting allegiances can also mean that someone or some group "shifts into neutral" for a short period of time.[27] For example, when the CIA had paid the local tribes a substantial amount of money to keep Osama bin Laden trapped in Tora Bora, bin Laden then paid the tribesmen even more money to let him pass through their lines. As a result, bin Laden escaped from Tora Bora because the Afghani tribesmen hired by the CIA "shifted into neutral" long enough for him to escape.[28]

Shifting allegiances have always been a problem historically. From individuals opening castle gates to large scale defections before or even during a key battle, empires have been lost or gained because of a timely shift in allegiance. In cyberspace, this may be as simple as "just put this thumb drive into a computer," or a longer-term campaign of convincing someone to switch sides. An example of shifting into neutral in cyberspace would be to ignore an alert or to fail to check certain logs until a specified time has passed.

Cyber maneuvers can support, and be supported by, non-cyber activities, such as **employing influence messages**. One type of influence message aimed at cyber adversaries is to misattribute a cyber action intentionally to stimulate an adversary response in Blue or Gray spaces. These misattribution messages are more likely to work against civilian criminal hackers than nation-state hackers; however, criminal hackers are often hired by nation-states to do their hacking, so this method may succeed. Messages may also be sent directly to Red space recipients informing them their identities and actions are known. USCYBERCOM allegedly sent such messages to the Russian IRA to attempt to dissuade them from further activities.[29]

Ensuring persistence, **varying launch points**, and **applying social engineering** are also standard hacking techniques and will not be further elaborated upon here.

Changing the terrain by manipulating the network works on both the defense and offense. Researchers have been working on various forms of moving target defenses for years with some success in changing memory address spaces. An alternative to just rotating IP addresses is to rotate Media Access Control (MAC) addresses, and changing the Organizationally Unique Identifiers (OUI), which are the first three octets of the universally administered address the manufacturer assigns to each device. These changes can be achieved by running a PowerShell script. The goal is to frustrate and complicate adversary reconnaissance and target identification – machines self-identifying as Dell laptops might roll their OUIs and suddenly appear on an adversary's sensors as iPhones, vulnerable IoT webcams, or Cisco firewall appliances. Note for example Operation ShadowHammer (the ASUS hack) targeted fixed MAC addresses.[30]

An offensive version of rotating MAC addresses and OUIs on an adversary's network can be part of a "moving target attack." While every adversary machine can still function, no communication between endpoints can occur for about 30-45 minutes until the Address Resolution Protocol (ARP) and Dynamic Host Configuration Protocol (DHCP) catch up and IP/MAC mapping concludes. Repeated application of this attack can keep the adversary endpoints isolated from each other for longer periods. Nothing is destroyed, making this an attractive permitted maneuver during Red Team engagements or during pre-conflict as it will likely meet rules of engagement (ROE).

The defender can also **leverage perishability** by increasing the rate of network changes. Access can be lost through normal system changes or upgrades, as well as by defender actions. Cyber techniques are perishable because evolving countermeasures and workarounds neutralize or reduce original use efficacy. "The technology upon which cyberspace is based is constantly evolving... This ongoing evolution leads to constant changes in tactics and procedures used by both attackers and defenders in cyberspace."[31] "This capability to maneuver and provide operational reach may be lost at any time if the configuration of the relevant cyberspace nodes is modified."[32]

Note that most of the maneuver actions listed in this article have yet to be laboratory tested. The article focuses primarily on the upper part of the stack illustrated above: How to connect goals to the scheme of maneuver, and to the categories of maneuver supporting the scheme of maneuver. The primary purpose of listing the component maneuver actions is to give examples, which should not be considered vetted maneuver actions.

JP 3-12, *Cyberspace Operations*, lists two main categories of cyberspace attack actions: manipulate and deny. Deny includes degrade (reduce capability to a specified level of operation), disrupt (100 percent denial for a specified period), and destroy. "Manipulate" includes changing information or information systems in Red or Gray spaces "using deception, decoying, conditioning, spoofing, falsification and other similar techniques."[33] The Table below shows that most categories of maneuver presented in this article belong to the "manipulate"

category. Only a few (spoiling attack, supporting attack, counterattack, leveraging shifting allegiances, and changing the terrain) support both "manipulate" and the three denial categories.

Table 1: Mapping the 21 Categories of Maneuver to JP 3-12 Attack Categories

Categories of Maneuver	Degrade	Disrupt	Destroy	Manipulate
Ambush: Attract to a "kill zone"				✓
Herd: Push to a "kill zone"				✓
Stimulate a Response				
Probe Adversary				
Distract				✓
Leverage Deception				✓
Delay Adversary				✓
Counter Asymmetric Advantage				✓
Launch Spoiling Attack	✓	✓	✓	✓
Launch Supporting Attack	✓	✓	✓	✓
Counterattack	✓	✓	✓	✓
Appear Invincible				✓
Undermine Adversary Confidence				✓
Create False Sense of Security				✓
Leverage Shifting Allegiances	✓	✓	✓	✓
Employ Influence Messaging				✓
Ensure Persistence				
Leverage Perishability				
Vary Launch Points				
Apply Social Engineering				✓
Change the Terrain	✓	✓	✓	✓

COMMANDER'S INTENT AND SCHEMES OF MANEUVER

> The commander's intent is a clear and concise expression of the purpose of the operation and the desired military end state that supports mission command, provides focus to the staff, and helps subordinate and supporting commanders act to achieve the commander's desired results without further orders, even when the operation does not unfold as planned.[34]

The scheme of maneuver is "the central expression of the commander's concept for operations that governs the development of supporting plans or annexes of how arrayed forces will

accomplish the mission."[35] In the preceding Figure, the commander's intent is represented within the scheme of maneuver, which includes a sequence of categories of maneuver like the ones described above. For example, if the mission is to use non-kinetic means to deter a nation from invading a neighboring US ally country, the scheme of maneuvers might be:

> Employ cyber *probing, ambushes,* and *herding* to *ensure persistent access* to the adversary network. By [specified date], launch actions to *undermine adversary confidence* in its network resources, followed by a *change the terrain* to preclude its network connectivity until [specified date]. If by this [specified date] the adversary has been deterred from invading the neighboring country, execute *create a false sense of security* on its network. If the adversary starts preparing again to invade its neighbor, execute *appearance of invincibility* maneuvers to deter their resumption of preparations.

Note that this scheme of cyber maneuver consists of a specified sequence of eight categories of maneuver (listed in italics). Which specific cyber maneuver actions and fires will be selected by the commander's staff is less important than *articulating the intent* described by the sequence of maneuver elements of the scheme of cyber maneuver. Moreover, if the intent of each category of maneuver has been approved, then the specific maneuver actions eventually selected to accomplish that intent are more likely to be approved as well.

Creating a common lexicon is important to identify clearly both the similarities and the differences among traditional military kinetic and PSYOP doctrines and cyber operations. "We should recognize when these constructs do not fit cyber and use simple, clear language to communicate."[36] "As the military continually seeks to adapt its approach to maneuvering intelligently in the cyberspace domain, it must also do the same with its practice of training cyberspace maneuver leaders." [37]

Cyber schemes of maneuvers not only should have their own synchronization matrix to coordinate and deconflict cyber elements of the operation; cyber maneuvers should also be included in the overall mission synchronization matrix across the whole force,[38] to preclude not only mission fratricide (such as cutting electrical power before broadcasting a TV message to the populace), but also fratricide among cyber maneuver elements.

A second sample cyber scheme of maneuver focuses on exposing and neutralizing adversary activity on a friendly network that will soon be used in a critical operation, the intent being to get the adversary off our networks for a specified time period–not forever.

> Increase monitoring on the network and then *stimulate a response* by changing all authentication passwords simultaneously. Watch for adversary attempts to regain access. *Leverage deception* to allow the adversary to regain access onto decoy assets to *delay adversary* regaining access and identify adversary TTPs. Simultaneously execute *delay adversary* maneuvers in identified adversary hop points and listening posts operating out of Gray space and Red space. This will increase the time the adversary needs to regain access and help identify new hop points and listening posts being used as alternative, faster routes.

A third sample cyber scheme of maneuver focuses on protecting another nation from adversary actions and eventually exposing the adversary actions on that country's networks.

> Identify adversary-compromised resources operating on another nation's networks. *Undermine adversary confidence* in its footholds on the network by feeding it false information and malware. Change the terrain by using SatCom box technology to relay more obviously the communications from the adversary to its listening posts such that the targeted nation can more easily identify the source of the adversary activities. Covertly assist the targeted nation in exposing the adversary presence on its network. In addition, *create a false sense of security* in the adversary for its implants that have not yet been exposed. When the adversary claims to have no further presence on the targeted nation's network, expose to the host nation via *influence messaging* these previously unexposed (but detected by us) adversary implants.

There are many negative effects for the adversary, such as its exposed presence (especially repeated exposed presence post-denial, which is politically damaging). Second, the adversary loses access to key networks in the targeted nation. Third, it likely will be more cautious about compromising other networks in the targeted nation for fear of a similar outcome.

Note: one category of maneuver can support another category of maneuver. For example, defensively modifying the MAC addresses is listed under the maneuver category "change the terrain," but changing the terrain can also be used to enable a deception for a defense maneuver, or a herding maneuver. The scheme of maneuver can describe these planned interactions between categories of maneuvers, to ensure the sequence of desired maneuver effects is achieved.

Overall, the mission or goal defines the objective. Then the commander's intent defines the scheme of maneuver at the level of the categories of maneuvers. The identified categories of maneuver are fleshed out by the staff with specific maneuver actions that meet the criteria to accomplish the scheme of maneuver and thereby accomplish the mission.

A key advantage of this framework is that commanders need not know all technical details of specific maneuver actions. So long as operational-level effects and tradeoffs are understood, the commander selects a category of maneuver tailored to his/her intent, and incorporates it as a component of the overall scheme of maneuver, then the gap between operational knowledge and objectives, and cyber knowledge and objectives, can be effectively bridged. This in turn should lead to better integration of cyber effects into overall operations.

NEXT STEPS

This section suggests some follow-on steps not covered in this article, and thus seeks to stimulate discussion that further fleshes out the optimal integration of the cyber domain into the overall operation and, in particular, the categories of maneuver. For example, one important

related topic not covered is how best to extend this analysis to integration of cyber actions with radio spectrum and electronic warfare capabilities within the schemes of maneuver.

Another goal is to institutionalize a lexicon for cyber maneuvers for military personnel who are more familiar with kinetic and PSYOP concepts. This in turn, should help facilitate multi-domain operations across both the physical and cyberspace domains, to include electronic warfare, and influence operations in both competition and conflict. While a shared culture of understanding of terminology does not yet exist for our cyber warriors, this article hopefully will stimulate rigorous discussion and thought as to how best we can solidify and clarify doctrine and terminology to strengthen a shared culture. This article gives an early snapshot glimpse of evolving thought on the topic at the Johns Hopkins University Applied Physics Laboratory (JHU/APL). The proposed definitions, maneuver actions, and benefits are all works in progress.

Addressing DoD's implementation of doctrine, organization, training, materiel, leadership, personnel, and facilities (DOTMLPF) issues is beyond the scope of this article.[39]

This article does not address one important consideration of conflict in cyberspace, which is being able to detect and identify adversary cyber maneuvers, and recommend counter-maneuvers designed to thwart or even exploit adversary maneuvers. The focus instead is first to facilitate agreement on formulating cyber maneuver actions, cyber maneuver categories, and schemes of maneuver. Establishing at least a preliminary set of clear definitions should prove valuable in tackling efforts to detect and counter adversary uses of cyber maneuvers.

Another important factor not addressed in this article is the need for good situational awareness (SA) and intelligence support to accomplish cyber maneuvers. The author assumes that intelligence dominates obtaining information about adversary capabilities in Red and Gray spaces, while SA dominates obtaining information about our cyber capabilities in Blue and Gray spaces. Intelligence can also be obtained directly from cyber maneuvers, such as probing actions to identify adversary responses.[40] Moreover, this paper does not address the important tradeoff issues associated with intelligence loss and gain that the staff must consider when using certain cyber capabilities. The commander obviously requires clear staff feedback whenever a potential scheme of maneuver cannot or should not be accomplished by the existing suite of available cyber actions. In addition, experiments will help determine how well these maneuvers work in a simulated environment with human opponents, as well as quantify the benefits of cyber maneuvers.

SUMMARY

This article grapples with the analysis and lexicon of commanders charged with integrating cyber domain operations into other much longer established domains of the battlefield. The article presents an approach to offensive and defensive cyber maneuvers at the operational level that starts with a goal or mission, and allows preparation of the commander's intent via a scheme of maneuver. The scheme of maneuver includes a sequence of *categories of maneuver*,

which in turn are accomplished by specific cyber (or non-cyber) maneuver actions or fires. This approach connects the mission to the scheme of maneuver, to categories of maneuver, and then to specific actions and fires. The categories of maneuver and their intent are much more enduring than specific cyber maneuvers or fires, which will evolve over time. Using this approach, commanders do not require technical expertise in order to define and execute a cyber scheme of maneuver. So long as the commander has, or has been provided, sufficient understanding of the operational-level tradeoffs and effects of offensive and defensive cyber maneuvers, the staff will provide the technical details.

This article has briefly described twenty-one categories of maneuvers, illustrated with a sample maneuver action for each, and presented three sample schemes of maneuvers. This is just the beginning. The author anticipates and welcomes additional cyber maneuvers, categories of maneuvers, and sample schemes of maneuver. Readers should feel free to contact the author directly.

DISCLAIMER

The views expressed here are those of the author and do not reflect the official policy or position of the Johns Hopkins University Applied Physics Laboratory.

ACKNOWLEDGMENTS

While Dr. Patrick Allen (COL Ret., USAR) was the initiator and primary author of this article, many Johns Hopkins University Applied Physics Laboratory (JHU/APL) staff and consultants contributed ideas, references, comments and reviews throughout the writing process. Since there were 35 other contributors and reviewers, they are listed here in alphabetical order: Natalie Anderson, Mika Ayenson, Alex Barut, Dave Bondura, Calvert "Triiip" Bowen, Bob Butler, Jamie Castle, Welton Chang, James Curbo, Matt Dinmore, Pete Dinsmore, Bud Halla, Bryon Hartzog, Kristine Henry, Mike Hostetter, Jessi Hupka, David Lachut, Alex Lee, Sue Lee, Stephen Lidard, Paul Markakis, Jennifer McKneely, Dan Meidenbauer, Rob Nichols, J. R. Parsons, Jody Patilla, Aaron Pendergrass, Doan-Trang Pham, John Quigg, Rob Schrier, Tamim Shookoor, Karl Siil, Kath Straub, Katherine Watko, and Keith Wichmann.

Brainstorming sessions were held at JHU/APL that included veterans and currently serving military reservists (from cyber, kinetic, PSYOP, and intelligence communities), staff member SMEs involved in both defensive and offensive cyber technology and operations, and staff knowledgeable in influence and Gray Zone operations. This article seeks to synthesize all preceding sources, and help discuss and the future of cyber maneuver.

NOTES

1. Army Doctrine Publication No. 3 *Operations,* ADP 3-0, para. 46.
2. "Objective, offensive, mass, maneuver, economy of force, unity of command, security, surprise, and simplicity." Joint Publication 3-0, *Joint Operations,* January 17, 2017, incorporating change 1, October 22, 2018. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf?ver=2018-11-27-160457-910
3. JP 3-0, Ibid.
4. John Whiteclay Chambers II, *The Oxford Companion to American Military History,* Oxford University Press, https://www.oxfordreference.com/view/10.1093/acref/9780195071986.001.0001/acref-9780195071986?btog=chap&hide=true&jumpTo=Do&page=14&pageSize=20&skipEditions=true&sort=titlesort&source=%2F10.1093%2Facref%2F9780195071986.001.0001%2Facref-9780195071986
5. TRADOC PAM 525-3-1 "The U.S. Army in Multi-Domain Operations 2028," December 6, 2018, Preface.
6. TRADOC PAM 525-3-1, Ibid.
7. TRADOC PAM 525-3-1, Ibid.
8. Joint Publication 3-12 Cyberspace Operations defines cyberspace as "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."
9. Aaron F. Brantly, "Strategic Cyber Maneuver," *Small Wars Journal,* October 17, 2015.
10. Paul Nakasone, "An Interview with Paul M. Nakasone," *Joint Forces Quarterly,* Issue 92, 1st Quarter 2019.
11. Robert R. Hoffman, *Cyber Defense Review,* Vol. 4, No. 1, Spring 2019.
12. Steven Musil, "Cybercrooks use DDoS attacks to mask theft of banks' millions," *CNet.com,* August 21, 2013.
13. Ellen Nakashima, "U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms," *The Washington Post,* February 27, 2019.
14. Kamal Jabbour, "The Science and Technology of Cyber Operations," *High Frontier,* (May 2009), 11.
15. Joint Publication 3-12 Cyberspace Operations, June 8, 2018, I-4.
16. Justin Lynch, "The voting day crisis election officials fear," t*he Fifth Domain,* 23 October 2018.
17. While FM 3-0 *Operations* defines an ambush as "an attack by fire or other destructive means from concealed positions on a moving or temporarily halted enemy," we modified the definition of ambush for increased applicability to cyberspace.
18. According to Tim Thomas, "Reflexive control is defined as a means of conveying to a partner or an opponent specially prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action." Timothy Thomas, "Russia's Reflexive Control Theory and the Military," *Journal of Slavic Military Studies,* 2004 17: 237–256.
19. FM 3-0, Ibid., Glossary.
20. Ellen Nakashima, Ibid.
21. Joint DoD Dictionary, "The point at which a force no longer has the capability to continue its form of operations, offense or defense."
22. Joint Information Operations Planning Handbook, January 2012, I-31 to I-32.
23. JP 3-12, II-4.
24. Al Zdon, "Persian Gulf War Ten Years Later: Winning the war by convincing the enemy to go home," http://www.iwar.org.uk/psyops/resources/gulf-war/13th_psyops.htm.
25. The phrase "horns of a dilemma" describes placing the adversary in a position of two options, where both options cause the adversary to lose something significant. B.H. Liddell Hart, *Strategy,* Praeger, New York, 1954, p. 152.
26. Zdon, Ibid.
27. Patrick Allen, "Training and Planning for Shifting Allegiances," *Royal Uniform Services Institute (RUSI) Journal,* October 2008.
28. Philip Smucker, 'How bin Laden got away: a day-by-day account of how Osama bin Laden eluded the world's most powerful military machine,' *The Christian Science Monitor,* 4 March 2002.
29. Ellen Nakashima, Ibid.

NOTES

30. Catalin Cimpanu, "Researchers publish list of MAC addresses targeted in ASUS hack," Zero Day, *ZDNet.com*, 29 March 2019.
31. Scott Applegate, "The Principle of Maneuver in Cyber Operations," Conference Paper, June 2012; https://www.researchgate.net/publication/236020494
32. JP 3-12, II-12.
33. JP 3-12 IV-6.
34. JP 3-0, GL-7.
35. Joint DoD Dictionary.
36. Rob Schrier, "Demonstrating Value and Use of Language–Normalizing Cyber as a Warfighting Domain," *The Cyber Defense Review*, Summer 2017, 19.
37. Andrew Schoka, Ibid.
38. Brett T. Williams, "The Joint Force Commander's Guide to Cyberspace Operations," *Joint Force Quarterly*, Issue 73, 2nd Quarter 2014.
39. *DoD Dictionary*. (Corresponding terms for civilian agencies are people, framework, processes, and pillars.)
40. JP 3-12, IV-1, IV-2.

Beyond Hyperbole: The Evolving Subdiscipline of Cyber Conflict Studies

Dr. Aaron F. Brantly

Hardly a day goes by without a cyber-related news story coming across the wires, yet the International Relations (IR) subdiscipline of cyber conflict studies has yet to meaningfully impact a wider discourse. This article examines the impact of five recent scholarly works on the evolution of this subdiscipline that, while quite popular within the general population, remains largely ignored by the broader International Relations (IR) scholarly community. The article dissects the strengths and weaknesses of these works and their place in the evolving literature by a generation of scholars who are moving debates beyond hyperbole. By highlighting cyber conflict studies to date, this roadmap hopefully will help to advance the study of cyberspace within the IR cyber community.

Kello, Lucas. *The Virtual Weapon and International Order*. New Haven: Yale University Press. 2017. 319 pp., $35 Hardcover (ISBN: 978-0300220230).

Buchanan, Ben. *The Cybersecurity Dilemma Hacking, Trust and Fear Between Nations*. New York: Oxford University Press. 2017. 290 pp., $35.62 Paperback (ISBN: 978-0190665012).

Valeriano, Brandon, Jensen, Benjamin M., & Maness, Ryan C. *Cyber Strategy: The Evolving Character of Power and Coercion*. Oxford University Press. 2018. 305 pp., $34.95 Hardcover (ISBN: 978-0190618094).

Mandel, Robert. Optimizing *Cyberdeterrence: A Comprehensive Strategy for Preventing Foreign Cyberattacks*. Washington, DC: Georgetown University Press. 2017. 289 pp., $64.95 Hardcover (ISBN: 978-1626164123).

Perkovich, George, & Levite, Ariel E. *Understanding Cyber Conflict: 14 Analogies*. Washington, DC: Georgetown University Press. 2017. 310 pp. $89.14 Hardcover (ISBN: 978-1626164970).

The sky is falling, or so it seems when watching the nightly news, newspapers, or many social media pundits. Cyber conflict appears to spell doom and gloom, and little can be done. The bits, bytes, and interwoven networks once jokingly (or not) referred to as "tubes" and meant to liberate and usher in a new era for humanity seemingly are now being turned against us in new and vicious forms of conflict.[1] Ironically, academia has been partially complicit in the hyperbole engulfing contemporary conversations on cyber conflict. The subdiscipline within security studies focusing on cyber security and conflict

Dr. Aaron F. Brantly is an Assistant Professor of Political Science at Virginia Tech (PhD, University of Georgia, 2012; MPP, American University, 2008). Dr. Brantly is the director of the Tech4Humanity Lab at Virginia Tech. His research focuses on national security policy issues in cyberspace including big data, terrorism, intelligence, decision-making and human rights. He is the author or editor of four books *The Decision to Attack: Military and Intelligence Cyber Decision-making, US National Cybersecurity: International Politics, Concepts and Organization,* and *Cybersecurity: Politics, Governance and Conflict in Cyberspace and The Cyber Deterrence Problem.*

has been advancing rapidly in recent years. The field has progressed substantially from the days when John Arquilla and David Rondfelt penned their work *In Athena's Camp:Preparing for Conflict in the Information Age in 1997*.[2] Since then the number of Internet-connected devices has grown exponentially, with Internet users now exceeding 50% of the global population. The last two decades have seen a bevy of new works addressing the growing concerns surrounding what is now ubiquitously, albeit unhelpfully, termed "cyberspace."

Over this time frame, the technical and organizational realities of cyberspace have changed dramatically. The US elevated cyber to warfighting domain status, and the associated force structure is now an independent combatant command headed by a 4-star general. Concurrently, the US has worked with NATO to establish cyber capabilities (a) in Tallinn, Estonia in response to Russian aggression against this small NATO member in 2007, and more recently (b) at an operations center in Brussels. Many, if not all, advanced countries are now developing cyber capabilities across their military, intelligence, and civilian sectors. The last two decades have also witnessed the theft of billions of dollars of intellectual property by state-sponsored hackers and cyber-attacks to manipulate elections, degrade nuclear facilities in Iran and North Korea, attack dams and industrial steel production, and briefly take power grids offline, to highlight some of the many of incidents that have taken place.

The rigor and depth of cyber conflict research is growing, yet there remains much hyperbole and lack of technical understanding. It is into this gap that the authors reviewed in this article attempt to delineate the mechanisms of conflict within cyberspace. Much discussion and scholarly work on cyber conflict is new, but much began far earlier.[3] Substantial research on cyber issues occurred well before 1984, when William Gibson coined "cyber" as it is commonly known today. Scholars such as Norbert Weiner established early radical

concepts of what the future of human-machine interaction would look like and actively used the word "cyber."[4] Wiener, along with John von Neumann, who invented modern computer architecture, were far ahead of their time in foreseeing the power and potential impact of computers on society, preceding even the Internet and its rise to global prominence. The rapid changes transpiring since the Cold War's end have prompted a global communications and information transmission substrate[5] that cuts across nearly every attribute of human existence. Chris Demchak and Peter Dombrowski define this substrate as a socio-technical system upon which modern world order is built.[6] The value and significance of cyberspace is difficult to assess and its full impact on international politics is obscured by its deep penetration into everyday life.

The importance of cyberspace to world order has been long debated. Among works that have greatly impacted the study of cyber conflict were those by Martin Libicki, an economist, who established an informed approach in a series of RAND-produced reports for the U.S. Air Force, including *Conquest in Cyberspace: National Security and Information Warfare,*[7] and *Cyberdeterrence and Cyberwar*.[8] Beyond Libicki, scholars such as Greg Rattray, Franklin Kramer, Stuart Starr, and Larry Wentz produced detailed analyses and edited volumes that confirmed why cyber conflict studies are critical to military audiences.[9] Myriam Dunn Cavelty extended the field to critical studies in her dynamic 2009 volume C*yber-security and Threat Politics.*[10] This flurry of early activity was measured in tone and sought to build a field based on informed study, without hyperbole.

Yet it was a 2010 book by former White House official Richard Clark and Robert Knake that catapulted the debate forward.[11] This book was aggressive, hyperbolic, and caused substantial ripples within the national security establishment. Yet, the rhetoric inspired substantial backlash within academia and spurred scholars such as Thomas Rid and Erik Gartzke to pen articles seeking to orient, both linguistically and theoretically, the impact of cyber conflict within the broader IR canon.[12] These works inspired the first set of conceptual volumes on cybersecurity, including the first two data-driven analyses of state behavior in cyberspace, by Brandon Valeriano & Ryan Maness,[13] and your author (Aaron Brantly).[14] They also inspired the first major analyses on cyber conflict cases by Jason Healey.[15] Combined, the literature up until the works discussed here sought to address arguments within a developing IR/security studies framework.

This is the historical backdrop for authors writing today, who face the challenge of establishing the relevance of their works to the broader discipline of IR, and, in particular, security studies. They also must address the challenges evident within the existing cyber conflict literature. These works must also capture the fine line between understating and hyperbolizing the importance of cyber conflict to security studies. Because cyber security and conflict issues often are poorly understood, authors sometimes are tempted to make claims based on public statements by government officials whose understanding of the nuanced realities of cyberspace, at best, is marginal. These claims, in contrast to these made about nuclear weapons

in an earlier era can, and often do, exceed reality. This article attempts to highlight how new works on cybersecurity can build upon existing literature and theory and add new concepts to the fields of IR and security studies without hyperbole. This analysis of the impact and effectiveness of arguments in advancing the evolving subdiscipline concludes by identifying three tracks in which works on cyber security and conflict fall.

Works examined below were chosen because they address the importance of theory to the evolving discipline of cybersecurity and conflict studies within a broader security studies subdiscipline. They offer five approaches to the study of cyber conflict, providing a cross-sectional view of a developing field of inquiry. Each offers a means of conceptualizing analytical leverage of a subdiscipline in constant flux. Some works attempt to build upon the past, while others appear wholly disconnected from existing literature. The central premise of this article is that, irrespective of the theoretical approach, new works that emerge from a core heuristic and expand knowledge within a novel domain of interaction via auxiliary hypotheses will better illuminate the security challenges of cyberspace, and also its broader security concepts. This does not mean that works that do not address theory are not valuable; they are, but their value added is derived through elevation of the discussion within the scholarly community, or the cataloging cases through informed commentary. Each work examines the challenges arising in cyberspace via a differing theoretical or methodological lens, each encompasses current relevant concerns, and each emphasizes state actions in cyberspace.

LEAVING THEORY BEHIND AND ELEVATING DISCUSSIONS

Lucas Kello in his 2017 book, *The Virtual Weapon: The International Order*, builds on his 2013 piece in *International Security*, with a discussion of the significance of conflict arising within cyberspace.[16] He provides robust examples of the many challenges associated with cyberspace and focuses on problems caused by particular state actors such as Russia and China while touching upon more complex issues surrounding policy, law, strategy, and tactics of offensive and defensive behavior. Kello begins his analysis aiming to establish a unifying theory around cyber conflict. He attempts to do this by robustly pushing back at critics of the subfield and advancing a distinct framework that elevates the position of cyber security and conflict. His approach is controversial and positions cyber security and conflict as something fundamentally distinct from conventional IR paradigms.

Kello diverges from more conventional theoretical approaches at the outset when he strikes swiftly against conventional IR theories: "Skeptics invoke that unfailing servant of intellectual reactionism in the field of international security studies: Carl von Clausewitz."[17] He then accurately argues that security studies have a substantial bias towards physical over virtual interactions.[18] Kello then turns to the hyperbole that dominates the balance of his book by comparing nuclear weapons and virtual ones. He writes:

> Some observers regard the advent of cyberspace as the greatest transformation in security affairs since the invention of nuclear arms. For all the symbolic enormity of the explosions over Japan in 1945, this comparison is wrong: it inflates the relative significance of the atomic bomb.
>
> ...both were driven by new technology and both were consequential in their own times. But the transforming potential of the cyber revolution is on a scale much deeper and broader than that of its older technological cousin.[19]

Kello's work is important to the literature on cyber conflict. Yet, by continuously trying to elevate the importance and value of cyber conflict above that of more conventional security paradigms he segregates his claims from the rigorous theoretical and conceptual works predating his analysis. When he writes "information is no longer just a source of power; it has become force itself,"[20] he hypes the centrality of cyberspace's role in international conflict so much that it negates the relative importance of other forms of conflict preceding it. The value of his work comes in his robust, provocative analysis of concepts such as deterrence, power, and state versus nonstate responsibilities. Each of these issues in isolation is of immense value and should serve to elevate the role of cyberspace within the broader security studies field without negating the more conventional security challenges. The framing of *The Virtual Weapon* makes it controversial. A more measured approach to conventional security challenges and the existing literatures would have made his point about the importance of cyber conflict. In contrast to Kello's claims, cyber conflict does not displace, but rather adds confusion and contention to, a security-challenged world.

Hyperbole aside, in many ways Kello accomplishes his goal: he contentiously elevates the value of cyber conflict, so much so that he questions whether IR scholars can even grasp the intricacies, nuances, and enormity of cyber conflict using conventional IR paradigms such as realism and liberalism. And while he correctly concludes that "[h]umans will be able to define many of its [cyberspace's] chief properties but without controlling or even grasping the security implications of its applications in society,"[21] His rejection of existing theoretical paradigms, and, instead, branching out with no grounding in pre-existing theory, adheres neither to a Lakatosian knowledge building approach of extending outward from a central core, nor to the rigors of Popperian analysis, which would require fully falsifying claims he ignores. He builds a case for developing a unified theory of cyber conflict within its own distinct ontological framework ungrounded in and unconstrained by prior international relations theories.

ROOTING IN A PARSIMONIOUS CORE

Where Kello's analysis seems almost deliberately hyperbolic and contentious, Ben Buchanan is measured and constructive. Buchanan's 2017 *The Cybersecurity Dilemma* arguably is one of the best theoretical works within the cyber conflict studies subfield and one that will impact the field in much the same way as Thomas Rid's *Cyber War Will Not Take Place*,[22] forcing the

subdiscipline to be more linguistically precise.[23] Buchanan's work meticulously covers many confounding aspects of state actions in cyberspace. His analysis of state perceptions interacting in a domain of uncertainty and obfuscation challenges readers to join him in pondering the complexities of conflict in a new way. His examination of the perspectives of cyber offense and defense as seen through the lens of the intruder and the defender, deftly examines what he refers to as a "paradox" in cyberspace. The argument and scope of *The Cybersecurity Dilemma* is narrowly focused and buttressed by substantial case analyses and anecdotes from historical intelligence and cyber incidents, thereby establishing it as a critical contribution. Rather than attempting to survey the entire field of cyber conflict writ large, or make grandiose claims about its importance, Buchanan allows the case analyses and mechanisms of state interaction to speak for themselves. In contrast to Kello, he builds deliberately on prior work to expand core theoretical debates on the security dilemma to encompass concerns about cyber conflict.

States use cyberspace to achieve advantages over one another. To do this they must seek out targets within cyberspace through a slow deliberate process in most instances. In building the logic for how states develop offensive capabilities against one another in cyberspace, Buchanan counters the fact that cyberspace events occur more rapidly than kinetic events and explains why the perception of speed arises disregards the deliberate and often painstaking efforts to identify relevant targets, penetrate them, and achieve persistent presence. He then connects this seemingly offensive behavior to the logic of defense by forward presence, a topic now highlighted in the 2018 U.S. Department of Defense Cyber Strategy which states:

> The Department will counter cyber campaigns threatening U.S. military advantage by defending forward to intercept and halt cyber threats and by strengthening the cybersecurity of systems and networks that support DoD missions.[24]

Buchanan anticipated US activities while highlighting how such behaviors further the mutual fear and mistrust between nations in a manner similar to Robert Jervis.[25] By going into adversaries' networks for defensive purposes, Buchanan notes that state defensive behaviors look remarkably offensive. He also draws out informational challenges such as attribution that give rise to the security dilemma.

By slowly, deliberately, and painstakingly building the case for a security dilemma in cyberspace, Buchanan is able to demonstrate why cyberspace is so important to international politics. He leverages this constrained approach to push back against common concepts in cyberspace, such as offense dominance.[26] He ties concepts of cyber conflict to conventional conflict where the analogies work well and by identifying areas where the logic of comparison fails. Specifically, he highlights the complexities of action in a domain where so much occurs behind the scenes. His final conclusion explores the likelihood that conflict and discord will continue within cyberspace as a function of the dilemma he builds, without implying anything beyond the scope of the existing data. Thus, he delineates the mechanics of a narrow, yet vital, set of attributes of conflict in cyberspace, and thereby provides a robust theoretical foundation

for future qualitative and quantitative analysis.

Buchanan's reticence to prognosticate on the potential severity of interactions in cyberspace allows the work to stand on its own merits and strengthens its argument without the rampant speculation of so many different works that came before. *The Cybersecurity Dilemma*'s constrained scope offers a model for how IR research on cyber conflict can be tied to the broader field, with a discipline that avoids addressing speculation as to a wider range of cyber challenges. His efforts have been mirrored in similar analyses such as Lonergan and Borghard's "The Logic of Coercion in Cyberspace."[27] Disciplined focus on one theory or issue at a time, allows these works to link cyber conflict and security to the broader security studies literature without artificially separating it as a new and fundamentally isolated from the rest of the discipline. The acceptance of existing ontologies, and the expansion of the core to encompass and explain novel phenomena, also avoids the pitfalls of hyperbole and groups the theory in tested, if not always entirely accurate, theories that predating cyberspace.

AN EXPANSIVE THEORETICAL APPROACH

Less parsimonious, but equally detailed, is the robust analysis of deterrence in cyberspace by Robert Mandel, in his 2017 book, *Optimizing Cyberdeterrence*, which leans more toward hyperbole than Buchanan's *The Cybersecurity Dilemma* but undertakes to analyze deterrence in cyberspace within the existing theoretical constraints of the broader discipline. In particular, Mandel builds his argument for tailored deterrence strategies in cyberspace by highlighting the weaknesses of targets to prevent, mitigate, and respond to cyber-attackers.[28] Mandel's analysis is detailed, yet broad in scope, examining a variety of means to engage in deterrence both within a domain and across domains. Mandel offers a more nuanced and likely more successful approach than those cyber deterrence scholars who urge only one option. He generally views cyber as requiring "broad inclusive deterrence,"[29] which contrasts with scholars such as Scott Jasper who seek out technical solutions (active deterrence),[30] normative forms of deterrence,[31] or other novel strategies such as entanglement.[32] Mandel analyzes deterrence less in conventional security paradigms offered by other scholars, but he does address many core concerns about cyber deterrence shared by these scholars.[33]

To explain why multiple deterrent options are needed, Mandel examines many reasons why deterrence in cyberspace is so difficult. In particular he identifies six key attributes: low perceived cyber defender credibility, high perceived cyber defender hypocrisy, high cyber attacker punishment resiliency, high cyber attacker obstacle adaptability, high cyber attacker operational secrecy, and low professed cyber attacker. These categories go beyond more constrained analyses associated with conventional deterrence literature, applying a logic more tailored to deter specific cyberspace threats. This deliberate choice is often criticized within the broader IR and security studies fields but is largely aligned with studies on nuclear deterrence. While such studies are robust in isolation, they often suffer from a loss of credibility due to failure to

consider escalatory behaviors that lead up to nuclear weapon use. Similarly, cyber deterrence viewed separately from the broader security implications of state interactions is problematic, as it often unduly prioritizes cyber conflict and attacks over more conventional solutions. Mandel avoids this by grounding his approach in case analyses that establish a concrete need for cyber-specific deterrence strategies.

One area where Mandel's work makes substantial headway in relation to deterrence is in a levels-of-analysis examination in Chapter 3. Whereas most conventional works on deterrence assume supremacy of the state,[34] Mandel takes special notice of those areas impacted by cyber-attacks that exist both below and above the nation-state.[35] He addresses often overlooked issues of capacity to deter that are missed in more conventional conversations on deterrence that are critically important in cyberspace. We obviously want to deter cyber adversaries, but how do we change bureaucracies, incentives, and public and private relationships to make deterrence viable? When discussing nuclear or even conventional kinetic deterrence, rarely are bureaucratic inertia or incentives to understand or implement new solutions considered. The organization of deterrence for kinetic options are established with clear hierarchies, and structured to facilitate or maximize deterrence. Cyberspace pervades all of government, private and civilian life, and infrastructures. Organizational understanding and capacities to deter, or the willingness to build in mechanisms, radically differ from conventional security studies models. Understanding these differences poses challenges to states seeking to deter. At the basic level they undermine the logic of deterrence and otherwise obfuscate successful deterrence strategies.

In concluding his analysis Mandel writes: [The] Cyberthreat does not exist in a vacuum, so responses should be formulated and implemented "in the context of larger global security affairs," explicitly connected to broader individual, local, national, regional and global security policies affecting both state and human security.[36]

This is good advice. Mandel's work throughout provides a robust assortment of case analyses framing the need for new, optimized deterrence strategies. He aptly frames the problem and hints at solutions, but does not prescribe them. His overall objective is not to provide a deterrence strategy, but rather, to set the stage for future scholars to build on his nuance in seeking out novel solutions, at the same time challenging decision-makers to implement concrete steps to secure cyberspace. Mandel essentially outlines the core heuristic and paves the way for subsequent scholars to expand upon his findings with novel auxiliary hypotheses.

MOVING BEYOND THEORY TO ANALOGICAL REASONING

Analysis in the first three works is rooted in theory and cases studies. Each work seeks to build a theory, whether broad and encompassing, as in the case of Kello, or narrow and focused by Buchanan. These efforts seek to tie cyber conflict to conventional security studies paradigms or leave them behind entirely. Cyberspace is and remains a socio-technical domain, replete with complex state and sub-state interactions. Use of cyberspace for conflict, for those

unfamiliar with its more advanced intricacies, can seem pedantic, even overwrought. To highlight the effects of cyber conflict in more conventional security studies it helps to reframe the arguments and use reasoning between two disparate albeit connected concepts. George Perkovich and Ariel E. Levite, in their edited volume *Understanding Cyber Conflict*, compiled a cohort of authors to leverage the power of analogy to generate frameworks for understanding the evolving subfield of cyber conflict within IR. Their work is thought-provoking and well organized. It helps provide a foundation for the expansion of theories outward from core heuristics by contextualizing complex interactions in cyberspace.

The use of analogy is not meant to elucidate a profound theory of how cyber conflict functions or how to achieve better deterrence in cyberspace. Instead, the 14 analogies presented attempt to link cyber conflict concepts directly to their conventional security studies counterparts. Each analogy, written by different authors, establishes a conceptual reference point for non-cyber conflict scholars. In the first, Michael Warner ties the form and function of cyber conflict to intelligence and in so doing highlights some of the many ways cyber conflict learns from and derives much of its applicability from intelligence.[37] Perhaps most importantly, Warner is able to tone down at the outset any potential hyperbole by noting:

> Both (intelligence and cyber) are inherently fragile and provocative. While neither is necessarily dangerously destabilizing in international relations, we must learn to perform cyberspace operations as we learned to perform intelligence activities - that is, with professional skill, with strict compliance with the law, and with careful oversight and accountability.[38]

Warner is joined in toning down hyperbole by retired LtGen Robert E. Schmiddle, Jr., USMC, Michael Sulmeyer, and Ben Buchannan in the second analogy, which compares nonlethal weapons and cyber capabilities carefully delineating the characteristics of cyber capabilities as different from nonlethal weapons,[39] thereby providing a robust starting point for plural analysis, not only on the use of such capabilities as acceptable in times of war and peace, but also in their material function. Questions raised on the reversibility, minimization of collateral damage, and deterrent attributes of the capabilities establish firm ground for future debates on the utility of cyber capabilities. The authors create parallels between a variety of nonlethal weapon systems and the actual use of cyber capabilities. This analogy permits rigorous conversations on severity and implications for use of cyber capabilities without resorting to exaggerated hypotheticals. Specifically, framing cyber capabilities as such also highlights their unique characteristics without equating them to the lethality of conventional kinetic weapons. Moreover, the discussion examines the concepts of attacking persons versus attacking materiel. By identifying that death by cyberattack has not yet transpired, the authors are able to focus on the true impact of cyber capabilities, i.e.: the destruction, denial, and degradation of systems. Constraining the scope of forecasts via analogy is important, and aligns studies of cyber conflict with security studies rather than science fiction.

One of the most interesting chapters examines the systematic utilization of cyber conflict by the Russian Federation in a variety of scenarios ranging from Estonia and Georgia to Ukraine.[40] Blank's analysis extends the breadth of impact of conventional cyber conflict outward to include the historically relevant forms of information and electronic warfare. While not an analogy, the case analysis does provide context in which cyber conflict is relevant to current security challenges. This chapter contrasts substantially with the chapter that follows, by John Arquilla, which examines the preventive nature of cyber conflict through multiple historical cases dating back to Thucydides and up to the DPRK and the use of Stuxnet against Iran.[41] The focused scope of Blank's chapter allows for the effects of specific cyber operations to be drawn out. Arquilla's sweeping comparisons are intellectually stimulating, but less effective in highlighting the true impact of cyber capabilities, if only because many of the effects are less than certain. Arquilla wisely hedges his assessment by characterizing cyber as a potential preventive measure, rather than declaring it a new weapon of critical importance in state conflict prevention.

In the contrast between these two chapters we see many of the fundamental challenges arising within the cyber conflict studies subdiscipline. Efforts to extend the logic of digital and virtual weapons, while highly relevant and of strategic and perhaps tactical value in one instance, are in others overextended and lack analytic leverage. Reining in the impulse to overvalue cyber conflict or capabilities helps to more accurately captures the true impact of cyberspace. As stated by Francis Gavin, "There is danger in focusing on technology to the exclusion of underlying political factors."[42] The chapters in this volume, provide a diversity of cases and analogies relevant security and conflict issues; each one caveats the arguments without hyperbole. Whether leveraging concepts of economic warfare,[43] Pearl Harbor,[44] air defense constructs,[45] or even nuclear technologies,[46] the scope, while detailed, does not exalt cyber conflict beyond reality.

This work establishes contours and grounds the domain's realities in a way that allows future scholars to apply theory. It stands as a key resource for those interested in studying cyberspace. The analogies within the volume help define the core ontologies of the field establish its foundations. While not driven by theory, they inform scholarship on an often-misunderstood technical domain.

PIECING THE PUZZLE: TESTING THE CORE

Because all things cyber, digital, Internet of Things, quantum, crypto, or whatever the buzzword, are often confusing to non-technical specialists, constructing theories based on reality can be challenging. One such challenge is the dearth of readily available public data on state interactions in cyberspace. Such data that is usable and relevant to cyber conflict scholars is often plagued by inaccuracies or derived from media reporting and hearsay, which has led to an abundance of case study-based works. Case studies are extremely valuable but are often obscure macro-level trends explainable by IR theories. Several projects are underway to operationalize cyber conflict data across all instances[47] and within specific conflicts such as Ukraine.[48] These studies will further add a data driven understanding of cyber conflict.

Brandon Valeriano, Benjamin Jensen, and Ryan Maness build upon previous efforts in their first work *Cyber War Versus Cyber Realities*[49] by continuing to develop a robust dataset of state cyber incidents in their new work *Cyber Strategy: The Evolving Character of Power and Coercion*,[50] and set the bar for data-driven analysis within the subfield. They use data to parse out many of the theoretical concepts developed by Buchanan, Kello, and Mandel, and analogies highlighted in Perkovich and Levite. Their analyses are robust and address the limits of coercive power within cyberspace. More importantly, they add quantitative rigor to a field too often dominated by conjecture and "Chicken Littles" that claim the sky is falling. By building a dataset and testing hypotheses, they rein in debate and challenge the subfield to build a more systematized foundation. This book is unique in tying cyber conflict literature directly to that of more conventional security studies. Equally important, the authors define their hypotheses at the outset and provide a consequential set of testable concepts around which they build arguments and engage in quantitative analysis.

By rigorously tying concepts of security studies to cyber conflict in their first several chapters, Valeriano et al., are able to use analytical/conceptual weight of their intellectual forebearers to carve out a niche for cyber conflict. When examining such conflict across the spectrum of espionage, and other disruptive and degrading activities, the authors found "cyber operations produce *only limited concessions*" (emphasis in original).[51] Diving deeper, their analysis found cyber espionage and disruption provided degradation but within the context of traditional powers, limited coercive impact.[52] Moreover, they identified the US as the primary coercive actor producing 89% of incidents of cyber degradation.[53] Beyond the limited scope of cyber to coerce, they also find there are "unique forms of coercion;" however, these are often combined with more traditional instruments of state power extending beyond cyberspace. Valeriano et al. rightly assess: "Cyber Coercion adds another vector for pressuring an adversary to change their behavior, but it must be evaluated in its proper geopolitical context."[54] They add:

> The more we study the impact of cyber actions, the more we find that those actions that do achieve a desired change in behavior in the target are rare, marginal in comparative impact, and costly in terms of giving up techniques to the adversary.[55]

Beyond the quantitative rigor, one of the more useful attributes of their analysis is a robust assessment of the effectiveness of various forms of coercion in cyberspace. This qualitative approach sets the stage for their subsequent tests, but also concisely frames much of the existing literature on cyber coercion. By examining disruption, intimidation, swaggering, espionage, deception, blackmail, denial, attrition, cost imposition, decapitation, punishment, risk, and control as means of cyber coercion, their exhaustive list of coercive methods is independently examined and critiqued.[56]

The deliberative approach by which Valeriano et al., establish the strengths, and perhaps more importantly the weaknesses, of cyber operations to achieve coercive power builds a place for cyber conflict within security studies more broadly. While unfairly criticized by some as

pessimists or for not fully grasping the "value" of cyber brings to modern state interactions, their middle-of-the-road, measured approach detracts nothing from cyber's future value and importance. Valeriano et al.'s analysis, both in *Cyber Strategy and Cyber War vs. Cyber Realities*, provides a solid foundation for the field. Cyberspace is important, but not clearly any more or less so than other forms of conflict. Their approach to collecting and analyzing data is valuable, but limited. Their data help elucidate the concepts they examine, but they do not rely solely on data without substantial case comparison and analysis within the broader context of security studies. Their work serves as a bridge between the largely qualitative works to date and a potential quantitative future open to cyber conflict scholars.

They conclude by highlighting the need for norms, information sharing, and public private frameworks, not because these matrices would mitigate challenges of cyberspace, but rather, because they would reemphasize and ensure global connectivity, education, communications, and economic markets rather than conflict. The work of Valeriano et al., serves as an azimuth test for the development of cybersecurity as a subdiscipline within IR and security studies. The data they collect, while in its early stages in comparison to long-established conflict datasets such as the Correlates of War Project or The Peace Research Institute Oslo Conflict, is a major step forward and allows for testing of auxiliary hypotheses against core theories within IR. Their work initiates a process of pulling together disparate pieces of a puzzle for testing.

BEYOND HYPERBOLE

Cyber conflict studies are advancing rapidly. As with any new and evolving field of inquiry, there are multiple approaches for a scholar. This article explains why the philosophy of science literature and concepts proposed by Imre Lakatos, predicated on building outward from a core by adding and testing auxiliary hypotheses, help generate new understanding without as yet unsupported and hence thus far, excessive claims.[57] The works considered in this essay follow three distinct tracks. The first follows the trajectory continued by Lucas Kello, and likely includes Alex Andrew Futter's *Hacking the Bomb*[58] and Clarke and Knake's, *Cyber War: The Next Threat to National Security and What to Do About It,*[59] among others. These works rightly raise alarm over a field many consider as receiving too little attention within the wider IR community. Their works are contentious, aggressive, and scoff at the constraints of conventional theoretical paradigms. Yet, they elevate the conversation with some hyperbole mixed in, plus a great deal of thought as to how cyberspace might influence security and conflict more broadly. These works are rigorous and well informed but are not beholden to the existing canon. In short, they cause scholars to rethink what the core of the research paradigm should be and whether maintaining a hold on conventional theories helps or hurts the study of a newly expanding domain of inquiry. They often do this by ignoring the existing core research programs of IR or security studies more specifically. The second track is populated by what is best referred to as informed commentators. These works span a wide spectrum of individuals and their audience is not academic. These works are filled with insider accounts, historical analyses, and case studies.

Works by journalists such as David Sanger,[60] Kim Zetter,[61] Ted Koppel,[62] Shane Harris,[3] and others are immensely valuable. They provide access and insights not otherwise available to many in the IR community. This track also includes individuals who have formally left the national security community, such as Richard Clarke,[65] John Carlin,[60] and Michael Hayden.[66] These works help scholars from both the first and third tracks understand the ontological nature of cyberspace and interactions within it. These works do not challenge the theoretical core of the research program but rather provide fodder for those seeking either to discard the core or to build auxiliary hypotheses to buttress it.

The third track of works includes those by Peter Shane and Jeffrey Hunker,[67] Nazli Choucri,[68] Tim Stevens,[69] Tim Maurer,[70] Herb Lin and Amy Zegart,[71] Alexander Klimburg,[72] and Adam Segal,[73] and more than a dozen others. Collectively, these works form a cohort of scholars best referred to as theoretical expansionists. Each attempt to take up conventional theories and build on them in unique ways, some more successfully than others. Yet, all have an eye toward expanding the reach of theories within IR and security studies more specifically to encompass topics relating to cyber security and conflict. The four works reviewed after Kello's book fit nicely within this third track. Each build upon the more conventional works within the IR canon while seeking to address both mundane and novel phenomena in a rigorous and informed manner within existing paradigms. They buttress the core and expand knowledge with auxiliary hypotheses to further existing research programs. In so doing, they generally avoid hyperbole due to the nature of the existing research programs they seek to build upon.

The subfield of cyber security and conflict studies will grow even more important as the penetration of cyberspace extends to more of the global population and the role and number of Internet-connected devices dominating economic, social, environmental, and political domains increase. Many of the most valuable contributions to date come in the form of edited volumes that span issue areas, including works by Van Puyvelde and Brantly;[74] Reveron;[5] Lindsay, Cheung, and Reveron;[76] Schaub;[77] and Jarmon and Yannakogeorgos;[78] plus journal articles that engage specific concepts or challenges associated with cyber conflict including Garzke and Lindsay,[79] Smeets,[80] Brantly,[81] Schneider, McDonald, and Krepps[82] and even policy pieces on websites such as War on the Rocks, Foreign Policy, or others. Multiple journals have published increasingly on cyber security and conflict, to include *International Security, Security Studies, Journal of Conflict Resolution, Survival, Journal of Cyber Policy, Journal of Cybersecurity, Intelligence and National Security, International Studies Review*, and others. The underlying tenets of security and conflict among states will rightly remain primary topics of study. However, the means by which to influence or prevent conflict, or potential avenues by which to escalate or deescalate, are likely finding increasing sources within cyberspace.

Cyber conflict is developing novel effects and is increasing in importance relative to the number and types of systems interconnected with a tendency to substitute complexity or hyperbole at the expense of sound social science. Works by scholars such as Valeriano et al. and Eric Jardine highlight how various attributes of cyberspace lead to bias, and, by extension, hyperbole.[83]

Those five works demonstrate is an increasing ability to engage the broader discipline of security studies while simultaneously surveyed here build understanding of cyber security and conflict within an expanding scope. Testable hypotheses developed to explain new forms of conflict offers fertile ground for future inquiry. Conventional theory remains important, if only as a sounding board (Kello) or a foundation (Buchannan, Mandel, Perkovich & Levite, Valeriano, Jensen, and Maness) for analysis. Each of the three tracks above has a place within the subdiscipline, and each has a role in informing the other tracks, scholarship, and policy.

BIBLIOGRAPHY

Arquilla, John. "From Pearl Harbor to the "Harbor Lights"." Understanding Cyber Conflict: 14 Analogies: Georgetown University Press, 2017.

———. "An Ounce of (Virtual) Prevention?". Understanding Cyber Conflict: 14 Analogies: Georgetown University Press, 2017.

Blank, Stephen. "Cyber War and Information War a La Russe." Understanding Cyber Conflict: 14 Analogies: Georgetown University Press, 2017.

Blum, Andrew. Tubes : A Journey to the Center of the Internet. Ecco. Ecco, 2013.

Borghard, Erica D., and Shawn W. Lonergan. "The Logic of Coercion in Cyberspace." [In English]. Security Studies 26, no. 3 (2017): 452 81. https://doi.org/10.1080/09636412.2017.1306396.

Brantly, Aaron F. "Aesop's Wolves: The Deceptive Appearance of Espionage and Attacks in Cyberspace." Intelligence and National Security 31, no. 5 (2015): 674-85. https://doi.org/10.1080/02684527.2015.1077620.

———. "The Cyber Deterrence Problem." (2018): 31-54. https://doi.org/10.23919/cycon.2018.8405009.

———. The Decision to Attack: Military and Intelligence Cyber Decision-Making. University of Georgia Press, 2016.

Buchanan, Ben. "Cyber Deterrence Isn't Mad; It's Mosaic." Georgetown Journal of International Affairs, no. 4 (2014): 130-40.

———. The Cybersecurity Dilemma Hacking, Trust and Fear between Nations. Oxford University Press, 2017.

Carlin, John P., and Garrett M. Graff. The Dawn of the Code War : America's Battle against Russia, China, and the Rising Global Cyber Threat. New York: NY: PublicAffairs, 2019.

Cavelty, Myriam Dunn. Cyber-Security and Threat Politics : Us Efforts to Secure the Information Age. 2009.

Choucri, Nazli. Cyberpolitics in International Relations. Cambridge, MA: MIT Press, 2012.

Clarke, Richard A. "The Risk of Cyber War and Cyber Terrorism." Journal of International Affairs 70, no. 1 (October 24, 2018 2018): 179-81.

Clarke, Richard A., and Robert Knake. Cyber War: The Next Threat to National Security and What to Do About It. Harper-Collins Publishers, 2010.

Demchak, Chris. "Rise of a Cybered Westphalian Age." 10.1126/science.aar6404. Science (New York, N.Y.) 362, no. 6419 (2018): 1140-44. https://doi.org/papers3://publication/doi/10.1126/science.aar6404. http://www.sciencemag.org/lookup/doi/10.1126/science.aar6404.

Denning, Dorothy E., and Bradley J. Strawser. "Active Cyber Defense: Applying Air Defense to the Cyber Domain." Understanding Cyber Conflict: 14 Analogies: Georgetown University Press, 2017.

Elman, Colin, and Miriam Fendius Elman. Progress in International Relations Theory: Appraising the Field. Cambridge, MA: MIT Press, 2003.

Feaver, Peter, and Kenneth Geers. ""When the Urgency of Time and Circumstances Clearly Does Not Permit...": Pre-Delegation in Nuclear and Cyber Scenarios." Understanding Cyber Conflict: 14 Analogies: Georgetown University Press, 2017.

Futter, Andrew. Hacking the Bomb: Cyber Threats and Nuclear Weapons. Washington, D.C.: Georgetown University Press, 2018.

Gartzke, Erik. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth." 10.1162/ISEC_a_00136. International Security 38, no. 2 (2013): 41-73. https://doi.org/papers3://publication/doi/10.1162/ISEC_a_00136. http://www.mitpressjournals.org/doi/abs/10.1162/ISEC_a_00136.

Gartzke, Erik, and Jon R. Lindsay. "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace." Security Studies 24, no. 2 (2015/04/03 2015): 316-48. https://doi.org/10.1080/09636412.2015.1038188. https://doi.org/10.1080/09636412.2015.1038188.

Gavin, Francis J. "Crisis Instability and Preemption." In Understanding Cyber Conflict: 14 Analogies. Understanding Cyber Conflict: 14 Analogies. Washington, D.C.: Georgetown University Press, 2017.

George, Alexander L., and Richard Smoke. Deterrence in American Foreign Policy: Theory and Practice. New York: Columbia University Press, 1974.

Glaser, Charles. Deterrence of Cyber Attacks and U.S. National Security. Cyber Security Policy and Research Institute (Washington, D.C.: 2011).

BIBLIOGRAPHY

Goldman, Emily O., and Michael Warner. "Why a Digital Pearl Harbor Makes Sense...And Is Possible." Understanding Cyber Conflict: 14 Analogies: Georgetown University Press, 2017.

Harris, Shane. @War: The Rise of the Military-Internet Complex. Boston, MA: Houghton Mifflin Harcourt, 2014.

Hayden, Michael V. Playing to the Edge : American Intelligence in the Age of Terror. New York, New York: Penguin Audio,, 2016. spoken word, 13 sound discs (17 hr.) : digital, CD audio ; 4 3/4 in., PRHA 5499 Penguin Audio.

Healey, Jason. A Fierce Domain: Conflict in Cyberspace, 1986 to 2012. Cyber Conflict Studies Association, January 1, 2013, 2013.

Hunker, Jeffrey. "U.S. International Policy for Cybersecurity: Five Issues That Won't Go Away." Journal of National Security Law & Policy 4, no. 2008 (January 1, 2010 2010): 197-216.

Huth, Paul K. "Deterrence and International Conflict: Emprical Findings and Theoretical Debates." Annual Review of Political Science (January 1, 1999 1999): 25-48.

In Athena's Camp. Edited by Arquilla John. Santa Monica, CA: The Rand Corporation, 1998.

Jardine, Eric. "Global Cyberspace Is Safer Than You Think: Real Trends in Cybercrime." SSRN Electronic Journal (2015). https://doi.org/10.2139/ssrn.2634590.

Jarmon, Jack A., and Panayotis A. Yannakogeorgos. The Cyber Threat and Globalization : The Impact on U.S. National and International Security. Lanham, UK: Rowman and Littlefield, 2018.

Jasper, Scott. Strategic Cyber Deterrence the Active Cyber Defense Option. Rowman & Littlefield. Rowman & Littlefield, 2017.

Jervis, Robert. "Cooperation under the Security Dilemma." World Politics 30, no. 2 (1978): 167-214. https://doi.org/10.2307/2009958. www.jstor.org/stable/2009958.

Kello, Lucas. "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft." International Security 38, no. 2 (2013): 7-40. https://doi.org/10.1162/ISEC_a_00138. https://www.mitpressjournals.org/doi/abs/10.1162/ISEC_a_00138 %X While decisionmakers warn about the cyber threat constantly, there is little systematic analysis of the issue from an international security studies perspective. Some scholars presume that the related technology's scientific complexity and methodological issues prohibit orderly investigation; only a minimum degree of technical acuity is needed, however, revealing the scope of maneuver in the cyber domain. Other skeptics argue that the cyber peril is overblown, contending that cyber weapons have no intrinsic capacity for violence and do not alter the nature or means of war. This view misses the essence of the danger and conceals its true significance: the new capability is expanding the range of possible harm and outcomes between the concepts of war and peace—with important implications for national and international security. The cyber domain, moreover, features enormous defense complications and dangers to strategic stability: offense dominance, attribution difficulties, technological volatility, poor strategic depth, escalatory ambiguity, and proliferation to nontraditional and subversive actors. But even if the cyber danger is overstated, the issue merits serious scholarly attention. Whatever the current cyber revolution signifies, it is detrimental to the intellectual progress and policy relevance of the field to continue to avoid its central questions.

———. The Virtual Weapon and International Order. Yale University Press. Yale University Press, 2017.

Klimburg, Alexander. The Darkening Web: The War for Cyberspace. Penguin Books. New York, NY: Penguin Books, 2017.

Koppel, Ted. Lights Out: A Cyberattack, a Nation Unprepared, Surviving the Aftermath. New York, NY: Crown Publishers, 2015.

Kostyuk, Nadiya, and Yuri M. Zhukov. "Invisible Digital Front." [In English]. Journal of Conflict Resolution 9, no. 1 (2017). https://doi.org/10.1177/0022002717737138.

Kramer, Franklin D, Stuart H Starr, and Larry K Wentz. "Cyberpower and National Security." (January 1, 2009 2009).

Kreps, Sarah, and Jacquelyn Schneider. "Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving Beyond Effects-Based Logics." Journal of Cybersecurity 5, no. 1 (2019): 1-11.

Lambert, Nicholas A. "Brits-Krieg: The Strategy of Economic Warfare." Understanding Cyber Conflict: 14 Analogies: Georgetown University Press, 2017.

Libicki, Martin C. Cyberdeterrence and Cyberwar. RAND Corporation, 2009.

Libicki, Martin C., Rand Corporation, and issuing body. "Conquest in Cyberspace : National Security and Information Warfare." (2007).

BIBLIOGRAPHY

Lin, Herbert, and Amy B. Zegart. Bytes, Bombs, and Spies : The Strategic Dimensions of Offensive Cyber Operations. Washington, D.C.: Georgetown University Press, 2019.

Lindsay, Jon R., Tai Ming Cheung, and Derek S. Reveron. China and Cybersecurity : Espionage, Strategy, and Politics in the Digital Domain. New York: Oxford University Press, 2015.

Macdonald, Julia, and Jacquelyn Schneider. "Presidential Risk Orientation and Force Employment Decisions." Journal of Conflict Resolution 61, no. 3 (2017): 511-36. https://doi.org/10.1177/0022002715590874.

Mandel, Robert. Optimizing Cyberdeterrence : A Comprehensive Strategy for Preventing Foreign Cyberattacks. Washington, DC: Georgetown University Press, 2017.

Maurer, Tim. Cyber Mercenaries : The State, Hackers, and Power. Cambridge, UK: Cambridge University Press, 2018.

Mazanec, Brian M., and Bradley A. Thayer. Deterring Cyber Warfare : Bolstering Strategic Stability in Cyberspace. 2015.

Nye Jr, Joseph S. "Deterrence and Dissuasion in Cyberspace." International Security 41, no. 3 (2017): 44-71. http://www.mitpressjournals.org/doi/10.1162/ISEC_a_00266.

Passeri, Paolo. "Hackmageddon: Information Security Timelines and Statistics." 2010. https://www.hackmageddon.com/.

Puyvelde, Damien Van, and Aaron F. Brantly. "Us National Cybersecurity." (2017). https://doi.org/10.4324/9781315225623.

Reveron, Derek S. Cyberspace and National Security : Threats, Opportunities, and Power in a Virtual World. Washington, DC: Georgetown University Press, 2012.

Rid, Thomas. "Cyber War Will Not Take Place." Journal of Strategic Studies 35, no. 1 (2012/02/01 2012): 5-32. https://doi.org/10.1080/01402390.2011.608939. https://doi.org/10.1080/01402390.2011.608939.

Sanger, David E. The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age. New York, NY: Broadway Books, 2018.

Schaub, Gary. Understanding Cybersecurity : Emerging Governance and Strategy. Rowman and Littlefield, 2018.

Schelling, Thomas. Arms and Influence. New Haven, Conn: Yale University Press, 1966.

Schmiddle Jr., Robert E. , Michael Sulmeyer, and Ben Buchanan. "Nonlethal Weapons and Cyber Capaiblities." Understanding Cyber Conflict: 14 Analogies: Georgetown University Press, 2017.

Schneider, Jacquelyn. "What War Games Tell Us About the Use of Cyber Weapons in a Crisis." Council on Foreign Relations (2018). cfr.org/blog/what-war-games-tell-us-about-use-cyber-weapons-crisis.

Segal, Adam. The Hacked World Order : How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age. Second edition. ed. New York: PublicAffairs, 2017.

Smeets, Max. "A Matter of Time: On the Transitory Nature of Cyberweapons." [In English]. Journal of Strategic Studies 41, no. 1-2 (2018): 6-32. https://doi.org/10.1080/01402390.2017.1288107.

Snyder, Glenn H. "Deterrence and Power." 4, no. 2 (June 1, 1960 1960): 163-78.

Stevens, Tim. Cyber Security and the Politics of Time. Cambridge, UK: Cambridge University Press, 2015.

Valeriano, Brandon, Benjamin M. Jensen, and Ryan C. Maness. Cyber Strategy: The Evolving Character of Power and Coercion. Oxford University Press. Oxford University Press, 2018.

Valeriano, Brandon, and Ryan C. Maness. Cyber War Versus Cyber Realities: Cyber Conflict in the International System. Oxford University Press. Oxford University Press, 2015.

Warner, Michael. "Cybersecurity: A Pre-History." Intelligence and National Security 27, no. 5 (2012): 781-99.

———. "Intelligence in Cyber-and Cyber in Intelligence." Understanding Cyber Conflict: 14 Analogies: Georgetown University Press, 2017.

Wiener, Norbert. Cybernetics or Control and Communication in the Animal and the Machine. MIT Press, 1965.

Zetter, Kim. "Countdown to Zero Day : Stuxnet and the Launch of the World's First Digital Weapon." (January 1, 2014).

NOTES

1. Andrew Blum, *Tubes: a journey to the center of the Internet*, Ecco, (Ecco, 2013).
2. *In Athena's Camp*, ed. Arquilla John (Santa Monica, CA: The Rand Corporation, 1998).
3. Michael Warner, "Cybersecurity: A Pre-history," *Intelligence and National Security* 27, no. 5 (2012).
4. Norbert Wiener, *Cybernetics Or Control and Communication in the Animal and the Machine* (MIT Press, 1965).
5. This is a term used by Chris Demchak to describe the role of cyberspace in society – i.e. forming a socio-technical-economic substrate.
6. Chris Demchak, "Rise of a Cybered Westphalian Age," 10.1126/science.aar6404, *Science (New York, N.Y.)* 362, no. 6419 (2018), https://doi.org/papers3://publication/doi/10.1126/science.aar6404, http://www.sciencemag.org/lookup/doi/10.1126/science.aar6404.
7. Martin C. Libicki, Rand Corporation, and issuing body, "Conquest in cyberspace : national security and information warfare," (2007).
8. Martin C. Libicki, *Cyberdeterrence and Cyberwar* (RAND Corporation, 2009).
9. Franklin D Kramer, Stuart H Starr, and Larry K Wentz, "Cyberpower and national security," (January 1, 2009 2009).
10. Myriam Dunn Cavelty, *Cyber-security and Threat Politics : us efforts to secure the information age* (2009).
11. Richard A Clarke, "The Risk of Cyber War and Cyber Terrorism," *Journal of International Affairs* 70, no. 1 (October 24, 2018 2018).
12. Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (2012/02/01 2012), https://doi.org/10.1080/01402390.2011.608939, https://doi.org/10.1080/01402390.2011.608939.; Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," 10.1162/ISEC_a_00136, *International Security* 38, no. 2 (2013), https://doi.org/papers3://publication/doi/10.1162/ISEC_a_00136, http://www.mitpressjournals.org/doi/abs/10.1162/ISEC_a_00136.
13. Brandon Valeriano and Ryan C. Maness, *Cyber war versus cyber realities: cyber conflict in the international system*, Oxford University Press, (Oxford University Press, 2015).
14. Aaron F. Brantly, *The Decision to Attack: Military and Intelligence Cyber Decision-Making* (University of Georgia Press, 2016).
15. Jason Healey, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Cyber Conflict Studies Association, January 1, 2013, 2013).
16. Lucas Kello, *The virtual weapon and international order*, Yale University Press, (Yale University Press, 2017); Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," *International Security* 38, no. 2 (2013), https://doi.org/10.1162/ISEC_a_00138, https://www.mitpressjournals.org/doi/abs/10.1162/ISEC_a_00138 %X. While decisionmakers constantly warn about the cyber threat, there is little systematic analysis of the issue from an international security studies perspective. Some scholars presume that the related technology's scientific complexity and methodological issues prohibit orderly investigation; only a minimum degree of technical acuity is needed, however, revealing the scope of maneuver in the cyber domain. Other skeptics argue that the cyber peril is overblown, contending that cyber weapons have no intrinsic capacity for violence and do not alter the nature or means of war. This view misses the essence of the danger and conceals its real significance: the new capability is expanding the range of possible harm and outcomes between the concepts of war and peace—with important implications for national and international security. The cyber domain, moreover, features enormous defense complications and dangers to strategic stability: offense dominance, attribution difficulties, technological volatility, poor strategic depth, escalatory ambiguity, and proliferation to nontraditional and subversive actors. But even if the cyber danger is overstated, the issue merits serious scholarly attention. Whatever the current cyber revolution signifies, it is detrimental to the intellectual progress and policy relevance of the field to continue to avoid its central questions.
17. Kello, *The virtual weapon and international order.*
18. See Jacquelyn Schneider, "What War Games Tell Us About the Use of Cyber Weapons in a Crisis," *Council on Foreign Relations* (2018), cfr.org/blog/what-war-games-tell-us-about-use-cyber-weapons-crisis.
19. Kello, *The virtual weapon and international order.*
20. Kello, T*he virtual weapon and international order.*
21. Kello, T*he virtual weapon and international order.*
22. Rid, "Cyber War Will Not Take Place."
23. Ben Buchanan, *The Cybersecurity Dilemma Hacking, Trust and Fear Between Nations* (Oxford University Press, 2017).
24. 2018 *Cyber Strategy.*

NOTES

25. Robert Jervis, "Cooperation Under the Security Dilemma," World Politics 30, no. 2 (1978), https://doi.org/10.2307/2009958, www.jstor.org/stable/2009958.
26. Buchanan, *The Cybersecurity Dilemma Hacking, Trust and Fear Between Nations.*
27. Erica D. Borghard and Shawn W. Lonergan, "The Logic of Coercion in Cyberspace," *Security Studies* 26, no. 3 (2017), https://doi.org/10.1080/09636412.2017.1306396.
28. Robert Mandel, *Optimizing cyberdeterrence : a comprehensive strategy for preventing foreign cyberattacks* (Washington, DC: Georgetown University Press, 2017).
29. Id.
30. Scott Jasper, *Strategic cyber deterrence the active cyber defense option,* Rowman & Littlefield, (Rowman & Littlefield, 2017).
31. Brian M. Mazanec and Bradley A. Thayer, *Deterring cyber warfare: bolstering strategic stability in cyberspace* (2015).
32. Joseph S. Nye Jr, "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (2017), http://www.mitpressjournals.org/doi/10.1162/ISEC_a_00266.
33. Aaron F. Brantly, "The cyber deterrence problem," (2018), https://doi.org/10.23919/cycon.2018.8405009; Charles Glaser, *Deterrence of CYber Attacks and U.S. National Security,* Cyber Security Policy and Research Institute (Washington, D.C., 2011); Ben Buchanan, "Cyber Deterrence Isn't MAD; It's Mosaic," *Georgetown Journal of International Affairs,* no. 4 (2014).
34. Alexander L. George and Richard Smoke, *Deterrence in American foreign policy: theory and practice* (New York: Columbia University Press, 1974); Thomas Schelling, *Arms and Influence* (New Haven, Conn: Yale University Press, 1966); Glenn H Snyder, "Deterrence and Power," 4, no. 2 (June 1, 1960 1960); Paul K Huth, "Deterrence and International Conflict: Empirical Findings and Theoretical Debates," *Annual Review of Political Science* (January 1, 1999).
35. Mandel, Optimizing cyberdeterrence : a comprehensive strategy for preventing foreign cyberattacks.
36. Mandel, Optimizing cyberdeterrence : a comprehensive strategy for preventing foreign cyberattacks.
37. Michael Warner, "Intelligence in Cyber-and Cyber In Intelligence," Understanding Cyber Conflict: 14 Analogies (Georgetown University Press, 2017).
38. Warner, "Intelligence in Cyber-and Cyber In Intelligence."
39. Robert E. Schmiddle Jr., Michael Sulmeyer, and Ben Buchanan, "Nonlethal Weapons and Cyber Capaiblities," Understanding Cyber Conflict: 14 Analogies (Georgetown University Press, 2017).
40. Stephen Blank, "Cyber War and Information War a la Russe," *Understanding Cyber Conflict: 14 Analogies* (Georgetown University Press, 2017).
41. John Arquilla, "An Ounce of (Virtual) Prevention?," *Understanding Cyber Conflict: 14 Analogies* (Georgetown University Press, 2017).
42. Francis J. Gavin, "Crisis Instability and Preemption," in *Understanding Cyber Conflict: 14 Analogies*, Understanding Cyber Conflict: 14 Analogies (Washington, D.C.: Georgetown University Press, 2017).
43. Nicholas A. Lambert, "Brits-Krieg: The Strategy of Economic Warfare," U*nderstanding Cyber Conflict: 14 Analogies* (Georgetown University Press, 2017).
44. John Arquilla, "From Pearl Harbor to the "Harbor Lights"," Understanding Cyber Conflict: 14 Analogies (Georgetown University Press, 2017); Emily O. Goldman and Michael Warner, "Why a Digital Pearl Harbor Makes Sense...and Is Possible," Understanding Cyber Conflict: 14 Analogies (Georgetown University Press, 2017).
45. Dorothy E. Denning and Bradley J. Strawser, "Active Cyber Defense: Applying Air Defense to the Cyber Domain," Understanding Cyber Conflict: 14 Analogies (Georgetown University Press, 2017).
46. Peter Feaver and Kenneth Geers, ""When the Urgency of Time and Circumstances Clearly Does not Permit...": Pre-Delegation in Nuclear and Cyber Scenarios," Understanding Cyber Conflict: 14 Analogies (Georgetown University Press, 2017).
47. Paolo Passeri, "Hackmageddon: Information Security Timelines and Statistics," (2010). https://www.hackmageddon.com/.
48. Nadiya Kostyuk and Yuri M. Zhukov, "Invisible Digital Front," *Journal of Conflict Resolution* 9, no. 1 (2017), https://doi.org/10.1177/0022002717737138.
49. Valeriano and Maness, *Cyber war versus cyber realities: cyber conflict in the international system.*
50. Brandon Valeriano, Benjamin M. Jensen, and Ryan C. Maness, *Cyber strategy: the evolving character of power and coercion,* Oxford University Press, (Oxford University Press, 2018).
51. Valeriano, Jensen, and Maness, *Cyber strategy: the evolving character of power and coercion.*

NOTES

52. Valeriano, Jensen, and Maness, *Cyber strategy: the evolving character of power and coercion.*
53. Valeriano, Jensen, and Maness, *Cyber strategy: the evolving character of power and coercion.*
54. Valeriano, Jensen, and Maness, *Cyber strategy: the evolving character of power and coercion.*
55. Valeriano, Jensen, and Maness, *Cyber strategy: the evolving character of power and coercion.*
56. Valeriano, Jensen, and Maness, *Cyber strategy: the evolving character of power and coercion.*
57. Colin Elman and Miriam Fendius Elman, *Progress in international relations theory: appraising the field* (Cambridge, MA: MIT Press, 2003).
58. Andrew Futter, *Hacking the Bomb: Cyber Threats and Nuclear Weapons* (Washington, D.C.: Georgetown University Press, 2018).
59. Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (HarperCollins Publishers, 2010).
60. David E. Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age* (New York, NY: Broadway Books, 2018).
61. Kim Zetter, "Countdown to Zero Day : Stuxnet and the launch of the world's first digital weapon," (January 1, 2014 2014).
62. Ted Koppel, *Lights Out: a Cyberattack, a Nation Unprepared, Surviving the Aftermath* (New York, NY: Crown Publishers, 2015).
63. Shane Harris, *@War: the rise of the military-Internet complex* (Boston, MA: Houghton Mifflin Harcourt, 2014).
64. Clarke and Knake, *Cyber War: The Next Threat to National Security and What to Do About It.*
65. John P. Carlin and Garrett M. Graff, *The Dawn of the Code War : America's Battle Against Russia, China, and the Rising Global Cyber Threat* (New York: NY: PublicAffairs, 2019).
66. Michael V. Hayden, *Playing to the edge: American intelligence in the age of terror* (New York, New York: Penguin Audio,, 2016), spoken word, 13 sound discs (17 hr.): digital, CD audio ; 4 3/4 in., PRHA 5499 Penguin Audio.
67. Jeffrey Hunker, "U.S. International Policy for Cybersecurity: Five Issues That Won't Go Away," *Journal of National Security Law & Policy* 4, no. 2008 (January 1, 2010).
68. Nazli Choucri, *Cyberpolitics in international relations* (Cambridge, MA: MIT Press, 2012).
69. Tim Stevens, *Cyber Security and the Politics of Time* (Cambridge, UK: Cambridge University Press, 2015).
70. Tim Maurer, *Cyber mercenaries : the state, hackers, and power* (Cambridge, UK: Cambridge University Press, 2018).
71. Herbert Lin and Amy B. Zegart, B*ytes, bombs, and spies : the strategic dimensions of offensive cyber operations* (Washington, D.C.: Georgetown University Press, 2019).
72. Alexander Klimburg, *The Darkening Web: the war for cyberspace*, Penguin Books, (New York, NY: Penguin Books, 2017).
73. Adam Segal, *The hacked world order: how nations fight, trade, maneuver, and manipulate in the digital age*, Second edition. ed. (New York: PublicAffairs, 2017).
74. Damien Van Puyvelde and Aaron F. Brantly, "US National Cybersecurity," (2017), https://doi.org/10.4324/9781315225623.
75. Derek S. Reveron, *Cyberspace and national security : threats, opportunities, and power in a virtual world* (Washington, DC: Georgetown University Press, 2012).
76. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron, *China and cybersecurity : espionage, strategy, and politics in the digital domain* (New York: Oxford University Press, 2015).
77. Gary Schaub, *Understanding cybersecurity: emerging governance and strategy* (Rowman and Littlefield, 2018).
78. Jack A. Jarmon and Panayotis A. Yannakogeorgos, *The cyber threat and globalization: the impact on U.S. national and international security* (Lanham, UK: Rowman and Littlefield, 2018).
79. Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies* 24, no. 2 (2015/04/03 2015), https://doi.org/10.1080/09636412.2015.1038188, https://doi.org/10.1080/09636412.2015.1038188.
80. Max Smeets, "A matter of time: On the transitory nature of cyberweapons," *Journal of Strategic Studies* 41, no. 1-2 (2018), https://doi.org/10.1080/01402390.2017.1288107.
81. Aaron F. Brantly, "Aesop's wolves: the deceptive appearance of espionage and attacks in cyberspace," *Intelligence and National Security* 31, no. 5 (2015), https://doi.org/10.1080/02684527.2015.1077620.

NOTES

82. Sarah Kreps and Jacquelyn Schneider, "Escalation firebreaks in the cyber, conventional, and nuclear domains: moving beyond effects-based logics," *Journal of Cybersecurity* 5, no. 1 (2019); Julia Macdonald and Jacquelyn Schneider, "Presidential Risk Orientation and Force Employment Decisions," *Journal of Conflict Resolution* 61, no. 3 (2017), https://doi.org/10.1177/0022002715590874.
83. Valeriano, Jensen, and Maness, *Cyber strategy: the evolving character of power and coercion*; Eric Jardine, "Global Cyberspace Is Safer than You Think: Real Trends in Cybercrime," *SSRN Electronic Journal* (2015), https://doi.org/10.2139/ssrn.2634590.

Why the Law of Armed Conflict (LOAC) Must Be Expanded to Cover Vital Civilian Data

Colonel Beth D. Graboritz
Lieutenant Colonel James W. Morford
Major Kelley M. Truax

> I assess we are seeing what we term *corrosive threats*, in which malicious cyber actors weaponize personal information, steal intellectual property, and mount influence campaigns. Such measures have had and will have strategic effects on our nation and allies.[1]
>
> *- General Paul M. Nakasone, 2019*

INTRODUCTION

In June 2017, during Ukraine's multi-year undeclared war with Russia, the NotPetya worm hit Ukraine as part of a "scorched-earth testing ground for Russian cyberwar tactics."[2] Between 2015 and 2016, Kremlin-backed hackers known as Sandworm focused on Ukrainian government organizations and companies. In the NotPetya cyber-attack against Ukraine, this worm spread automatically, rapidly, and indiscriminately throughout thousands of computers worldwide, crippling multinational companies, including maritime shipping giant Maersk, pharmaceutical giant Merck, food producer Mondelēz International, and even Russia's state-owned oil company, Rosneft. NotPetya is unlike other malware to date because its goal was purely destructive. It mimicked ransomware but was, in reality, more sinister since there was no amount of ransom that could be paid to decrypt a system's data because no decryption key even existed. Damages associated with the 2017 NotPetya attack exceeded $10 billion. While there was no loss of life, former U.S. Department of Homeland Security advisor Tom Bossert equated NotPetya's destructiveness to "using a nuclear bomb to achieve a small tactical victory."[3]

Colonel Beth D. Graboritz recently began serving as the Deputy Director, for the National Security Agency Command, Control, Communications and Cyber Systems Directorate. Previously, she was the Commander, 65th Air Base Group, with four squadrons of 750 personnel located at Lajes Field, Portugal and Morón Air Base, Spain, and served as the Installation Commander for US Forces at Lajes Field, fulfilling the duties of the Commander, US Forces Azores in accordance with US and Portuguese bilateral agreements. Colonel Graboritz received her commission upon graduation from Embry-Riddle Aeronautical University with a Bachelor of Science degree in Aviation Computer Science. She has served in a variety of base-level, command and staff assignments. Additionally, she has deployed several times in support of Operations SOUTHERN WATCH, IRAQI and ENDURING FREEDOM.

Cyber-attacked data was vital to both Ukraine and private companies; ultimately, the attack led to dire second- and third-order consequences to international commerce. NotPetya is a prime example of collateral damage to civilian data through cyberspace operations (CO), where national borders have no meaning, and the scale of destruction is intolerable. Yet, vital civilian data is not generally considered a Civilian Object (capitalized to differentiate it from the more general sense) under the Law of Armed Conflict (LOAC), the international law that governs conduct during armed conflicts. Currently, LOAC defines a Civilian Object as all things that do not fall within the definition of a military objective, with examples that only encompass the physical, brick and mortar domain such as civilian housing, schools, and churches. Thus, data is not afforded the protections of Civilian Objects.

Not surprisingly, data characterization and whether data manipulation, disruption, and destruction constitute an attack is one of many contentious topics now being examined by cyber law experts. Why? Because this is where adversaries conduct CO: in the gray zone between war and peace, where LOAC is murky or inapplicable, and where terms like "Civilian Object" and "cyber-attack" are unclear or incomplete and often esoteric, leaving a wide gap for interpretation and debate. The U.S. Department of Defense (DoD) must advocate for, and the Joint Staff adopt, an updated definition that protects vital civilian data as a Civilian Object, and Congress should incorporate this as national policy, and urge its adoption into international law, and hence be governed by the LOAC.

Understanding Current International Cyber Law

Better understanding of the current environment and its challenges requires us to examine existing international law governing data characterization and its application in LOAC. One definitive reference detailing how international law applies to the cyber domain

Lieutenant Colonel James W. Morford is the Deputy Director for Communications and Information (A6) at 7th Air Force. He and his team are responsible for planning, upgrading and maintaining communications and information systems on behalf of the Korean theater's air component. During exercise and contingency, they provide full situational awareness on AFFOR systems' status, capabilities, and any issues, as well as support and guidance to field units on the restoration of C4 systems after outages. He received his undergraduate degree from the University of Arizona, graduate degree from American Military University, Charles Town WV, and graduated Intelligence Officer School at Goodfellow AFB, TX. His operational assignments include tours at Dyess AFB, Texas, Osan AB, Republic of Korea, the Pentagon, Charleston AFB, and Headquarters United States Transportation Command at Scott AFB, with five deployments supporting Operations IRAQI FREEDOM, ENDURING FREEDOM, and INHERENT RESOLVE.

in armed conflict is the *Tallinn Manual 2.0* (hereafter "Tallinn Manual"), as published in 2017. Edited by 19 international law experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence, the Tallinn Manual includes 154 rules governing CO, with extensive commentary on each rule.[4]

Rule 92 in the Tallinn Manual describes a cyber-attack as "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or *damage or destruction to objects* [emphasis added]."[5] To fully understand whether a CO is, in fact, an attack and thus subject to the LOAC, the scope of the term "Object" is important. Rule 100 in the Tallinn Manual addresses civilian Objects and military objectives, with the definition of Object being derived from the International Committee of the Red Cross (ICRC) Additional Protocols 1987 Commentary (protocols over and above the Geneva Convention of 1949).[6] The English text uses *objects* which means "something placed before the eyes, or presented to the sight or other sense, an individual thing seen, or perceived, or that may be seen or perceived; a material thing." The French text uses *biens*, which means "chose tangible, susceptible *d'appropriation*." So the word in both English and French means something that is "visible and tangible."[7] Further, Article 52 of Additional Protocol I defines a military objective as "those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage," and a Civilian Object as "all objects which are not military objectives."[8] Thus, what we deem as Civilian Objects cannot be cyber-attacked.[9]

The international law experts who collaborated on the Tallinn Manual agreed cyber infrastructure such as computers, computer networks, and other tangible components are considered Objects, but not Data. They also

Major Kelley M. Truax is the Deputy Chief, Strategy and Policy Analysis Division, under the Command, Control, Communications and Cyber Systems Directorate (J6) for U.S. Transportation Command, located at Scott AFB, IL. Her division is responsible for preparing enterprise-level guidance and audits for on-premise and cloud service acquisition, transition, and management in sup-port of combatant command global operations, ensuring the availability of U.S. Transportation Command's global cyber domain, supporting 39,000 users and 77 command and control systems. She received her commission upon graduation from Embry-Riddle Aeronautical University with a Bachelor of Science degree in Computer Science, and later attended Western International University where she obtained a Master of Science in Information Systems Engineering. She has served in a variety of base-level, Forward Operating Agency, Major Command, Combatant Command, and Joint assignments, with a deployment supporting Operations ENDURING FREEDOM, IRAQI FREEDOM and NEW DAWN.

agreed that Object, properly defined, should exclude data because data is neither visible nor tangible.[10] As such, data cannot be characterized as either a civilian or military Object, meaning an attack on data cannot normally be characterized as a cyber-attack; nor can data be afforded the protections of a Civilian Object in armed conflict. Thus, data manipulation, disruption, and destruction are also typically exempt from the LOAC. Yet a minority of experts dissented, arguing that the majority opinion did not consider the severity of consequences if data is manipulated. The minority also believed "essential" civilian data, such as tax records and social security data, should be included in the definition of Civilian Objects for the purposes of LOAC protections.[11]

The majority did note that a CO targeting data may qualify as an attack if it "...foreseeably results in the injury or death of individuals or damage or destruction of physical objects, those individuals or objects constitute the 'object of attack,' and the operation, therefore, qualifies as an attack."[12] This occurred in 2009 when Stuxnet worked its way inside Iran's Natanz uranium enrichment facility,[13] taking control of 1,000 uranium enriching centrifuges, manipulating data so as to cause the centrifuges to spin at varying speeds and ultimately self-destruct, without displaying abnormal parameters to control center operators. Iran was forced to decommission about 20 percent of its centrifuges during the months-long cyber-attack.[14] Stuxnet was the most sophisticated virus or worm yet, and unlike any that came before, masking its corruption with espionage-level stealth, showing the world the destruction CO can wreak in the physical domain.

Current US Law and Policy Applicable to CO

Shifting to domestic law and policy, the US adheres to international law regarding the conduct of CO and uses it as the basis for domestic laws and policies, but also recognizes the complexities and inconsistencies within

the cyber environment. DoD authority to conduct military CO is governed by statute. For example, Title 10 U.S. Code authorizes the DoD to conduct military CO in response to malicious cyber activity.[15] Fiscal Year 2012 (FY12) National Defense Authorization Act (NDAA), Section 954 states, "Congress affirms DoD has the capability, and upon the direction by the President may conduct offensive operations in cyberspace to defend our Nation, Allies, and interests."[16] FY13 NDAA directed U.S. Cyber Command (USCYBERCOM) to protect the networks and critical infrastructure of the US, both offensively and defensively,[17] and the FY17 NDAA elevated USCYBERCOM to a Combatant Command underscoring the importance of this task.[18]

Based on Congress' direction to conduct CO, DoD formulated policies to govern the conduct of CO and manage associated risks. "Targeting" under Joint Publication 3-60 is defined as "an entity (person, place, or thing) considered for possible engagement or action to alter or neutralize the function it performs for the adversary," without explicitly including data as an entity.[19] When reviewing targets for legal sufficiency, military staff judge advocates consider laws of war, U.S. Code, rules of engagement, commander's guidance, and other limiting factors. They also carefully consider risks to noncombatants, i.e., civilians and Civilian Objects. Because cyber law and cyber-attack capabilities continually evolve, the US must frequently revise policies governing CO.

Understanding the Characterization of Cyber Espionage and Intelligence Collection

Data is characterized differently depending on whether it pertains to cyber espionage and intelligence collection. International law as applied to espionage is murky, and legal scholars differ as to what is legal, depending upon the purposes of espionage, but all generally agree that it *may* be legal. A contradiction exists inside US law, with the NDAA 2019 modifying Title 10 U.S. Code (Armed Forces) § 130g (renumbered § 394) to "[The Secretary of Defense shall] conduct, military cyber activities or operations in cyberspace, including clandestine military activities or operations in cyberspace, to defend the US and its allies, including in response to malicious cyber activity carried out against the United States or a United States person by a foreign power." Further, Title 50 U.S. Code (War and National Defense) Chapter 36 (Foreign Intelligence Surveillance) § 1802 allows the President to authorize foreign intelligence surveillance against foreign powers via electronic surveillance, provided there is no substantial likelihood of collection where a U.S. Person is a party.[20] At the same time, Title 18 U.S. Code (Crimes and Criminal Procedures), Chapter 37, in some detail defines a wide variety of espionage-like acts as illegal. Doubtless, most foreign powers have a similar legal dichotomy; as an example, China has both the Counter-Espionage Law of 2014[21] and the National Intelligence Law of 2017.[22]

Controversy exists as to cyber espionage, which can reasonably be defined as the "exercise of state power within the bounds of another state,"[23] no doubt breaking the second state's espionage laws, and thereby implicating sovereignty issues. The Tallinn Manual suggests "although peacetime cyber espionage by states does not *per se* violate international law, the *method* by which it is carried out might do so [emphasis added]."[24] For example, the experts' majority

opinion in the Tallinn Manual was that a cyber-attack on another State's infrastructure clearly violated sovereignty if it created damage (even unintended), yet opinion differed as to implants, or malware, that caused no particular damage.[25] But manipulating or damaging targeted vital data during cyber espionage, as Object is now defined, is wholly unprotected under LOAC.

An increasingly interconnected, or networked, globe will only muddy the waters further. Network infrastructure is mostly owned and operated by nominally civilian institutions, yet law and reality complicate the matter from a military operations standpoint. Huawei, China's telecommunications giant, for example, for years has been installing networking hardware in countries worldwide, and is a leader in global 5G development and deployment. Nominally a private corporation,[26] the CEO, Ren Zhengfei, is a prior Information Technology officer in China's Peoples' Liberation Army with close government ties.[27] An editorial report by Dr. Murray Tanner in *Lawfare Blog* notes that China's 2017 National Intelligence Law places an affirmative burden on all Chinese peoples and entities to provide "access, cooperation, or support for Beijing's intelligence-gathering activities."[28] And many laws are so broad they cover a wide range of eventualities. No great leap is required, then, to see that Huawei not only is *obligated* but *likely* to forward information of major intelligence value to the Chinese government whenever possible. From a CO perspective, is the legal status of civilian data residing on Huawei equipment outside of China to be classified as a Civilian Object and hence LOAC-protected, or a military Object, and thus fair game for cyber-attack?

In the US, no state-owned communications enterprises exist. Dr. Tanner contrasts China's National Intelligence Law with the U.S. Executive Order 12333 and its "detailed definitions, procedures, limitations and prohibitions regarding a number of intelligence activities, including government collection, retention, and dissemination of information on US persons and corporations."[29] That said, the Foreign Intelligence Surveillance Act compels private carriers, when requested by the Attorney General, to "furnish all information, facilities, or technical assistance necessary to accomplish the electronic surveillance [against foreign powers, outlined above] in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier is providing its customers."[30]

Why the Current Definition of Object is Inadequate

National interests wholly unprotected by LOAC already have been compromised by the CO destruction or manipulation of vital civilian data that is not currently considered an Object. In 2007, the decision by Estonia to relocate a World War II memorial from the center of its capital, Tallinn, to a military cemetery outside the city, ignited tensions between ethnic Russians and Estonians, which were further enflamed by false Russian reports. Within days of the decision, Estonia experienced weeks of major denial of service, impairing banking, media outlets, and government institutions. Access to ATMs and online banking was crippled, as were government employee communications,[31] thereby demonstrating the ease whereby CO can manipulate access to data to exploit tensions, and create disturbances and instability, even in a NATO

country like Estonia, in efforts to extort political outcomes. Military reprisal by NATO was avoided by acting below the level of armed conflict; despite the crippling damage wrought, this was not even classified as a cyber-attack.

On December 23, 2015, 225,000 Ukrainians were denied power for hours after a cyber-attack took down part of Ukraine's power grid. Three electricity distribution companies reported being unable to remotely restore power from the control room computers, which required workers to switch to manual controls and travel to 30 substations to restore power.[32] Almost a year to the day, Ukraine experienced a similar cyber-attack against an electric transmission station causing an hour-long outage. The chilling difference of the later attack was its autonomous nature of producing mass power outages, displaying the most evolved and adaptable grid-sabotaging malware seen yet, thereby threatening critical infrastructure and power grids worldwide, including the US.[33]

These two examples illustrate a growing category of CO designed to sabotage critical civilian infrastructure by altering data that is unprotected under LOAC. As the Tallinn Manual points out, the real-world effects of these CO could be deemed as cyber-attacks given their physical impact. Expanding or clarifying the definition of Object to include civilian data not only would help legitimize a proportional response by the victim; it also would disincentivize the targeting of that civilian data in the first place.

There also are examples of adversary CO not manipulating or destroying the targeted data. In January 2015, the second-largest health insurer in the U.S. was targeted, reportedly exposing extremely sensitive data for as many as 80 million current and former customers and employees, including social security numbers, birth dates, and addresses.[34] Post-attack analysis of the Anthem cyber-attack supported the conclusion that this was a practice run for the OPM breach that followed within months, both tracing back to China.[35]

The largest US compromise of sensitive personal information was disclosed in April 2015, with the hack commencing as early as November 2013. The personal information of some 21.5 million current and former government employees and job applicants was stolen,[36] as were security clearance forms and digital images of government employee fingerprints.[37] The far-reaching extent of this breach not only impacts past and current employees and job applicants, but also, all others listed on the security clearance forms, such as spouses, parents, siblings, and college roommates. This breach poses US national security risks that may haunt generations to come. US government costs of credit monitoring services may eventually top $1 billion,[38] and some of that stolen data has surfaced in subsequent financial fraud cases.[39]

As these two examples show, the repercussions are directly or indirectly tied to national security and should not be ignored. Expanding the LOAC's reach with a more inclusive definition of Object is overdue. This no doubt will not always dissuade an adversary from deciding to launch attack, but surely international law should characterize such attacks as illegal.

Moreover, victim States would be justified in retaliating, and calling upon partner States to also retaliate, sanction, censor, etc. The LOAC, properly expanded, should give an adversary pause before attacking civilian data of another country. It's worth highlighting here other responses to such attacks, such as Sony, refusing to be cyber-bullied, responding to North Korea's CO to block the release of a movie satirizing Kim Jong-un by publishing the movie online,[40] and Israel's May 2019 response against a Hamas cyber group with a kinetic strike on its building.[41]

The Case for a Broader Definition of an Object

Confidentiality, integrity, and availability of vital civilian data are key to U.S. national interests, both from economic and political perspectives. Industries have risen and fallen based on advantages gained or lost by proprietary and intellectual property, which, like civilian data, is not classified as an Object or protected by LOAC. Compromise of this type of data often falls within the realm of corporate espionage. Objects as now defined in the Tallinn Manual, simply lags behind the rapidly changing uses and misuses of cyberspace worldwide. For example, what used to be gold, silver, silk, and spices as primary bartered wares has given way to electronic banknotes and cryptocurrencies, all still accepted as forms of payment but, by the above definitions, not real or tangible, yet dramatically impacting our global economy.

Dr. Robert G. Papp, the CIA's former director of the Center for Cyber Intelligence, urged a cyber treaty, a treaty that would ban nations from using cyber weapons in the virtual domain, to help govern these issues for the international community, akin to the 1967 Outer Space Treaty or the 1959 Antarctic Treaty.[42] Substituting the word cyber into those treaties unfortunately oversimplifies the challenge here, but these frameworks are models that could help. Any cyber treaty effort should aim to create a common framework from which all responsible parties can create "expectations and develop a set of principles, rules and procedures, and norms about how states behave with respect to an entire domain."[43] Creating a common baseline is crucial. Without that, it is hard to imagine any incentives or rewards for honoring a treaty, or ways to identify expectations, or workable enforcement consequences for violators.[44]

The US, by adopting a national policy that defines civilian data as an ICRC Civilian Object, not only takes a high ground in cyberspace; it will also reassure allies and neutral powers that, even in peacetime, CO will abide by LOAC concepts of *military necessity, proportionality, and distinction*. The US pledged in the 2018 National Cyber Strategy, to "promote a framework of responsible state behavior in cyberspace built upon international law, adherence to voluntary non-binding norms of responsible state behavior that apply during peacetime."[45] More broadly defining Object to include vital civilian data will enable U.S. planners to categorize it more effectively as either a military or Civilian Object and treat it accordingly. This clarity should benefit all States. The US should also advocate for the incorporation of these changes to LOAC and other international laws in pursuit of universal, responsible state behavior in cyberspace. Simultaneously, the Joint Staff should revisit "target" as defined in Joint Publication 3-60 so as to include data as a targetable entity if it meets the criteria of a military objective, and DoD

should submit a legislative proposal for the National Defense Authorization Act for 2020 to identify, classify, and legally define data as an Object.

CONCLUSION

More inclusively defining Object would allow for appropriate LOAC protections for vital civilian data targeted in a cyber-attack. This alone may not prevent another Sandworm from launching NotPetya and destroying vital civilian data, but it would provide State and organizational victims a far more robust legal standing to respond directly or seek other indirect actions. An adversary knowing of this legal protection is more likely deterred than one that is considering a cyber-attack that international law arguably sanctions. Cyber-attack victims deserve the right to strike back proportionately, take legal action, and/or seek international support, including reparations for the damage caused by the cyber-attack. Redefining Object to include vital civilian data is one of many keys that will help resolve the myriad challenges international and domestic law and policies face in addressing CO in armed conflict. With or without a more inclusive definition, any nation can strike back in self-defense, or pursue appropriate actions when other international law violations occur, such as violation of sovereignty. Expanding the definition of Object to protect vital civilian data so that it can be LOAC-protected, with accompanying broader definitions adopted by DoD, the Joint Staff, and Congress, will put much needed teeth in deterrence that is missing today.

DISCLAIMER

Opinions expressed here are solely those of the authors and do not represent the official policies or endorsements, either ex¬pressed or implied, of the DoD, USCYBERCOM, or any U.S. Government agency.

ACKNOWLEDGMENT

The authors are grateful for the contributions to the research presented here by U.S. Navy Commander Peter Pascucci, now serving as Deputy Staff Judge Advocate for U.S. Special Operations Command; U.S. Army Colonel Gary Corn, now serving as the Staff Judge Advocate for U.S. Cyber Command; and Mr. Bryan Bird, now serving as the Cyber and National Security Law Attorney for U.S. Transportation Command.

NOTES

1. U.S. Senate Committee on Armed Services, *Hearing to Review Testimony on United States Special Operations Command and United States Cyber Command in Review of the Defense Authorization Request for Fiscal Year 2020 and the Future Years Defense Program*, 116th Congress, February 14, 2019 (statement of General Paul M. Nakasone, Commander, United States Cyber Command).
2. Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired: Security,* August 22, 2018, accessed May 9, 2019, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.
3. Andy Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* (Doubleday, 2019), 17-18, 197-8.
4. Michael N. Schmitt and Liis Vihul, eds., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Op-erations* (Cambridge, UK: Cambridge University Press, 2017), p.i. Positions expressed in the Tallinn Manual are based on interpretations of International Law by the experts in their personal capacity and do not reflect the official position of any particular nation or organization.
5. Ibid., 415.
6. Ibid., 437.
7. International Committee of the Red Cross (ICRC) Additional Protocols 1987 Commentary (1987), Art. 47, 2007-2008.
8. Ibid., 435.
9. Ibid., 434.
10. Ibid., 437.
11. Ibid., 437.
12. Ibid., 416.
13. Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," *Wired: Security,* November 3, 2014, accessed May 10, 2019, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.
14. Gordon Corera, "What Made the World's First Cyber-Weapon So Destructive?" *BBC: iWonder,* accessed May 10, 2019, http://www.bbc.co.uk/guides/zq9jmnb.
15. U.S. Code Title 10, § 130g.
16. National Defense Authorization Act of Fiscal Year 2012, § 954.
17. National Defense Authorization Act of Fiscal Year 2013.
18. National Defense Authorization Act of Fiscal Year 2017.
19. Joint Chiefs of Staff, *Joint Targeting*, Joint Publication 3-60 (Washington, DC: US Joint Chiefs of Staff, Janu-ary 31, 2013), I-1.
20. As defined in Exec. Order No. 12333.
21. China Law Translate, "Counter-Espionage Law of the People's Republic of China," *China Law Translate*, No-vember 1, 2014, accessed May 16, 2019, https://www.chinalawtranslate.com/anti-espionage/?lang=en.
22. Murray Scot Tanner, "Beijing's New National Intelligence Law: From Defense to Offense," *Lawfare*, July 20, 2017, accessed May 9, 2019, https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense.
23. Craig Forcese, "Pragmatism and Principle: Intelligence Agencies and International Law," *Virginia Law Review*, July 9, 2016. Accessed May 11, 2019. http://www.virginialawreview.org/volumes/content/pragmatism-and-principle-intelligence-agencies-and-international-law.
24. Tallinn Manual 2.0, 168.
25. Ibid., 173.
26. In their article for Columbia Law School, "Beyond Ownership: State Capitalism and the Chinese Firm," the authors Milhaupt and Zheng note, "Functionally, [state-owned enterprises] and large [privately-owned enterprises] in China share many similarities in the areas commonly thought to distinguish state-owned firms from privately owned firms: market access, receipt of state subsidies, proximity to state power, and execution of the government's policy objectives." https://www.law.columbia.edu/node/5344/beyond-ownership-state-capitalism-and-chinese-firm-curtis-j-milhaupt-and-wentong-zheng.
27. "The Company that Spooked the World," *Economist*, August 4, 2012, accessed May 8, 2019, https://www.economist.com/briefing/2012/08/04/the-company-that-spooked-the-world.
28. Tanner, "Beijing's New National Intelligence Law: From Defense to Offense."

NOTES

29. Ibid.
30. U.S. Code Title 50, §1802.
31. Damien McGuinness, "How a Cyber Attack Transformed Estonia," *BBC News: Europe,* April 27, 2017, ac-cessed May 10, 2019, https://www.bbc.com/news/39655415.
32. Chris Vallance, "Ukraine Cyber-Attacks 'Could Happen to UK,'" *BBC News: Technology,* February 29, 2016, accessed May 10, 2019, https://www.bbc.com/news/technology-35686493.
33. Andy Greenberg, "'Crash Override': The Malware that Took Down a Power Grid," *Wired: Security,* June 12, 2017, accessed June 10, 2019, https://www.wired.com/story/crash-override-malware/.
34. Kim Zetter, "Health Insurer Anthem is Hacked, Exposing Millions of Patients' Data," *Wired: Security,* February 5, 2015, accessed May 12, 2019, https://www.wired.com/2015/02/breach-insurer-exposes-sensitive-data-millions-patients/.
35. Brendan I. Koerner, "Inside the Cyberattack that Shocked the US Government," *Wired: Security,* October 23, 2016, accessed May 11, 2019, https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/.
36. Evan Perez, "FBI Arrests Chinese National Connected to Malware Used in OPM Data Breach," CNN: Justice, August 24, 2017, accessed May 11, 2019, https://www.cnn.com/2017/08/24/politics/fbi-arrests-chinese-national-in-opm-data-breach/index.html.
37. Brendan I. Koerner, "Inside the Cyberattack that Shocked the US Government," *Wired: Security,* October 23, 2016, accessed May 11, 2019, https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/.
38. Josh Fruhlinger, "The OPM Hack Explained: Bad Security Practices Meet China's Captain America" *CSO,* No-vember 6, 2018, accessed May 12, 2019, https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-prac-tices-meet-chinas-captain-america.html.
39. Derek Hawkins, "The Cybersecurity 202: 'A Wake Up Call.' OPEM Data Stolen Years Ago Surfacing Now in Finan-cial Fraud Case," *The Washington Post: Cybersecurity 202 Newsletter,* June 20, 2018, accessed May 11, 2019, https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/06/20/the-cybersecurity-202-a-wake-up-call-opm-data-stolen-years-ago-surfacing-now-in-financial-fraud-case/5b2924ca1b326b3967989b66/?utm_ter-m=.4ea7357ae96d.
40. Michael Cieply and Brooks Barnes, "Sony Cyberattack, First a Nuisance, Swiftly Grew Into a Firestorm," *The New York Times,* December 30, 2014, accessed May10, 2019, https://www.nytimes.com/2014/12/31/business/media/sony-attack-first-a-nuisance-swiftly-grew-into-a-firestorm-.html?module=inline.
41. Shannon Vavra, "It Was 'Inevitable' That Bombs Would Fall in Response to a Cyberattack," *Cyberscoop: Government,* May 6, 2019, accessed May 7, 2019, https://www.cyberscoop.com/hamas-cyberattack-israel-air-strikes/.
42. James Carden, "Time to Pursue an International Cyber Treaty?" *The Nation,* April 30, 2019.
43. Ronald Deibert, "Tracking the Emerging Arms Race in Cyberspace," *Bulletin of the Atomic Scientists* 67, (Janu-ary-February 2011): 1-8.
44. P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know®* (New York: Oxford University Press, 2014), 185-193.
45. Donald J. Trump, *National Cyber Strategy of the United States of America* (Washington, DC: The White House, September 2018), 20.

Contesting Key Terrain: Urban Conflict in Smart Cities of the Future

Maxim Kovalsky
Lieutenant Colonel Robert J. Ross, Ph.D.
Greg Lindsay

ABSTRACT

Smart City initiatives are multiplying at an accelerated pace. Hundreds of Smart City pilot projects are aiming to make urban dwelling more sustainable by leveraging automation, and digitizing interactions among technologies, people, and the physical environment. Each project is an ecosystem, with stakeholders ranging from government officials and technology firms with their near infinite supply chains to city residents. Many projects that began as experimental pilots are now integral to the way city government organizations deliver services to their constituents. An increasingly urbanized world, rapidly becoming more dependent upon sophisticated technologies, presents novel and substantial complexities to future military operations.

Smart Cities will become the status quo operating environment for future urban military operations. This article illustrates the implications of misestimating the impact of connected infrastructure during post-conflict operations in the networked urban environment of tomorrow and proposes a methodology to assess and manage risks associated with operating in densely networked environments. The authors rely on a combination of qualitative methodologies (Threatcasting, Thematic Analysis) to identify key technological trends being adopted by municipal governments around the world and to explore the implications these technologies pose for future military operations in urban environments. Based on their findings, the article presents eight supplemental questions to help military planners understand and anticipate vulnerabilities and opportunities associated with operating in Smart Cities, and otherwise improve operational decision-making and the prognosis for success in the urban battlespace.

Maxim Kovalsky is a Senior Manager in Deloitte's Cyber Risk Advisory practice. With over ten years of experience in technology and cyber security, Maxim's work at Deloitte has focused on security intelligence and operations strategy and implementation projects across multiple sectors. He has led engagements in areas covering cyber security program assessments, threat detection and response, and threat intelligence. Prior to joining Deloitte, Maxim worked for the Federal Bureau of Investigation, providing operational and intelligence support to complex cybercrime investigations. Mr. Kovalsky is a reservist in the U.S. Army and a member of the Cyber Electromagnetic Activities portfolio team within the 75th Innovation Command.

PREFACE

"They've turned the city against us," thought Major General Adam Larsen as he surveyed the smoking wreckage of several personnel carriers in the town square. The enemy was still nowhere to be seen, but it clearly was doing everything short of showing itself to expel his division out of the city. First, trash mountains began appearing atop overflowing waste bins at every intersection, attracting vermin. Then traffic signals malfunctioned, leading to citywide crashes and collisions. Then, most major thoroughfares became impassable as frustrated police cleared intersections while fending off rats.

Things had begun going awry when the city of Gnok's sanitation control center started directing its autonomous garbage trucks to random locations, none of which was a collection point. Too late, system operators realized something was wrong when electric trucks en-route to depots stopped dead in their tracks, blocking streets and intersections. Attempts to send troubleshooting teams were thwarted when they discovered their remaining fleet had drained batteries due to suspicious errors in their recharging systems. Pleas to borrow gas-powered vehicles from other departments fell on deaf ears; there were no longer enough to go around after the city allocated most transportation funds to autonomous systems. That is when they came to him for help. And that is when drones began raining explosives on his division's personnel carriers.

His intelligence officer initially suspected the traffic camera network had been hacked, enabling the drones to find–and strike–coalition vehicles with lethal precision. But even after he had made the call to shut it down, the attacks continued. Their next working hypothesis was that the enemy had compromised the 5G network somehow, using it to geolocate his troops. Consequently, the division took the city's wireless broadband offline as well, and with it the sensors monitoring

Lieutenant Colonel Robert J. Ross is the Information Warfare Team Lead in the Army Cyber Institute at the United States Military Academy (USMA) located at West Point, New York. Lieutenant Colonel Ross leads a 7-person, multi-disciplinary research team dedicated to expanding the Army and the nations body of knowledge on cyber and information-age conflict. He has a B.S. in Computer Science from Rowan University, an M.S. in Computer Science from Monmouth University, and a Ph.D. in Information Science from the Naval Postgraduate School. Additionally, Lieutenant Colonel Ross is an assistant professor in the Electrical Engineering and Computer Science Department at USMA, teaching primarily information technology courses. Lieutenant Colonel Ross' is currently a cyberwarfare officer and former artilleryman with two combat deployments to Iraq. His research interests are organizational science, strategic foresight, information warfare education, and digital economics.

and directing traffic. Gnok's streets were at a standstill, first responders were immobilized, and ongoing cyber-attacks were slowly degrading other essential services. Larsen contemplated a conundrum: "How is it possible to succeed in the physical occupation, while at the same time lose all control of the city? We are about to lose the people as well." A Smart City-led insurgency was the last thing he needed...

INTRODUCTION

Inter-connectivity is designed to increase the efficiency of city government operations and the quality of life for its citizens. It decreases costs and increases the municipal government's ability to efficiently manage the flow of traffic, control emissions, manage waste, and direct first responders. The goals of these, and many other Smart City initiatives, are to improve the quality of life for the city's residents, increase economic competitiveness, and achieve sustainability. The trade-offs for technologies that enable municipal digital transformations are the vulnerabilities that accompany any networked technology. Smart City technologies come with a panoply of vendors and other stakeholders, each with competing visions for the future. As the world becomes more urbanized and technologies become cheaper and more readily available, their use throughout cities in the industrialized and non-industrialized world will become more prevalent. The ramifications for military planning and operations increases in parallel. Smart Cities will become the status quo operating environment for urban military operations of the future. Occupying military forces will be responsible for the governance of these technologically controlled cities, particularly at the conclusion of large-scale military conventional operations (LSCO).[1] Future military forces must understand the implications for complex network ecosystems or risk ceding control over urban areas to the adversary during the return to competition phases of Multi-Domain Operations (MDO).[2] The

Greg Lindsay is a non-resident senior fellow of the Atlantic Council's Foresight, Strategy, and Risks Initiative, a senior fellow of MIT's Future Urban Collectives Lab, and director of applied research at NewCities. He speaks frequently about cities and technology, most recently at the United States Military Academy, Sandia National Laboratories, the U.K. Treasury, the OECD, Harvard Business School, and the MIT Media Lab. His writing has appeared in *The New York Times*, *The Wall Street Journal, The Atlantic*, *The New Republic*, and *World Economic Forum*, among many other publications.

Preface illustrates what could play out as a result of underestimating the impact of connected infrastructure during post-conflict operations in the networked urban environments of tomorrow. The scenario outlined above raises the specter of physically occupying urban terrain while losing control of the city.

Smart City initiatives are multiplying at an accelerated pace.[3] As of this writing, hundreds of Smart City pilot projects seek to make urban dwelling more sustainable by leveraging automation and digitizing interactions among technologies, people, and the physical environment. Each project is an ecosystem, with stakeholders ranging from government officials and technology firms with their near infinite supply chains to city residents. Many projects that began as experimental pilots are now integral to the way city government organizations deliver services to their constituents. Many more will follow.

An increasingly urbanized world, rapidly becoming more dependent upon technologies, adds ever greater complexities to future military operations. This article explores not only the implications these technologies will present to future military planners, but also proposes a framework for conducting joint intelligence preparation for military staff planning such operations in urban environments. Complex military operations begin with understanding the operational environment. The process by which the US military does this is the Joint Intelligence Preparation of the Operational Environment (JIPOE).[4] The complexity of digital ecosystems, their profound impact on city dwellers, and the potential opportunities and vulnerabilities they present to military commanders should be considered during that process. The authors propose here a framework that will enable the military intelligence community to begin designing a repeatable process to assess the Smart City environment and its impact on future military operations. More broadly, this framework can be used in the strategic planning process to aid in

identifying, visualizing, and communicating this information, and as a way to begin considering current gaps in military capabilities to disrupt, mitigate, or exploit these issues.

METHODOLOGY

The authors leveraged a combination of qualitative methodologies to identify key technological trends being adopted by municipal governments worldwide. Subsequently, the implications these technologies pose for future military operations in urban environments were derived. Three salient trends were identified after a comprehensive review of the literature on Smart City pilot projects implemented in urban areas throughout the world: autonomous mobility, machine-aided decision-making, and sustainability. These trends contained the primary data points to begin the process of Threatcasting, which is a strategic foresight methodology using narrative-building exercises dependent upon inputs from diverse groups of subject matter experts or knowledgeable agents.[5], [6] The contributing group was comprised of researchers with expertise in information warfare, cybersecurity, and urbanization. The Threatcasting process was used to derive several narratives describing a protagonist experiencing future threats, such as the one found in the Preface, after a series of remote and in-person interactions.

Threatcasting scenario modelling was conducted with the aid of a hypothetical adversary mission intended to influence the fictitious city government to withdraw from its security assistance agreement. The adversary sought to achieve its goals by disrupting government functions, eliminating the advantages of friendly exploitation of Smart City systems, and maintaining a foothold in these systems to retain the same advantages. This scenario was modelled to take place approximately ten years in the future. Each narrative derived from the scenario identified the importance for the adversary of keeping Smart City digital ecosystems operational to cause misattribution of violence and civilian suffering, and to discredit the occupying military force and host municipal government.

Upon completion of the narratives, the authors analyzed them using a methodology known as Thematic Analysis.[7] The Thematic Analysis process entailed decoding salient themes discovered within each of the narratives. Identifying the patterns of similar and dissimilar themes of each enabled the authors to identify inductively potential impacts of cyber-physical Smart City systems on urban military operations.[8] The combination of these qualitative methodologies was chosen as a method to provide description and a plausible explanation for the complexity that will be experienced by military forces operating in future urban environments.

SMART CITY TRENDS

The authors reviewed over 100 Smart City initiatives around the world, both past and present.[9] These initiatives, while interconnected in many ways, can be categorized as autonomous mobility, machine-aided decision making, and sustainability. These three technological

trends support the overarching goals and objectives of Smart City projects: sustainable urbanization, more efficient allocation of resources, and improved quality of life for city residents.

Autonomous Mobility

Municipal governments worldwide intend to use autonomous transportation to reduce congestion sharply and decrease private car ownership. By some estimates, driverless cars will quadruple today's highway capacity of 2,000 cars per lane per hour, to 8,000.[10] While the public trust in autonomous vehicles has declined due to recent fatalities, many cities worldwide are continuing to adopt technologies such as autonomous park shuttles and rail carriages.[11] As of this writing, over 70 global rail systems are equipped with trains capable of unattended operations such as closing doors, detecting obstacles, and reacting to emergencies.[12]

In the European Union, 47 participant organizations from academia, government, and the private sector deployed fleets of 10-passenger driverless vehicles in Italy, France, Switzerland, Finland, Greece, and Spain as part of a four-year, €15 million European Commission CITYMOBIL2 project.[13] In North America, New York City, Tampa, Ann Arbor, Columbus, and Las Vegas are testing vehicle-to-vehicle communications to enable building roads with built-in safety features. This technology connects vehicles to devices transmitting data about direction, speed, and location to roadside equipment, which sends it in turn to other vehicles, along with information from traffic light countdown, pedestrian presence, and cyclist sensors.[14]

Machine-Aided Decision-Making Affecting Changes in the Physical Environment

Advances in data collection, storage, and processing capabilities dramatically shorten the time between information inputs and decisions. The right data coupled with the right algorithm can help public officials gain insights into patterns of city-resident interactions and make decisions on improving infrastructure, optimizing the use of government resources, and enhancing public safety. Urban sustainability strategies outline objectives around more efficient sanitation management, energy utilization, traffic congestion, street parking, and other issues.

As an example, Milton Keynes' "data hub" was featured in the 2017 World Bank Internet of Things (IoT) report. Milton Keynes, a city in the United Kingdom with a population of 230,000, developed a central repository of data from an array of sensors, such as weather, traffic, lighting, trash bins, parking, satellite imagery, and air monitors.[15] The city made these data available via an application programming interface (API) to "inform analytics at different levels of detail to support intelligent planning and usage of resources across city systems."[16]

Another example is Barcelona, one of the "smartest" cities in Europe and host to the annual Smart City Expo World Congress. This city has implemented a range of systems affecting change in the physical environment based on sensor data. One example is a self-regulating park irrigation system that controls water delivery valves based on rain and humidity data. Another involves sensor-equipped trash bins able to detect weight and the presence of

hazardous materials, making collection more efficient.[17] Several international cities have installed under-asphalt weight sensors to guide city residents to open parking spaces. Yet another commonly adopted technology allows traffic lights to change their timing based on real-time traffic data.

Sustainability

Sustainability is an umbrella term encompassing a range of projects aimed at sustainable consumption of energy resources. These efforts include alternative energy production methods, zero-carbon initiatives, and energy conservation projects. Networked technologies that inform autonomous and human decision-making will continue to play a pivotal role in the success and sustainability of these projects.

The CELSIUS project, adopted by Genoa, Cologne, Gothenburg, Rotterdam, and Islington, uses systems that redeploy excess heat produced at commercial facilities, such as data centers, or extracted heat from sewage and biodegradable materials to heat residential facilities in high-density urban areas.[18]

The GrowSmarter project, piloted in Barcelona, Cologne, and Stockholm, aims to reduce energy consumption and green-gas emissions by 60% through a range of interconnected Smart City solutions, including waste heat recovery, smart street lighting, and smart mobility solutions.[19]

Smart City technologies supporting autonomous mobility, machine-aided decision making, and sustainability goals have the potential to greatly improve public service delivery, while presenting risks to rapidly degrade the quality of life for urban societies, particularly in the context of military operations. In a growing number of recent examples potentially debilitating cyberattacks have occurred against networked critical infrastructure. In the first widely reported attack against cyber-physical systems since Stuxnet, in 2017 a group of Russian hackers gained remote access to commonly used power equipment and shut down segments of Ukraine's power grid.[20] In April 2020, Iran attempted to penetrate Israel's water treatment facility "to mix chlorine or other chemicals into the water supply," resulting in the shutdown of agricultural pumps.[21] Sudden loss of critical services such as potable water and electrical power during stability operations are just two possible nightmare scenarios.

By the very nature of their functional requirements, Smart City devices are always on, continuously communicating with other system components. Their attack surface is always visible to malicious actors. Coupled with often poor situational awareness by owners and operators of these ecosystems, the sprawling attack surface provides ample opportunities for attackers to exploit these systems without notice.

Due to the relatively low opportunity cost, adversaries will continue attempting to exploit vulnerabilities in cyber-physical infrastructure to achieve their operational and strategic objectives, especially in situations where they lack conventional military advantage. Military forces conducting operations in future urban environments must identify and understand the

vulnerabilities inherent in Smart City technologies. Grasping the potential effects of adversaries exploiting these systems must occur during the planning phases prior to operations.

PLANNING CONSIDERATIONS

As the three trends outlined above materialize into everyday reality in cities, military planners will face increasing challenges if they misestimate role of digital ecosystems in supporting city life. As with any complex problem, it is helpful to break the problem down into components and visualize the relationships between those components.

Autonomous mobility, machine-aided decision-making, and sustainability are three functional categories introduced as salient Smart City trends discovered within the literature on urban pilot programs. Each category has been developed for a unique purpose; however, the components that comprise systems within each category have similar functional characteristics. At a minimum, the digital ecosystems comprising each category contains sensors that measure the current state of an object (e.g., temperature, weight, location, and velocity). Measurements obtained by sensors effect physical changes to an object's state (e.g., acceleration of a vehicle, turning a valve, changing the voltage in a power system) to achieve a desired end state. These same concepts are comparable to current industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems and are extended to other applications of Operational Technology (OT) and Industrial IoT devices.

OT networks composed of systems that communicate with each other, rather than with human users, must be viewed as a part of the convergent technology gestalt during planning considerations. Other intermediary components that facilitate the collection, processing, analysis, and transport of data from sensors to controllers and actuators will be introduced below. Smart City digital ecosystems are comprised of physical objects and digital devices that inform each other's state in a continuous cycle which is depicted in the Figure below.

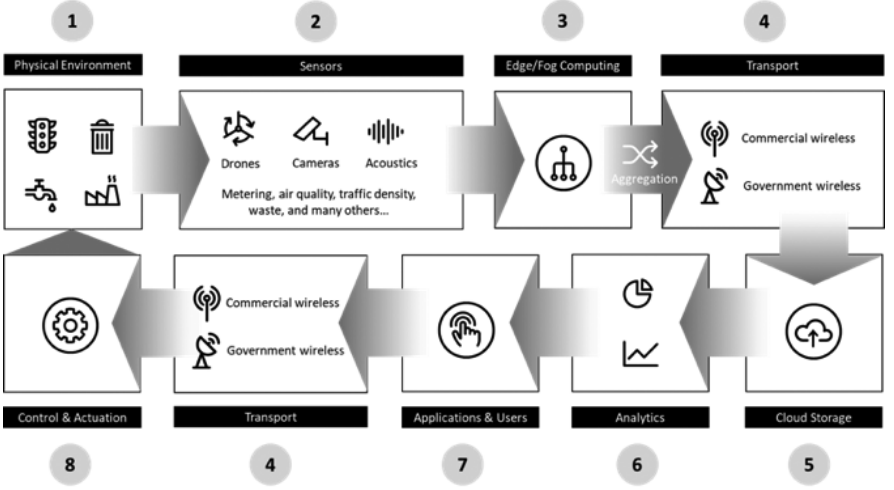


Figure 1: Common Smart City Ecosystem Components

The authors propose the following definitions for components depicted in the image above:

1. Physical environment contains physical objects that are affected by force applied to them through controllers and actuators for the purpose of changing their state.

2. Sensors measure the state of an object, convert analog measurement into digital signal, and transmit that signal over wires or a frequency within the radio spectrum. Data collected by the sensors may be transmitted to centralized computing and storage resources in the cloud or enterprise data centers, or to edge computing nodes for initial processing.

3. Edge computing systems collect digital signals near the source of the data, apply transformation to the data (e.g., selection of relevant fields or rearranging of fields into a common data model), and make decisions regarding which data should be sent further upstream (e.g., send to the cloud only data that indicate a change from the last known state). Fog computing extends cloud computing to the edge of the enterprise network decentralizing data processing activities across several local devices. As opposed to edge computing, which processes data on the sensor devices, fog computing places intelligence within processing hubs on the same local area network.

4. Data **transport** networks facilitate the transfer of data in real time from local devices to traditional data centers or the cloud. While the data can be transferred over the wire, wireless technologies play an increasingly central role in enabling the transfer of data from the enterprise network to the cloud. Furthermore, the rollout of 5G technology promises to provide the bandwidth, low latency, reliability, and increased network capacity required to accelerate adoption of Smart City technologies.[22] The features offered by 5G technology, particularly as they relate to mission-critical reliability, will extend the application of Industrial IoT use cases being piloted and adopted by cities worldwide.[23] Today, there are two primary operating models used to facilitate the transport of data: government wireless broadband networks (which may be owned and operated by a chain of private sector vendors and leased by the municipal government for its exclusive use), or commercial wireless broadband networks.

5. Remote **cloud** computing and storage facilitate the necessary on-demand elasticity and scalability to collect and process vast amounts of data from many millions of devices within a digital ecosystem. For the purpose of this analysis, storage and processing of data within data centers owned and operated by third-party providers present an additional layer of opportunity for attackers.

6. Analytics platforms, which may be extended components of the cloud computing platform or fourth-party Software-as-a-Service tools, filter and further transform the data, then stream them through an analysis engine to make decisions on the required alteration of an object's state. Analytics engines apply algorithms to data pre-processed at the edge to extract actionable insights within or across data sets.

7. Application is the layer where users of an ecosystem interact with its components. This layer may be used to customize analytic models, override or halt autonomous processes, or interact directly with controls and actuators. Autonomous OT operations are also configured and monitored at this layer.

8. Actuators change the state of physical objects by receiving digital signals over optical fiber, copper wire, or radio, converting digital signals into electrical pulses which excite physical objects into motion. Other types of **controllers** may change the display on a billboard or traffic signal, or input to another system.

During the planning process, the ecosystem components described above should be further decomposed into devices and nodes, with a mapping of interdependencies between the nodes. Each of those nodes should then be examined in the context of vulnerabilities or the opportunities it presents to both friendly and enemy forces.

Table 1: Operational Advantages and Effects

Component	Potential Operational Advantages	Enabling Effects
1. Physical Objects	• Remotely, controlled machinery supporting critical services—such as water treatment—may be physically destroyed in order to influence city residents' sentiment. • Delivery of power or connectivity may be disrupted or disabled to render physical objects inoperative.	• Physical Destruction • Disruption in Energy Supply or Communication
2. Sensors	• May provide additional intelligence, surveillance, and reconnaissance capabilities through legitimate or illegitimate access. • May be disabled through physical destruction or denial of service to counter adversary surveillance, or to disrupt government services. • May be used as nodes in covert mesh communication networks. • Sensors can be spoofed in order to transmit false data to computing devices.	• Physical Destruction • Endpoint Denial of Service • Device Spoofing
3. Edge Computing	• May be leveraged as data interception nodes. • Data altered at points of collection may result in misleading representation of ground truth. • May be used as entry points into upstream networks. • Traffic may be forwarded to unauthorized destination.	• Physical Destruction • Exfiltration • Transmitted Data Manipulation • Runtime Data Manipulation • Endpoint Denial of Service
4. Transport	• Capabilities can be integrated into Primary, Alternate, Contingency, Emergency (PACE) planning to augment limitations and vulnerabilities of line-of-sight and satellite radios. • May be used for device geolocation and precision physical and logical targeting.	• Physical Destruction • Exfiltration • Network Denial of Service
5. Cloud Storage	• Access to cloud-based services can be temporarily disabled through bandwidth or resource depletion denial of service attacks, causing disruption of government services during critical temporal junctures.	• Network Denial of Service • Stored Data Manipulation
6. Analytics	• Unauthorized access to analytics platforms allows altering decision algorithms, directing controls and actuators to effect desired change in the physical environment.	• Runtime Data Manipulation
7. Applications	• Access to applications can be denied at critical locations through application-level attacks. • Access to underlying data through application-level attacks can aid in surveillance and targeting efforts.	• Endpoint Denial of Service • Runtime Data Manipulation • Account Access Removal
8. Control/ Actuation	• May be used to effect changes in the physical environment at the device or remotely via ecosystem components. • Center of gravity in shaping attitudes of city residents about intention and competence of municipal government and foreign forces.	• Physical Destruction • Device Spoofing • Transmitted Data Manipulation

Table 1 represents common Smart City ecosystem components supporting any of the three functional categories—autonomous mobility, machine-aided decision making, and sustainability—and presents potential operational advantages provided to either friendly or adversary forces through legitimate or illegitimate access. The authors did not attempt to create a comprehensive list, instead depicting only some of the possible advantages and enabling effects. The planning process should reflect the current state of intelligent infrastructure within urban space specific of a particular environment.

PROPOSITIONS

Rapid urbanization and adoption of Smart City technologies are creating "conditions, circumstances, and influences" that will be exploited by future adversaries, particularly by militarily inferior state and non-state actors.[24] The Joint Intelligence Preparation of the Operating Environment (JIPOE) process requires joint force staff to define and describe the operating environments holistically using a systems perspective.[25] However, this macro-analytical process does not specifically account for the unique implications, cognitive and technical, posed by technologies that connect digital networks with the physical environment and exert an influence on the latter. The same is true on the micro-analytical level. While the U.S. Army's Intelligence Preparation of the Battlefield (IPB) process can be used to address informational and cognitive aspects of the operational environment, high-level cyberspace considerations are relegated to an appendix of the IPB application doctrine, and do not explicitly discuss implications for operating in digitally networked urban environments.[26]

The US military envisions the future operational environment as increasingly urbanized; however, the challenges anticipated with operating in that environment are primarily classified as physical and social, drawing on the lessons of recent conflicts in the Middle East.[27] A framework is urgently needed to layer understanding of rapid technological advances in the areas of autonomous mobility, machine-aided decision- making, and sustainability with military strategic planning.

The authors propose that military planners consider the following set of questions in order to understand the impact of Smart City infrastructure on future operations. These questions will help anticipate potential vulnerabilities in force protection, counterintelligence, and civil considerations, and aid in identifying opportunities for exploitation. More broadly, they can be used to formulate a framework for identifying, visualizing, and communicating this information as a way to begin considering—on a strategic level—current gaps in military capabilities to disrupt, mitigate, or exploit these issues, and developing solutions.

I. What are the essential government services that leverage technological advances in autonomous mobility, machine-aided decision making, and sustainability?

Planners should first identify services that are critical to the sustainment of life and safety of city residents. Next in order are services essential to the economic well-being of the city. Last

are services that aim to improve the quality of life for residents. Information should be collected on organizations and identities of "business owners" and stakeholders of essential services.

II. What are the components that make the delivery of those services possible?

Once services and their owners are identified, planners should identify the traversal path of the signal lifecycle, from sensor to actuator or controller for each essential service. This analysis will identify key technical components that make the delivery of a specific service possible. During this stage, technology owners of a given essential service should also be identified. These may be specific groups within the city's centralized Chief Technology Officer or Chief Information Officer functions, or within similar groups at organizations responsible for the delivery of services under consideration. At this level of analysis, the type of components represented in the table above should be identified and visualized.

III. What are the devices that make up components of the ecosystem?

High-level components are made up of physical devices that play a specific function in the signal's lifecycle. Planners should identify as many of those devices as feasible, including makes and models. To the extent possible, planners should identify parties responsible for operations and maintenance of those devices. These parties may be government employees, prime contract vendors, manufacturers, or any combination of the three. Network device tracking tools should be identified, and devices that make up the subcomponents of a given ecosystem should be mapped by authorized systems. Identification and monitoring of authorized devices prevent nefarious network devices from entering these networks.

IV. What are the interdependencies between essential services, their components, and devices?

The objective of this step is to map out the entire "system of ecosystems" with the aim of identifying technical interdependencies. It is becoming increasingly likely that data collected and processed by one city organization for the delivery of its service are being shared with another organization. A service of this second organization may use the first organization's data along with other data types to produce decisions supporting the delivery of that service. Interdependency analysis will identify system nodes of an even higher priority. Emerging technologies that aid in the discovery of system dependencies (through agentless collection and analysis of network packets, for example) should be utilized when feasible, and represented as visual graphs.

V. What are the supply chain dependencies within the digital ecosystem?

Supply chains supporting complex systems are becoming nearly infinite. Nevertheless, or perhaps because of it, the supply chain remains the threat vector of choice for advanced attackers. Supply chain analysis should include the identification of Industrial IoT vendors and their suppliers, mapped to system and device components and potential vulnerabilities in those components. It should also include the identification of the digital supply chain dependencies

such as code compilers.[28] Supply chain visibility is needed for increased vigilance, but most importantly for the city's reliance on those systems. While it is the city government's primary responsibility to identify supply chains and require primary contract vendors to conduct resilience and recovery exercises with their suppliers, military planners should map out supply chain dependencies to be able to support recovery operations as situations require.

VI. What operational and strategic advantages may be gained by friendly or adversary forces through legitimate or illegitimate access to ecosystem components and devices?

Given both the friendly and enemy missions with respect to a given urban environment, planners should consider how control of the digital ecosystems may assure or accelerate mission success. Further analysis in this step will identify components or devices that may facilitate this success. It is also important to consider during this step which components and devices, when subjected to degradation or destruction, may alter the lives of city residents significantly enough to delay mission fulfilment, or cause the tide to turn in another direction. Center of Gravity (COG) analysis may aid in the identification of cyber capabilities, requirements, and vulnerabilities that will yield the greatest operational gain.[29]

VII. What vulnerabilities are present in the devices that would allow the adversary to exploit them for their operational advantage?

Given the list of prioritized systems and devices, planners should identify Common Vulnerabilities and Exposures (CVEs) associated with those systems. Planners should also identify which systems are exposed to the Internet and conduct non-intrusive reconnaissance to assess the presence of those vulnerabilities within exposed systems. Adversary capabilities and intent to exploit those vulnerabilities in prioritized systems should also be assessed during this step.

VIII. What tactical effects should friendly or adversary forces seek to achieve to realize the operational or strategic advantages through legitimate or illegitimate access to ecosystem components and devices?

Cyber Operations Officers on the Joint Staff can help narrow down cyber effects that would enable friendly or adversary commanders to achieve operational or strategic advantages identified in the earlier phase of planning. While the U.S. Joint Cyberspace Operations doctrine lists cyber effects as secure, defend, exploit, and attack, it does not offer cyber planners at the operational level enough specificity to describe desired outcomes.[30] The authors suggest leveraging a commonly used taxonomy of adversarial behavior, such as MITRE ATT&CK framework.[31] The use of commonly accepted terminology will facilitate integration among military and civilian planners and operators, and cybersecurity researchers from both the public and private sectors.

- **Physical Destruction** of a device degrades or disables a service permanently.
- **Account Access Removal** impacts the availability of systems through the removal, locking or modification of user accounts.[32]

- **Endpoint Denial of Service** attack degrades the performance of a computing device through resource depletion, or causes a persistent crash condition.[33]
- **Network Denial of Service** attack degrades or blocks access to systems by users or other systems through network bandwidth depletion.[34]
- **Runtime Data Manipulation** modifies information displayed to users or transmitted to other systems in order to alter business processes and/or human or machine-based decision-making processes.[35]
- **Stored Data Manipulation** through inserting, deleting, or manipulating data at rest with the intent of altering business processes and/or human or machine-based decision-making processes.[36]
- **Transmitted Data Manipulation** through manipulation of data in transit to storage or other systems with the intent of altering business processes and/or human or machine-based decision-making processes.[37]
- **Exfiltration** is a category of techniques that facilitate the unauthorized transfer of data out of the target network or device.[38]
- **Device Spoofing** exploits trusted communications by inserting rogue devices into the network that masquerade as legitimate devices and introduce false and/or misleading signals into the system.

The eight questions above are tailored for military staffs preparing their forces to conduct urban operations. These questions are intended, until formally written into military doctrine, to supplement the intelligence preparation process. Understanding the effects of Smart City technologies and how adversaries will exploit them as a method for influencing local populations and governments within urban areas controlled by military forces is paramount for success in any future military operation. These questions are part of a continuous intelligence process that should last throughout the entirety of any operations within future urban environments. As the uncertainty about each question is reduced, the information will contribute to the joint force commander's (JFC) decision-making on how to react holistically in defending against the exploitation of these technologies, as well as the cognitive effects on local populations.

CONCLUSION

The threat effects experienced by Major General Larsen and his troops in the Preface of this article may have been disrupted or mitigated, or the division may have been prepared to recover from them, had the commander's staff planned using the supplemental questions proposed in this article during their intelligence preparations for operations in the fictional Smart City of Gnok. The Commander's Operations, Intelligence, Electronic Warfare, Cyber, and Information Operations staff answering these supplemental questions would have identified vulnerabilities in the city's digital infrastructure. With this knowledge the division would have the potential

to disrupt adversarial attempts to exploit these vulnerabilities or raise them as threats to the division's mission. Answering the supplemental questions during intelligence preparation and then wargaming against them during the division's military decision-making process (MDMP) would have provided Major General Larsen's division a far greater chance of success.

This article defined three key trends—autonomous mobility, machine-aided decision-making, and sustainability—affecting future military operations in urban environments. It defined a generalizable, yet complex, technical ecology and the nefarious implications they pose within the context of military operations. Finally, the article proposed eight questions that are intended to supplement and enhance current intelligence preparation doctrine found at the strategic, operational, and tactical levels of warfare. The answers to these proposed questions are intended to define how adversaries may exploit urban COG technologies, and thus affect the way in which commanders bring capabilities to bear in defending against these exploitive efforts during future military operations in urban environments.[39]

US military staff planners working for global combatant commands, in conjunction with our allies and strategic partners, should start preparing for this and similar scenarios now. They should start by identifying, collecting, and cataloguing Smart City technologies being adopted by major urban areas throughout the world in the form of a high-level running estimate. This information should be included in the updating and development of contingency plans for military operations in major urban areas throughout their areas of responsibility. Supplementing the current JIPOE process with the techniques proposed in this article will help develop understanding of, and forge relationships with, the relevant urban governments and their commercial industry partners managing Smart City technologies.

Once situational awareness—at a technical level—of Smart City ecosystems in major urban centers has been obtained, future research on this topic is needed to identify capability gaps in force structure, along with requirements to disrupt, mitigate, or exploit these issues during urban combat operations of the future.

ACKNOWLEDGEMENTS

The authors thank Colin Ahern (Deputy Chief Information Security Officer, City of New York) for contributions to this article and for providing insightful comments on early drafts of the manuscript.

NOTES

1. "Field Manual 3.0: Operations," (2017), 1-1.
2. "Training and Doctrine Command Pamphlet 525-3-1: The U.S. Army in Multi-Domain Operations 2028," Department of the Army (Washington, DC: U.S. Department of the Army 2018), iii.
3. "Smart Cities–Adoption of Future Technologies," *World Engineering Day* online, January 2020, https://worldengineeringday.net/wp-content/uploads/2020/03/Smart-City-IOT-WFEO-Version-1.pdf.
4. "Joint Publication 2-01.3: Joint Intelligence Preparation of the Operational Environment," United States, Joint Chiefs of Staff (2014).
5. Natalie Vanatta and Brian David Johnson, "Threatcasting: A framework and process to model future operating environments," *The Journal of Defense Modeling and Simulation* 16.1 (2019), 79-88.
6. Dennis A. Gioia, Kevin G. Corley, and Aimee L. Hamilton, "Seeking qualitative rigor in inductive research: Notes on the Gioia methodology," Organizational Research Methods 16.1 (2013), 15-31.
7. Richard E. Boyatzis, *Transforming qualitative information: Thematic analysis and code development* (Sage, 1998).
8. Kathy Charmaz, *Constructing grounded theory* (Sage, 2014).
9. "List of Smart City Projects," Nominet, October 10, 2018, https://www.nominet.uk/list-smart-city-projects/.
10. Emily Badger, "Pave Over the Subway? Cities Face Tough Bets on Driverless Cars," *The New York Times* online, July 20, 2018, https://www.nytimes.com/2018/07/20/upshot/driverless-cars-vs-transit-spending-cities.html.
11. "Ground Rapid Transit," Get There, accessed January 3, 2020, https://www.2getthere.eu/group-rapid-transit/.
12. Wikipedia, 2020, "List of Automated Train Systems," last modified December 31, 2019, https://en.wikipedia.org/wiki/List_of_automated_train_systems.
13. "Cities Demonstrating Cybernetic Mobility," European Commission CITYMOBIL2, accessed January 3, 2020, https://cordis.europa.eu/project/id/314190.
14. Andrew Macleod, "Autonomous Driving, Smart Cities and the New Mobility Future," Siemens, accessed January 3, 2020, https://www.techbriefs.com/autonomous-driving-smart-cities-and-the-new-mobility-future/file.
15. "Internet of Things. The New Government to Business Platform: A Review of Opportunities, Practices, and Challenges," The World Bank Group, 2017, http://documents.worldbank.org/curated/en/610081509689089303/pdf/120876-REVISED-WP-PUBLIC-Internet-of-Things-Report.pdf.
16. "MK Data Hub," MK: Smart, accessed on January 3, 2020, http://www.mksmart.org/data/.
17. "Seven Ways that Barcelona Is Leading the Smart City Revolution," *Edie Newsroom,* December 12, 2018, https://www.edie.net/news/7/Seven-ways-that-Barcelona-is-leading-the-smart-city-revolution/.
18. "CELSIUS: Combined Efficient Large Scale Integrated Urban Systems," EU Smart Cities Information System, accessed January 3, 2020, https://smartcities-infosystem.eu/sites-projects/projects/celsius.
19. "GrowSmarter: Transforming Cities for a Smart, Sustainable Europe," EU Smart Cities Information System, accessed January 3, 2020, https://smartcities-infosystem.eu/sites-projects/projects/growsmarter
20. Andy Greenberg, "'Crash Override': The Malware That Took Down a Power Grid," *The Wire* online, June 12, 2017, https://www.wired.com/story/crash-override-malware/.
21. "Cyber attacks again hit Israel's water system, shutting agricultural pumps," *Times of Israel* online, July 17, 2020, https://www.timesofisrael.com/cyber-attacks-again-hit-israels-water-system-shutting-agricultural-pumps/.
22. Sagar Paliwal, et al., "5G as the Principal Enabler Towards the Establishment of 'IoT' Society," paper presented at 2017 International Conference on I-SMAC, Palladam, India, February 10-11, 2017.
23. Liz Centoni, "How 5G Will Accelerate Industrial IoT," Cisco, October 17, 2019, https://blogs.cisco.com/news/how-5g-will-accelerate-industrial-iot.
24. "Joint Publication 2-01.3: Joint Intelligence Preparation of the Operational Environment," United States, Joint Chiefs of Staff (2014), I-1.
25. Ibid.
26. "Army Techniques Publication 2-01.3: Intelligence Preparation of the Battlefield," United States, Department of the Army (2019), Appendix D: IPB Cyberspace Considerations.
27. "TRADOC Pamphlet 525-92-1: The Changing Character of Warfare: The Urban Operational Environment," United States, Department of the Army (2020).

NOTES

28. Yong Kang, et al., "XcodeGhost: A New Breed Hits the US," FireEye Threat Research, November 3, 2015, https://www.fireeye.com/blog/threat-research/2015/11/xcodeghost_s_a_new.html.
29. Rock Stevens, Daniel Votipka, Elissa M Redmiles, Colin Ahern, Patrick Sweeney, and Michelle L Mazurek, "The battle for New York: A case study of applied digital threat modeling at the enterprise level," in 27th {USENIX} Security Symposium {USENIX} Security 18.
30. "Joint Publication 3-12: Cyberspace Operations," United States, Joint Chiefs of Staff (2018), II-5.
31. "MITRE ATT&CK Matrix™ for Enterprise," MITRE ATT&CK, last modified October 9, 2019, https://attack.mitre.org/matrices/enterprise/.
32. "MITRE ATT&CK Matrix™ for Enterprise: Impact Techniques," MITRE ATT&CK, last modified July 25, 2019, https://attack.mitre.org/tactics/TA0040/.
33. Ibid.
34. Ibid.
35. Ibid.
36. Ibid.
37. Ibid.
38. "MITRE ATT&CK Matrix™ for Enterprise: Exfiltration," MITRE ATT&CK, last modified July 19, 2019, https://attack.mitre.org/tactics/TA0010/.
39. "Joint Publication 2-01.3: Joint Intelligence Preparation of the Operational Environment," United States, Joint Chiefs of Staff (2014), I-1.

The Cyber Defense Review

Research Notes

Prioritizing SOF Counter-Threat Financing Efforts in the Digital Domain

Hugh Harsono

ABSTRACT

Threat financing describes how threat actors move, manage, and raise funds to support their specific goals. One emerging challenge for Special Operations Forces (SOF) support to counterterrorism missions is digital threat financing. This has risen to prominence in recent years with the evolution of digital currencies, cashless payments, and other forms of financial technology that allow for the near-instantaneous transfer of funds from one party to another. As such, SOF must undertake and prioritize counter-threat finance (CTF) efforts for its Theater Special Operations Commands (TSOCs) and its intelligence analysts to deter violent extremist organizations (VEO).

Keywords: *digital threat financing, counter-threat financing, cryptocurrency Campaigns*

INTRODUCTION

Special Operations Forces (SOF) routinely combat threats to the United States, with a specific focus on counterterrorism and counter-violent extremist organizations (CT/CVEO) missions. These efforts include the disruption and surveillance of enemy networks, direct-action missions, and partner-nation capacity building in advise-and-assist roles, among many others. While demonstrating great success at the tactical level, there is a clear need for "more sophisticated counterterrorism training and exchanges that specifically seek out and address the financial aspects of terrorist and VEO operations," argues SOF Colonel Clarence Bowman.[1] *Additionally, the Integrated Financial Operations Commander's Handbook*, which was developed with counter threat-finance

First Lieutenant Hugh Harsono is an Army officer most recently assigned as an Assistant Operations Officer in an Asian-based Special Operations Task Force. His previous military assignments have taken him throughout the Middle East and Asia, and he has served at various levels within the special operations enterprise. He holds a B.A. from the University of California, Berkeley, with a major in economics. Prior to commissioning through the United States Army Officer Candidate School at Ft. Benning, Georgia, Hugh worked in finance for an agrotechnology firm.

activities in mind, specifically mentions that it does not "adequately address counter-threat finance (CTF) activities designed to deny, disrupt, destroy, or defeat financial systems and networks that negatively affect US interests."[2] Keeping this in mind, SOF must begin to address the root causes supporting terrorist/VEO actions, understanding that a critical factor of these root causes revolves around threat financing. As a result, the SOF community must continue to refocus its priorities of effort and dedicate increasing resources to counter-threat finances to provide a long-term solution for CT/CVEO concerns.

Counter-threat financing is a particularly critical factor for SOF to address, given U.S. Special Operations Command (SOCOM) is the "DoD CTF lead component for synchronizing DoD CTF activities and operations."[3] CTF efforts apply to various threat actors, including hostile governments, violent extremist organizations, and paramilitary groups. This is critical because threat actors require financial resources to carry out their specific activities. Today, threat groups often fund these activities utilizing tactics ranging from criminal activities to the taxation of a local populace and online fundraising.[4] In fact, the U.S. Department of the Treasury estimates place similarly-raised Islamic State funds at over $1 billion in total revenue for 2015 alone.[5] Countering threat financing is becoming an increasingly important role within the SOF community. Understanding why it must receive such an intense focus will allow SOF elements to play an effective role in CT/CVEO.

HAWALAS: A TIME-HONORED CODE WITH DIGITAL POTENTIAL

The *hawala* system is a popular informal banking network and money transfer mechanism utilized primarily in the Middle East, North Africa, the Horn of Africa, and the Indian subcontinent.[6] Hawala forgoes modern banking technology in favor of a time-tested

network of honor-bound money brokers, also known as *hawaladars*,[7] who move funds without concern for specific nation-state borders or banking system rules. The hawala system is especially appealing to threat actors due to its relatively untraceable nature and ability to mobilize funds quickly from around the globe.[8] Despite the longstanding popularity of hawala, cryptocurrency has gained traction among an ever-increasing pool of users worldwide in recent years. More popularly known through brands such as Bitcoin, Ripple, and Ethereum, cryptocurrencies are peer-to-peer, public, and open-source digital platforms that also possess the ability to facilitate the movement of money with relative anonymity. This ability also makes cryptocurrency popular among threat actors, from fundraising in the Gaza Strip by the Ibn Taymiyya Media Center[9] to the allegation of digital currency used to help organize the ISIS-backed 2019 Sri Lanka Easter bombings.[10]

However, as efficient as the hawala system may be, younger generations are more often in tune with the utilization of the Internet in conducting everyday transactions,[11] to include money movement among different nation-states and groups. As such, digital currencies have, in some ways, replaced the hawala network, allowing individuals to bypass the socialized and relationship-based nature of the hawala in favor of near-instant transactions.[12] Therefore, the US government must continue to monitor digital currencies for involvement in terrorist activity, enabling the disruption of specific funding, activities, and organizing of threat actors.

HOW DIGITAL CURRENCIES WORK

Digital currencies, also known as cryptocurrencies, have the potential to replace traditional banking systems, with their source of innovation coming from the blockchain construct. Utilizing conventional banking as an analogy, the blockchain is essentially a full historical log of banking transactions shared by all users.[13] However, unlike traditional banking, the blockchain is public and decentralized, providing a higher degree of transparency within the cryptocurrency construct. Therefore, the transfer of cryptocurrencies is 100 percent digital in nature and conducted between two individuals or organizations through online exchange platforms. This type of peer-to-peer transaction allows for a certain level of anonymity when using digital currencies.[14] This relatively anonymous framework emerges primarily in two forms: the tying of individuals to specific cryptocurrency accounts as well as the utilization of digital exchanges. The relatively anonymous nature of cryptocurrency has created significant differences in the enforcement of Know Your Customer/Anti-Money Laundering (KYC/AML) regulations across various nation-state borders.[15] This presents challenges in tying individuals to specific cryptocurrency accounts.[16] Similarly, the use of digital exchanges to transfer cryptocurrency into spendable money is also difficult to trace due to the relative fluidity of such exchange organizations.[17] Therefore, cryptocurrencies have become a kind of virtual hawala,[18] utilizing a network of connected digital actors to move specific amounts of money throughout the world.

Threat actors are continuing to expand their ability to maintain, store, and share funds among themselves, while taking advantage of a lack of oversight and regulations.[19] Consequently, with digital currencies allowing for the virtual movement of money that is protected under an umbrella of anonymity, it is vital for the SOF community to properly assess the threat for what it is: a difficult-to-trace way of funding threat actors, which has received insufficient emphasis in today's military. It is therefore incumbent on SOF to understand and counter the potential risk that digital threat financing poses to national security.

CAN SOF COUNTER DIGITAL THREAT FINANCING?

The SOF community has the unique ability to carry out a variety of missions throughout the world. However, its focus must shift from strictly kinetic engagements to cooperating with US partners. There are a variety of ways that SOF can utilize both current and emerging assets to provide further emphasis on the root funding sources of terrorist/VEO groups. It is critical for SOF to increase CTF personnel presence at Theater Special Operations Command (TSOC) unit level, as well as providing more emphasis on digital financial intelligence (FININT) collection.

Some readers may pose the question, "Why SOF?" Other organizations are already tackling the problem of threat financing, including the National Security Agency, the State Department,[20] and the Federal Bureau of Investigation-led National Cyber Investigative Joint Task Force.[21] Additionally, many defense practitioners believe it is difficult to operationalize threat finance intelligence efforts. However, the increasingly digital-exclusive nature of finance requires increased coordinated efforts between all government and law enforcement entities, necessitating SOF-led Department of Defense (DoD) involvement in such requirements. Additionally, SOF is the one entity most flexible and adaptable organization within the DoD, providing the military with the potential ability to action and operationalize any intelligence that emerges from CTF efforts.

SOF must begin to provide additional resources to staff CTF global requirements. Currently, USSOCOM has minimal personnel working on countering threat financing. This group is located within the Counter-Threat Finance Branch of USSOCOM's J-36 Transnational Threats Division.[22],[23] Despite an established ability to examine threat financing, the J-36 is extremely limited in size, with the Counter-Threat Finance Branch having less than a handful of individuals to tackle issues globally.[24] This framework helps consolidate information at the USSOCOM level. It demonstrates that USSOCOM is shifting its focus to emphasize and examine threat finance. Unfortunately, to create actionable objectives arising from CTF efforts, USSOCOM must increase CTF personnel presence at TSOCs to establish global reach and presence, specifically with an emphasis on digital fund payments and transfers. Establishing such a priority will drive the regionally aligned TSOCs to focus on CTF efforts specifically in their regions of responsibility and the digital domain, allowing a deeper understanding

of both area-based and online nuances regarding digital threat financing. Additionally, the joint nature of TSOCs provides for a distribution of information within SOF, branching out to all the different service components within DoD and providing further engagement to each subordinate component cyber group. Ultimately, distributed CTF personnel will allow for tailored region-specific capabilities approach to be implemented much more effectively at the local level.

Additional emphasis must also be placed upon collecting digital FININT while ensuring that CTF efforts remain an emerging critical priority. This precise targeting method as a military strategy is particularly important, given the almost limitless area covered by the Internet. Therefore, if applied with extreme precision, CTF can be a useful tool for network disruption by tracking and potentially halting the monetary flow between terrorists and VEOs. FININT will continue to evolve in the digital realm regarding financial records, specific VEO-favored exchanges (such as those lacking in KYC/AML regulations), and much more. However, intelligence collectors must be aware and capable of exploiting and operationalizing FININT.[25] While traditional methods of tracking money flow between international organizations are notions that have been accepted and utilized for some time, the use of digital networks to transfer funds remains relatively new.[26] This creates a scenario where the value of such intelligence is through its recognition and interpretation, with careful analysis enabling the identification of specific items such as critical targets, monetary flow, and terrorist/VEO affiliates.[27] These digital trails can be followed by a careful collection of FININT, allowing SOF intelligence analysts to enhance their understanding of digital terrorist/VEO funding methods. Additionally, financial disruption strategies will enhance CT/CVEO operations with immense effect, ensuring a more sustainable way of effecting actions against threat actors. These efforts are possible only if FININT is prioritized and taught to intelligence collectors, with many of these individuals already having a presence within the SOF community.

SOF possesses a ready-made framework to help curb digital threat finance opportunities. With key stakeholder relationships created between strategic interagency and international partners, the SOF community already has a presence and intelligence collector ability to provide this shift in emphasis to CTF efforts. However, additional personnel must be placed at the TSOC level to increasingly effect CTF presence, while SOF intelligence collectors must be trained to identify and analyze FININT. These two critical opportunities offer other means to address threat actors in their tracks through countering digital threat financing.

CONCLUSION

Digital threat financing is an emerging issue with which SOF must swiftly contend. The emerging nature and use of digital currencies afford SOF the ability to shape the digital battlefield and develop the proper implementation actions to address this critical national security threat. SOF possesses the necessary tools to commit to such actions, and with its unique flexibility and skill in adapting to dynamic situations it is postured to be the premier US instrument to counter digital threat financing. In conjunction with the abilities of and cooperation with, other organizations, SOF can genuinely help make a difference on the frontline in curbing digital threat financing efforts.

NOTES

1. Clarence W. Bowman, *Countering Threat Finance as a Critical Subset of Irregular Warfare: An Interpretive Case Study of Northern Nigeria*; Report, Fort Leavenworth, KS: United States Army Command and General Staff College, 2009, 1-63.
2. Joint Warfighting Center, *Integrated Financial Operations Commander's Handbook*. Manual. Joint Concept Development and Experimentation, United States Joint Force Command, 2010, 1-126.
3. Jennifer E. Carter, *Emerging DoD Role in the Interagency Counter Threat Finance Mission*, Report, Fort Leavenworth, KS: United States Army Command and General Staff College, 2012, 1-34.
4. Howard Altman, "SOCOM Tracking Money that Funds Violent Extremists," March 29, 2015, accessed August 1, 2019, http://tbo.com/list/military-news/altman/socom-tracking-money-that-funds-violent-extremists-20150329/
5. Zachary Goldman, Ellie Maruyama, and Elizabeth Rosenberg, *Terrorist Use of Virtual Currencies*, Report, Washington DC: Center for a New American Security, 2017, 1-56.
6. Genesis Martis, *A guide to understanding hawala and to establish the nexus with terrorist Financing*, Report, Miami: Association of Certified Anti-Money Laundering Specialists, 2018, 1-25.
7. Martis, 9.
8. Financial Action Task Force, *The Role of Hawala and Other Similar Service Providers in Money Laundering and Terrorist Financing*, Report, "Paris: Organisation for Economic Co-operation and Development," 2013, 1-70.
9. Yaya J. Fanusie, "The New Frontier in Terror Fundraising: Bitcoin," August 24, 2016, accessed July 15, 2019, https://www.thecipherbrief.com/column/private-sector/the-new-frontier-in-terror-fundraising-bitcoin.
10. Yashu Gola, "ISIS Used Bitcoin to Fund Horrific Sri Lanka Easter Bombings, Research Claims". February 05, 2019, accessed August 10, 2019, https://www.ccn.com/isis-bitcoin-fund-sri-lanka-easter-bombings/.
11. Jaime Toplin, "Gen Z Banking & Payments Trends for 2020." May 1, 2019, accessed December 29, 2019, https://www.businessinsider.com/banking-and-payments-for-gen-z.
12. Atanu Biswas and Roy, Bimal, "Bitcoin, the new hawala," June 14, 2017, accessed August 10, 2019, https://economictimes.indiatimes.com/blogs/et-commentary/bitcoin-the-new-hawala/.
13. Australia Securities & Investments Commission, "Cryptocurrencies," October 24, 2018, accessed July 30, 2019, https://www.moneysmart.gov.au/investing/investment-warnings/virtual-currencies.
14. Australia Securities & Investments Commission, 2.
15. Allen & Overy Consulting, Cryptocurrency AML risk considerations, Report, "Legal and Regulatory Risks for the Finance Sector," 2018, 1-10.
16. Allen & Overy, 3.
17. Allen & Overy, 4.
18. Biswas & Roy, 2.
19. Cynthia Dion-Schwarz, David Manheim, and Patrick Johnston, 16.
20. Dana Priest and William Arkin, "A hidden world, growing beyond control," July 18, 2010, accessed August 5, 2019, https://www.pulitzer.org/cms/sites/default/files/content/washpost_tsa_item1.pdf
21. Brandon Gaskew, "Reader's Guide to Understanding the US Cyber Enforcement Architecture and Budget," February 21, 2019, accessed July 30, 2019, https://www.thirdway.org/memo/readers-guide-to-understanding-the-us-cyber-enforcement-architecture-and-budget.
22. Altman, 3.
23. House Committee on Armed Services Subcommittee on Terrorism and Unconventional Threats and Capabilities, 111th Congress, 7 (2009) (testimony of Matthew Levitt).
24. Kurt Gredzinski. "LinkedIn Profile," accessed August 10, 2019, https://www.linkedin.com/in/kurt-gredzinski-0a9b7315.
25. Joint Warfighting Center, 15.
26. Resty Woro Yuniar, "Bitcoin, PayPal Used to Finance Terrorism, Indonesian Agency Says,"World - Asia News. January 10, 2017, accessed October 18, 2017, https://www.wsj.com/articles/bitcoin-paypal-used-to-finance-terrorism-indonesian-agency-says-1483964198.
27. Shima D. Keene, "Operationalizing Counter Threat Finance Strategies," Paper, Carlisle. PA: U.S. Army War College, 2014, 1-51.

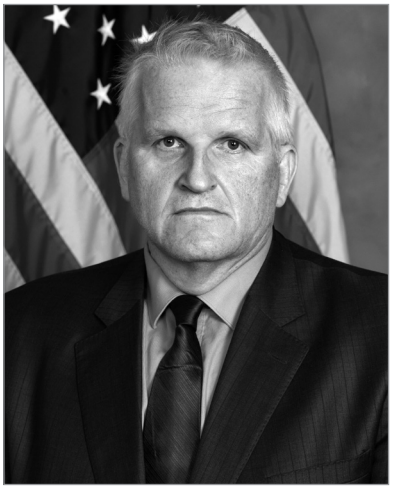
COVID-19: The Information Warfare Paradigm Shift

Jan Kallberg, Ph.D.
Rosemary A. Burk, Ph.D.
Bhavani Thuraisingham, Ph.D.

INTRODUCTION

Thomas Kuhn's *The Structure of Scientific Revolutions* highlights the critical term "paradigm shift," which occurs when it suddenly becomes evident that earlier assumptions are no longer correct. The plurality of the scientific community studying this domain accepts the change. These paradigm-shifting events can be scientific findings or, as in the social sciences, a system shock that creates a punctured equilibrium, triggering a leap forward acquiring new knowledge.

In information warfare, the government lines of effort have been to engage fake news, intercept electoral interference, fight extremist social media as the primary combat theater in the information space, and use the tools to influence a targeted audience to defend against an adversary that seeks to influence our population. The COVID-19 pandemic generates a rebuttal, or at least a challenge, of the information warfare assumption that our government's authority, legitimacy, and control are mainly challenged by tampering with the electoral system, fueling extremist views, and distributing fake political news. The fake news and extremist social media content exploit fault lines in our society and create civil disturbances, tensions between federal and local government, and massive protests that impact only a fraction of the population. We have seen with COVID-19, for example, public health has a far more powerful effect on public sentiment and is more likely to create reactions of larger magnitude within the citizenry, which ripple out. These ripple effects



Dr. Jan Kallberg is Assistant Professor of American Politics in the Department of Social Sciences and Cyber Policy Fellow at the Army Cyber Institute at West Point. He holds a Ph.D. in Public Affairs and a Master's Degree in Political Science from the University of Texas at Dallas, and a J.D./LL.M. from Stockholm University. Prior to joining the West Point faculty, Jan was a researcher and Post-Doc at the Cyber Security Research and Education Institute, Erik Jonsson School of Engineering and Computer Science, at the University of Texas at Dallas under Dr. Bhavani Thuraisingham. Dr. Kallberg's research interest is the intersection between public leadership and cyber capabilities, especially offensive cyber operations as an alternative policy option. His personal website is www.cyberdefense.com.

have been hard to predict. The long-term psychological, societal, and health impacts of COVID-19 events have still not yet unfolded. As an example, according to the National Bureau of Economic Research, no other historic pandemic event has affected the stock market as profoundly as COVID-19.[1]

SOCIETAL PRIORITIES

COVID-19 has provided an essential data set for understanding what matters to the population. The environmental aspect of cyber defense, linked to public health, has not drawn attention as a national security matter. As living beings, we react to threats to our living space and the immediate environment. Jeopardizing the environment, intentionally or unintentionally, has historically led to the direct injection of fear and strong reactions in the population. Even unexpected accidents with environmental impact have triggered strong moves in public sentiment towards fear, panic, anger against the government, and challenges to public authority. One example is Chernobyl, which according to former Soviet leader Gorbachev was accredited as the reason for the Soviet collapse five years later as the popular lost faith in their government and their ability to protect their citizens.[2]

An adversary seeks effects that support its agenda and strategy. If an adversary engages in information operations, there is a goal and endgame that it is trying to achieve. From the adversary's perspective, what impact can it have on a US Presidential election, and does it matter whether a Democratic or Republican President is elected? What is the upside? The inference is concerning, and adequate resources are dedicated to addressing the problem.[3] However, if we look at the actual changes to policy outcome, the interference will likely not meet the intended goals of swaying the elections.

Dr. Rosemary Burk is a Senior Biologist with the Department of the Interior, U.S. Fish and Wildlife Service, Head Quarters, Falls Church, Virginia. She earned a Ph.D. in Biology from the University of North Texas with a specialization in aquatic ecology and environmental science. She has co-authored several articles that have linked failed cyber defense and environmental consequences including "Failed Cyberdefense: The Environmental Consequences of Hostile Acts," which was published by the U.S. Army's *Military Review* in 2014.

US defense spending and its grand impact on the world order have been nearly consistent over the decades. Even when presidents and political leaders have made drastic policy decisions, the actual change in the geopolitical landscape has been marginal. As a recent example, President Trump's movement of troops from Germany to Poland, Belgium, and Italy is simply a rearrangement and a new geopolitical position. From a Russian perspective, with an increasingly more military-able Poland and increasing commitment from several NATO countries, the US movement of troops out of Germany does not change the current situation. Until COVID-19, the return on the Russian information warfare investment was not present if the intended goal were to directly impact US policy and general sentiment. Groups and fragments of the population have been impacted, but the general population and large parts of the government and political machinery have been unaffected. We have seen that COVID-19 and information operations have fueled public health concerns and those fears are producing sentiment swings and foreign influence at a higher magnitude.

According to Kenneth Waltz, it is not what you do, but instead what you can do, that gives you the power.[4] A foreign adversary can gain more influence over popular sentiment through threatening to harm the immediate environment and public health, especially as these adversaries do not subscribe to the same ethics, code of conduct, and playbook as the US. COVID-19 has shown that cyber-attacks which create environmental and health threats, even those with a very low probability of occurring, can cause drastic swings in sentiment. Cyber-attacks that threaten public health and the citizens' immediate environment put the government's legitimacy, authority, and control under pressure, and trigger a significant decrease in citizen confidence in the current political leadership. The magnitude of such impacts can hardly be created by tweets and fake news, or rally

Dr. Bhavani Thuraisingham is the Founders Chair Professor of Computer Science and the Executive Director of the Cyber Security Research and Education Institute at The University of Texas at Dallas (UTD). She is also a visiting Senior Research Fellow at Kings College, University of London and an elected Fellow of the ACM, IEEE, the AAAS, and the NAI. Her research interests are on integrating cyber security and artificial intelligence. She has received several awards including the IEEE CS 1997 Technical Achievement Award, ACM SIGSAC 2010 Outstanding Contributions Award, and the IEEE ComSoc Communications and Information Security 2019 Technical Recognition Award. Her 40-year career includes industry (Honeywell), federal research laboratory (MITRE), US government (NSF) and US academia. Her work has resulted in 130+ journal articles, 300+ conference papers, 150+ keynote addresses, six U.S. patents, and fifteen books as well as technology transfer of the research to commercial products and operational systems.

extremists on social media because these events can be proven false and quickly forgotten by the public. Still, plausible threats to health and environment have a lasting impact.

Humans have survived thousands of years by learning and adapting to avoid threats to life and limb. Therefore, cyber-attacks that trigger fears of threats to public health and personal life have a massive initial impact and lasting effects which influence general perception and policy.

One such example is the Three Mile Island accident, which created significant public turbulence and fear and still profoundly impacted how we envision nuclear power. For a covert state actor that seeks to cripple society, embarrass the political leadership, and project to the world that we cannot defend ourselves, environmental damages are inviting.[5] An attack on the environment feels to the general public more close and scary than a dozen servers malfunctioning in a server park. It is tangible and quickly becomes personable and relatable, beyond what politically incendiary memes and social media storms can create.

We are all dependent on clean drinking water and non-toxic air. Cyber-attacks on these fundamentals for life could create panic and desperation in the general public–even if the reacting citizens were not directly affected.[6]

The last decade's study of cyber has left the environmental risk posed by cyber-controlled networks unaddressed.[7] The focus on cybersecurity has included providing for restoration of information systems by incorporating detection, protection, and reactive capabilities. From information security's early inception in the 1980s to today's secured environments, we have become skilled in our ability to secure and harden information systems. The interest in critical infrastructure is to a high degree concerned with accessibility, dependence, and availability, that the systems are working, and restoring

their working condition after an attack. However, the long-lasting impact of threats to human health or the immediate environment drives sentiment and affects policy more seriously than a temporary loss of service. Environmental effects such as contamination of drinking water, degradation of ecosystem's functionality, toxic agents released, and flooding with massive soil erosion arising would be dramatic and long-term. Environmental damages and threats to our immediate environment are tangible and highly visible, as problems like flooding, loss of drinkable water, pandemics, biological hazards, mudslides, toxic air, and chemical spills directly affect the population and its surrounding environment. A failed computer server park does not drive media attention, nor can a few hundred tweets create such an impact on the public sentiment as a hundred thousand dead fish floating down a river because of an environmental cyber-attack. The environmental impact is visible, connects with people on a visceral level, and generates a notion that human existence is in jeopardy. Humans put survival first.

Environmental damages trigger radical shifts in the public mind and general sentiment. For a minor state actor, such as an adversarial developing nation, these attacks can be conducted with a limited budget and resources while still creating significant political turbulence and loss of confidence by a targeted major state actor's population. Conflict and potential war, as mentioned, seek to change policy and influence another nation to take steps that it earlier was unwilling to take. The widespread anxiety and stress that can follow environmental damages is a political force worth recognizing, which COVID-19 has evidenced. Systematic cyber-attacks that threaten public health will likely generate influence with enough momentum to change national policy.

LOSS OF LEGITIMACY AND AUTHORITY

Successful covert cyber-attacks that lead to environmental impact are troublesome for the government–the specific damage to systems and the challenge to legitimacy, authority, and confidence in the government and political leadership. The citizens expect the state to protect them. The protection of the citizenry is one of the core elements in the concept of a democratic government. The security of citizens is a part of the unwritten social contract between citizens and their government. The federal government's ability to protect is taken for granted. If the government fails to protect and safeguard its citizens, its legitimacy is challenged. Legitimacy concerns not who can lead, but who can govern. A failure to protect is an inability to govern the nation, and legitimacy is eroded. Institutional stability can be affected, which destabilizes the nation. The political scientist Dwight Waldo believed that we need faith in government; for the government to have strong legitimacy, it has to project, deliver, and promise that life is better for its citizens. In a democracy, the voters need a sense that they are represented, the government works for their best interests, and the government will improve the quality of life for its citizens. In the *Administrative State*, Waldo defined his vision of the "good life" as the best possible life for the population that can be achieved based on time, technology, and resources. [8] Authority is the ability to implement policy.

Environmental hazards that lead to loss of life and a dramatic long-term decrease in quality of life for citizens trigger a demand for the government to act. If the population questions the government's ability to protect and safeguard it, the government's legitimacy and authority will suffer. In the Three Mile Island accident, the event impacted sentiment and risk perception, even decades after the incident, of how citizens perceived the government's nuclear policies and ability to ensure that nuclear power was safe.

President Carter needed to demonstrate the ability to handle the incident and restore the general public's confidence in government policies. Environmental risks tend to appeal to the general public's logic and emotions, especially uncertainty and fear, and a population that fears the future has instantly lost confidence in the government.

The difference between the Three Mile Island accident and cyber-attacks on infrastructure that create environmental damage is that, during the Three Mile Island accident millions of Americans had a real fear for their life and future when faced with the possibility of a nuclear meltdown. Cyber-attacks on our national infrastructure that threaten public health cannot be predicted or potentially contained. These attacks can be massive if they exploit a shared vulnerability. Consequently, the fear generated by Three Mile Island could, in retrospect, have been marginal in comparison to the fear caused by a large-scale cyber-attack on national infrastructure.

ENVIRONMENTAL CYBER DEFENSE

Defending US infrastructure from cyber-attacks is not only protecting information, network availability, and the global information grid. It is also safeguarding public health and the environment, which affect the citizens' lives, their health, and their immediate living environment. The COVID-19 epidemic demonstrated the magnitude of impact attacks on the immediate environment. The citizenry's quality of life directly affects the confidence the population has in the government's ability to govern. From a rogue and unethical adversary's perspective, this represents an "opportunity" that the US needs to address by increasing the environmental cyber defense and clarifying the intersection between public health and cyber.

DISCLAIMER

The views expressed herein are those of the authors and do not reflect the official policy or position of the Army Cyber Institute, the United States Military Academy, the Department of the Army, the Department of Defense, the U.S. Fish and Wildlife Service, or the Department of the Interior.

NOTES

1. Scott R. Baker, Nicholas Bloom, Steven J. Davis, Kyle J. Kost, Marco C. Sammon, and Tasaneeya Viratyosin, "The unprecedented stock market impact of COVID-19," No. w26945, *National Bureau of Economic Research*, 2020.
2. Abbie Llewelyn, "Chernobyl: How Gorbachev claimed disaster was real reason behind the Soviet Union's collapse," *The Express,* June 6, 2019, https://www.express.co.uk/news/world/1137086/chernobyl-hbo-series-sky-atlantic-nuclear-disaster-gorbachev-soviet-union-spt.
3. FBI, 2020, "Safeguarding Your Vote: A Joint Message on Election Security." *FBI*, last modified 8 October 2020, https://www.fbi.gov/video-repository/interagency-election-security-psa-100520.mp4/view.
4. Kenneth N. Waltz, "Nuclear Myths and Political Realities," *American Political Science Review*, (1990), 731-745.
5. Jan Kallberg and Rosemary A. Burk, "Failed Cyberdefense: The Environmental Consequences of Hostile Acts," *Military Review* 94, no. 3 (2014): 22.
6. Jan Kallberg and Rosemary A. Burk (2013), *Cyber Defense as Environmental Protection—The Broader Potential Impact of Failed Defensive Counter Cyber Operations in Conflict and Cooperation in Cyberspace-The Challenge to National Security in Cyberspace*, Edited by P.A. Yannakogeorgos and Adam Lowther, (New York: Taylor & Francis, 2013).
7. Idaho National Laboratory, 2005. US-CERT Control Systems Security Center, Cyber Incidents Involving Control Systems, INL/EXT-05-00671.
8. Dwight Waldo, *The Enterprise of Public Administration*, (Novato, CA: Chandler & Sharp, 1980).

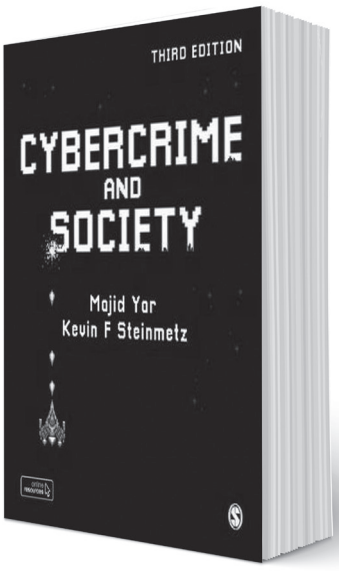
The Cyber Defense Review

BOOK REVIEW

Cybercrime and Society
Third Edition

by Majid Yar and
Kevin F. Steinmetz

Reviewed by
Stanley Mierzwa



EXECUTIVE SUMMARY

The following book review covers the overview, content, and insights of Majid Yar and Kevin F. Steinmetz's "Cybercrime and Society" Third Edition, published by SAGE publication in 2019. The structure of the book review includes a cursory background on the authors, the structure of the book content design, an overview of the chapter contents, and a book review conclusion. The book is being reviewed as part of a process to evaluate it for an upcoming undergraduate course in Foundations in Cybersecurity for Computer Science and Criminal Justice students working towards a minor or concentration in Cybersecurity. Provoking questions about our dependence on the Internet and approach to cyber threats.

REVIEW

Majid Yar is the original author of the first two editions of "Cybercrime and Society", and Chair of Criminology and Professor at the University of Lancaster in the United Kingdom. Yar focuses his research on cybercrime, criminological theory, crime control, policing, and culture. Kevin F. Steinmetz is an Associate Professor in the Department of Sociology, Anthropology, and Social Work at Kansas State University in the United States. His research focuses on technology crime, criminal justice, inequality, and popular culture.

"Cybercrime and Society" is now in its third edition, the first published in 2006, followed by the second edition in 2013, and now this latest in 2019. The book introduces a second author with this latest edition, which is a wise move to inject different perspectives,

Stanley Mierzwa is the Director, Center for Cybersecurity at Kean University. He lectures on Cybersecurity topics, including Cybersecurity Risk Management, Cyber Policy, and Foundations in Cybercrime. Previously, he worked at the State of New York, Metropolitan Transportation (MTA) Police as the Lead Application Security. Prior to the MTA, Stan was the Director of Information Technology at the Population Council. Stan has vast international technology implementation experience, having worked "on the ground" in over 15 countries, many in the developing world in Sub-Saharan Africa and Southeast Asia. He has over 12 published peer-review research articles and is a peer reviewer for the Online Journal of Public Health Informatics journal, a member of the FBI Infragard, IEEE, and ISC(2). Stan holds an M.S. in Management of Information Systems from the New Jersey Institute of Technology, a B.S. in Electrical Engineering Technology from Fairleigh Dickinson University, and is also a Certified Information Systems Security Professional (CISSP).

insights, and knowledge. The authors have also made available an accompanying website that offers online resources, such as web links, podcasts, and videos for instructors and students. The authors have divided the book into 12 chapters, which start with the content on history, perception, and defining cybercrime, before moving into criminological theory, which for the more technical, is a refreshing review of criminological aspects. The book takes the reader into light technical content on hacking, and then examines different shades of focus on hacking, scams and theft, illegal and offensive content, and the methods perpetrators work to avoid being caught. Cybercrime content would not be complete without a consideration of the less savory areas of abuse, victims of cyberstalking, and pornography. Finally, the book takes the reader through the work of law enforcement and then looks forward to the future of cybercrime.

As with any discipline to be covered in a book, starting with the origins of the vehicle, platform, or solution is important to explain the concept. The authors provide circumstantial knowledge into the ancestries of the current Internet. For those students who grew up with the World Wide Web always being available, an understanding of its beginning is essential. Many technology inventions surrounding security and protection can be attributed to the military, and the Internet is no exception, with the creation of the Semi-Autonomous Ground Environment (SAGE) system, ARPANET and DARPANET. Readers will be introduced to the varieties included in criminological theory. A deep dive into the background, history, and current perceptions of hackers and hacking is provided in Chapter 3. Hackers were previously viewed as explorers and they purported their efforts out of curiosity to benefit others in the community by freely sharing what was learned and discovered. The recent change in the definition of hackers is that cybercrime and hacking have become identical.

The authors raise interesting content related to cinema and how movies related to hacking and computers taking over our environments can have an influence on the public's perceptions of computer hacking. The authors provided a theoretical look at what hackers do to commit computer crime; this included the fundamental view of unauthorized access to computer systems, theft of resources, damaging or making systems inaccessible, and distributing malware. Finally, academic background on the why and who is involved in computer crime is discussed, an appreciated move in charting out time to trace the path for criminal computer activity. Still, for technologists or those studying cybersecurity from the technical perspective, the discussion of crime theory is not often raised in technology tracks.

Consideration of the political angles or benefits that can be gained from hacking and cybercrime are discussed in Chapter 4. This allows the reader to make connections. Hacking was initially viewed as a positive activity for technologists to learn and share computing skills, but then the movement led to criminal activity. Then the reader sees the progression to political hacking, or hacktivism, and cyberterrorism. Hacktivism can take on many shapes, including virtual sit-ins and denials of service, overloading email systems, website defacements, inflicting viruses and worms, and using or developing systems to allow censored users to operate and communicate. The use of Internet tools has many political advantages by enabling the coordination of participants dispersed throughout the globe. A review of why cyberterrorism flourishes with the use of the Internet is debated, including such points as the way in which the internet, by its very nature, promotes activity from far away, requires limited financial and infrastructure resources, allows for anonymity and the use of compromised systems to forge attacks, and lacks regulation since the Internet is so decentralized. The reader is then presented with a variety of scams and frauds, including the diversity of phishing and social engineering, which criminals use to great effect.

The authors noted that because of the high volume of computer crime, the police only investigate the most serious or large-scale offenses. The majority of computer crimes go unreported and only adds to the difficulties of estimating its extent. In addition to the estimated large and increasing numbers of computer-related crimes, the issue is complicated by a lack of police resources available as well as a lack of expertise in the time-consuming task of forensic work. Larger law enforcement agencies have specialized cybercrime units in place to focus on policing crimes, but this does not help most agencies that exist in smaller municipal or county units. The authors explain that the Internet, by its very design, inherently favors a self-regulated model for management and security. With this, the concept of web content activists is brought forward, and examples of how organizations, such as the Anti-Discrimination Committee and Simon Wiesenthal Center, actively monitor the Internet for hate-related crimes and expose them to mount legal actions. This raises the idea of self-policing to complement formal law enforcement organizations, such as the anti-virus or anti-malware security software in which most computer users are familiar. There is a perspective that categorizes such

products as privatized, 'for-profit' cybercrime policing. Because no single body or agency can truly police the Internet or our technology infrastructure, it is necessary that we conduct our own security provisioning or shift the responsibility of cybercrime control to non-state agencies. It is no surprise that the 'for-profit' industry of information security includes spending in the range of hundreds of billions of US dollars, with an ever-increasing and expanding array of services becoming available yearly.

CONCLUSION

Readers will obtain an international perspective of cybersecurity and cybercrime as the primary author is based in the United Kingdom. This is beneficial for readers with more global interests, and because of the ease at which cybercrime can be committed far from its actual location. Additionally, throughout the book, data and figures are provided to support an argument specific to the US, with a similar comparison for examples in the United Kingdom. One example is compares estimates of cyberstalking in the US with that in the UK.

Neither author is a computer science or pure technology engineering cybersecurity guru. However, this works to the advantage for those studying at an introductory level or wishing to learn about cybercrime from a broad viewpoint that relates to crime, analysis, investigations, legal aspects, and law enforcement.

The book provides many examples to show how non-cyber and cybercrimes are similar but with cybercrimes, including extended qualities due to the introduction of distance and the Internet. For example, while stalking and cyberstalking, on the surface, can appear quite the same, Yar and Steinmetz introduce many details to help the reader understand the subtleties between each. The challenges of safeguarding personal and organizational data from cybercrime actors will continue to expand as the endpoints of the Internet expand, as is seen with the advent of bio-devices on the human body, cloud computing, the Internet of Things, and growing efforts in state-sponsored hacking.

Yar and Steinmetz provide an excellent cybersecurity resource that can be utilized in introductory coursework at the undergraduate and graduate levels. Any of the chapters could be expanded upon to become a book on its own, and the value provided is that the reader or student will get a treasured primer and summary.

Title: ***Cybercrime and Society***
Paperback edition – Third Edition 2019

Authors: Majid Yar; Kevin F. Steinmetz

Publisher: SAGE Publications, Ltd., 2019

Paperback: 350 pages

Language: English

Price: $30.49 paperback

ISBN: 978-1-5264-4064-8

ISBN: 978-1-5264-4065-5

THE CYBER DEFENSE REVIEW

CONTINUE THE CONVERSATION ONLINE

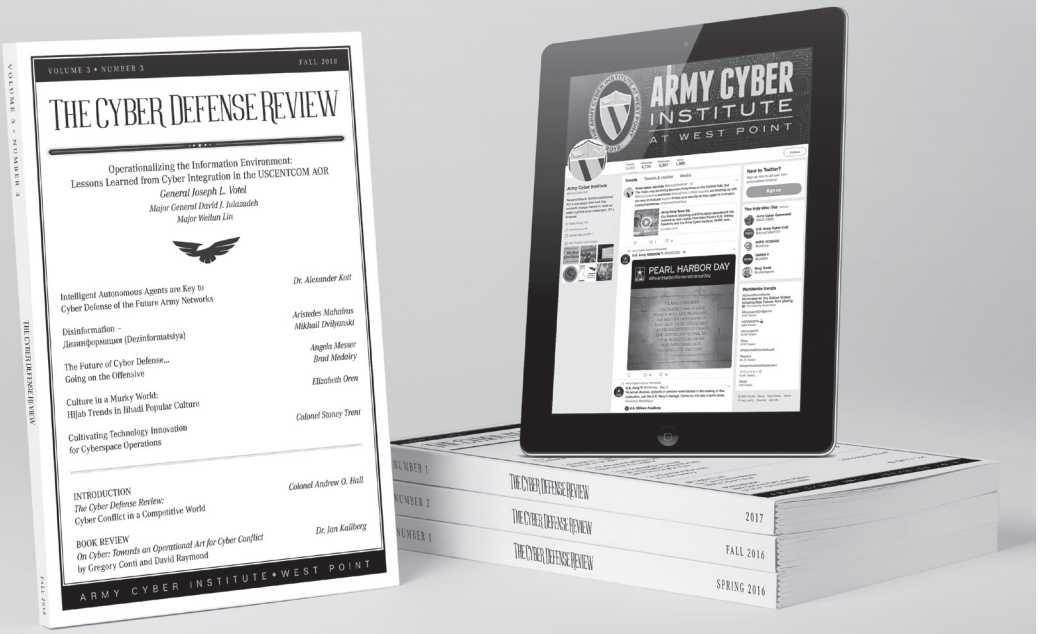
CyberDefenseReview.Army.mil

AND THROUGH SOCIAL MEDIA

Facebook @ArmyCyberInstitute

LinkedIn @LinkedInGroup

Twitter @ArmyCyberInst
@CyberDefReview



ARMY CYBER INSTITUTE • WEST POINT

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