VOLUME 8 ◆ NUMBER 1 SPRING 2023

THE CYBER DEFENSE REVIEW

ARMY CYBER INSTITUTE ◆ WEST POINT PRESS

The Cyber Defense Review

Spring Edition

THE CYBER DEFENSE REVIEW

A DYNAMIC MULTIDISCIPLINARY DIALOGUE

CONTACT
West Point Press
Taylor Hall, Building 600
West Point, NY 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 West Point Press. The views expressed in the journal are those of the authors and not the United States Military Academy, the Department of the Army, or any other agency of the U.S. Government. The mention of companies and/or products is for demonstrative purposes only and does not constitute endorsement by United States Military Academy, the Department of the Army, or any other agency of the U.S. Government.

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

BOOK REVIEW

The Cyber Defense Review

Introduction

VOL. 8 ◆ NO. 1

Leadership in the Digital World

Dr. Corvin J. Connolly

Welcome to the Spring CDR. We proudly announce that the CDR has a new home with the West Point Press. This reorganization aligns with the vision of the 15th Dean of the Academic Board, BG Shane Reeves, for West Point to be "the intellectual engine of the Army." At the unveiling of the West Point Press in January 2023, BG Reeves asserted, "Our faculty and cadets are conducting research that impacts some of the Nation's toughest problems and most pressing issues ... producing scholarship [with] major impacts across academia, the Army, and the world." The CDR will continue its special relationship with the Army Cyber Institute (ACI) at West Point.

The Press serves as the publishing arm of West Point's "intellectual engine" and a member of the Association of University Presses. It embodies and advances the Academy's mission and core values by publishing digital textbooks, white papers, articles, reports, podcasts, and platinum open-access, peer-reviewed monographs and journals. The Press is a vehicle for West Point faculty and staff to publish their research, and will also publish work from outside scholars regardless of institutional affiliation.

Dr. Corvin J. Connolly is Editor-in-Chief of *The Cyber Defense Review* (CDR) at the United States Military Academy (USMA) at West Point, New York. In this capacity, Dr. Connolly publishes the flagship cyber journal for the U.S. Army and Department of Defense. Under his tutelage, the CDR was selected by JSTOR and for "Security Studies Collection." Before his current assignment, he was a consultant and senior manager with Lockheed Martin Corporate Strategy and Business Development. Dr. Connolly is a retired U.S. Air Force officer with leadership assignments in executive communications, legislative affairs, NATO command & control, and missile operations. He has a B.A. in History from Assumption College, an M.S. in International Relations from Troy University, and a Ph.D. in History from Texas A&M University.

What has not changed is that the CDR will continue its robust coverage of the cyber domain and embody a commitment to the highest standards of scholarship. Our elite CDR team remains in place with Managing Editor Dr. Jan Kallberg, magnificent Assistant Editors from the West Point Class of '70, Hon. Joe Reeder, Chip Leonard, Dr. Bill Spracher, and Dr. Bill Lane, and Assistant Editors Charles Leonard and Courtney Gordon Tennant, Esq. The CDR continues with a phenomenal group of 21 Area Editors who review CDR submissions through the ScholarOne workflow processing platform. The members of the CDR Editorial Board, led by its Chair and former ACI Director, Dr. Andy Hall, are tremendous ambassadors for the journal.

The CDR has a tradition of showcasing leadership in the digital world. Throughout our tenure, we have been honored to feature the Hon. Joe Reeder, GEN Paul Nakasone, GEN (Ret.) Keith Alexander, ADM (Ret.) Dennis Blair, GEN (Ret.) David Petraeus, GEN (Ret.) Joseph Votel, LTG (Ret.) Stephen Fogarty, VADM (Ret.) Nancy Norton, VADM (Ret.) TJ White, Dr. Chris Demchak, Dr. Martin Libicki, Prof. Michael Schmitt, and Rob Schrier, to name just a few of the distinguished CDR contributors. Over the last seven years, these leaders have provided CDR readers and the cyber community with unparalleled insight into the digital world. As such, the CDR continues this proud tradition in its Spring 2023 edition with a profound leadership essay from cyber legend Dan Geer and Glenn Gaffney, the former Director of Science and Technology for the CIA. In "Establishing the Conditions of Engagement with Machines," the authors tackle the current perspectives, operational reality, and government responsibility regarding autonomous AI systems.

This Spring edition features two distinguished professional commentaries. First, Paul Schuh of U.S. Cyber Command expertly explains important military terminology in "Expeditionary Cyberspace Operations." In the second commentary, LTC Mark Visger

and Prof. Zhanna Malekos Smith provide a meaningful counterpoint argument to Dr. Nori Katagari's Summer CDR article. In "Countermeasures as Lightning, not a Lighting Bug: Illuminating the Legal Doctrine," the authors explore international law as applied to cyber operations and explain the notion of cyber countermeasures.

Research articles have always been the CDR's bread and butter, and we are pleased to feature five exceptional articles that expand upon the CDR's multidisciplinary construct. We showcase LTC Nate Bastian's blockbuster article, "Gaining Competitive Advantages in Cyberspace." LTC Bastian examines the military integration of autonomy, AI, and machine learning. Sarah Chen, Rhodes Scholar and recent graduate of Claremont McKenna College, and Dr. Jennifer Taw of Claremont McKenna College deliver a superbly crafted article for the cyber community. In "Conventional Retaliation and Cyber Attacks," Chen and Taw tackle nation-state response to attacks through the prism of retaliation, escalation, and attribution. CDR readers will benefit from the authors comprehensive literature review. In "Machine Learning Applications for Cybersecurity," Dr. M.A. Thomas provides a detailed study of machine learning and its transformation of the cybersecurity environment. In "What Types of Tactical Vulnerabilities do Future Officers Most Anticipate?" Dr. Aryn Pyke, Dr. James Ness, and MAJ Dave Feltner provide a dynamic data-driven study of vulnerabilities in the cyber domain. In MAJ Travis Siemion's article, "Rethinking US Concepts and Actions in Cyberspace: Building a Better Foundation for Deterring China's Aggression," the author clearly outlines China's cyber threat and provides suggestions to improve US national security.

We continue the CDR's tradition of publishing book reviews by a variety of contributors, including West Point cadets. In this edition, Cadet Dylan Green reviews *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats* by Richard Clarke and Robert Knake. Cadet Green delivers a comprehensive assessment and provides added insight into the importance of resilience in the cyber battlespace.

We would like to recognize Sergio Analco and Gina Daschbach for their flawless layout and design of the Spring CDR. Their creativity and energy continually elevate the CDR. In the same vein, we also appreciate the remarkable dedication of Hon. Joe Reeder, Chip Leonard, Dr. Bill Spracher, Dr. Bill Lane, Charles Leonard, Courtney Gordon-Tennant, and LTC Mark Visger. Their dynamic editing and thoughtful leadership have enhanced the content and transformed the CDR.

In closing, the CDR staff would like to thank the Army Cyber Institute (ACI) for its incredible support. Over the last seven-and-a-half years, the ACI's Erik Dean, Clare Blackmon, Don Carmel, Dr. Ed Sobiesk, Prof. Rob Barnsby, LTC Bob Ross, Dr. Paul Maxwell, Lance Latimer, and Nataliya Brantly have fostered a collaborative environment, which made creating the CDR immensely gratifying. The CDR is honored to be sponsored by the ACI and their world-class team of cyber researchers. As always, we are excited to continue the cyber conversation together!

The Cyber Defense Review

Senior Leader Perspective

Establishing the Conditions of Engagement with Machines

Dan Geer
Glenn Gaffney

Realism is dealing with the machines, people, organizations, and governance systems we have, not those we wish for.

We begin our discussion of "autonomy" with its Western meaning for the human individual: "to be autonomous is to govern oneself, to be directed by considerations, desires, conditions, and characteristics that are not simply imposed externally upon one." Autonomy is "the capacity to impose upon ourselves, by virtue of our practical identities, obligations to act."[1] Similarly, extending autonomy to machines is a partial release from external control that comes with obligations to act. That's the easy part.

Until the last decade, machines with no human in the loop had very limited repertoires of actions they could take, turning on the pump when they detected the water was rising. From that set of inherent constraints came reliability and understandability. As is obvious, we are transiting an inflection point where machines are gaining trained reasoning capacity that can allow problem-solving without a human in the loop. Even the training can be self-administered: the autonomy of self-modification (and, with it, emergent behavior — a topic to which we return below).

This leads to the set of interactions touched upon in this essay: Western principles of control, various tradeoffs, drivers of adoption, responsibilities, predictability, and recovery from faults — a list that is neither ordered nor exhaustive of the work remaining to be done. We are well past arguing over whether autonomy is coming, or that it is a national security issue.[2] However, while the transiting of the inflection point is clear and many of

Dan Geer, Senior Fellow, In-Q-Tel. Milestones: The X Window System and Kerberos (1988), the first information security consulting firm on Wall Street (1992), convenor of the first academic conference on mobile computing (1993), convenor of the first academic conference on electronic commerce (1995), the "Risk Management is Where the Money Is" speech that changed the focus of security (1998), the Presidency of USENIX Association (2000), the first call for the eclipse of authentication by accountability (2002), principal author of "Cyberinsecurity: The Cost of Monopoly" (2003), co-founder of SecurityMetrics.Org (2004), convener of MetriCon (2006-present), author of "Economics & Strategies of Data Security" (2008), and author of "Cybersecurity & National Policy" (2010). Creator of the Index of Cyber Security (2011) and the Cyber Security Decision Market (2012). Lifetime Achievement Award, USENIX Association, (2011). Expert for NSA Science of Security award (2013-present). Cybersecurity Hall of Fame (2016) and ISSA Hall of Fame (2019). Testified five times before Congress.

the national security concerns recognized, less obvious is whether we as a nation have a preferred destination point/performance design in mind. We appear instead to have grown comfortable letting market forces drive development and consumer outcomes, and only then to intervene around any undesirable outcomes and effects as they arise. This approach is unsound given China's fierce competition in pursuit of the foundational technology of the next-generation economic infrastructure and whose principles will dominate next generation infrastructure, and otherwise be embedded in technologies that will mediate our day-to-day life.

SPEED AND COMPLEXITY DRIVE THE DISTRIBUTION OF ROLES AND CONTROLS

This may be easy to say and accept on first reading but analyzing the implications is more complicated. We (humans) have long since proven that we can build systems that we cannot then understand enough to control. This should not surprise; complexity ensures emergent behavior. It has been 25 years since Dyson wrote, "Emergent behavior is that which cannot be predicted through analysis at any level simpler than that of the system as a whole. Emergent behavior, by definition, is what's left after everything else has been explained."[3] Therefore, when we cannot explain the cause-and-effect relationship of some autonomous system's choices that crashed some platform, we revert to comparing the overall safety of the system as a whole and "accept" the attendant risks. The contribution of algorithmic trading to flash crashes at the NYSE might be a recognizable example.[4] In striving for machines to learn not only during preparation for going live but also to learn as a result of having gone live, we are actively seeking emergent behavior yet not preparing for the potential consequences of that emergent behavior.

Consequently, we ask: should hands-off mathematical operations — autonomous algorithms — be treated as if they are correct-by-definition or incorrect-by-definition?

Glenn Gaffney is the Chief Strategy Officer for the NobleReach Foundation. The NobleReach Foundation is a nonprofit organization on a mission to inspire tech talent to tackle our nation's most pressing challenges. Before joining NobleReach, Mr. Gaffney served as a senior fellow at IQT, supporting the identification of and strategic investment in ready soon technology that can uniquely meet economic and national security needs. Before joining IQT in 2017, he enjoyed a 30+ year career in science, technology, analysis, and operations within the U.S. Intelligence Community. Mr. Gaffney's government service included senior positions as the Director of Science and Technology for the Central Intelligence Agency, the Deputy Director of National Intelligence for Collection, and the Associate Director of CIA for Talent.

Do we default to trust or mistrust? Given the myriad parameters, ML algorithms likely will never be 100% susceptible to coherent explanation[5] (see Fig. 1); hence the venerable strategy of trust-but-verify seems permanently unattainable. That leaves only slow, measured delegation of authority to the AI under the banner of hope or fighting fire with fire under the banner of the precautionary principle,[6] i.e., using one AI to watch another[7] in an attempt to constrain the emergent behavior of the base AI system, and the hope that collusion does not follow.[8] Exhaustively testing an autonomous system is impossible; reserving part of the training data for post-training validation runs is about all there is. Why? Because the possible outcome space is too large to explore — the only place to test is in production, which brings us back to the question of whether we treat the AI by default as correct or incorrect. Yes, the reality is more complex than that. In much of cybersecurity design, the emphasis is now on "zero trust;" every interaction between components must be challenged to prove it is wanted. What that means for autonomy is unclear; some argue that imposing upon ourselves an obligation to act includes the Golden Rule, which should also apply to autonomous systems.[9] Others say that trust is "confident anticipation backed by effective recourse,"[10] the antithesis of saying that every thinking entity is my friend.[11] What is the recourse when an autonomous system produces an unwanted result? Does that not imply a base requirement that all actions by autonomous systems must be inherently attributable in terms of cause and effect? Our desire for attribution is such that, even though the size of emergent behavior space is too large to predict, we will still define any system by the extrema that emerge from it and look to hold someone or something accountable for the "failure" — System X crashed the plane, or shut down the power grid, or launched a cyber-attack against an ally because some third party was using the ally's infrastructure to attack the US.

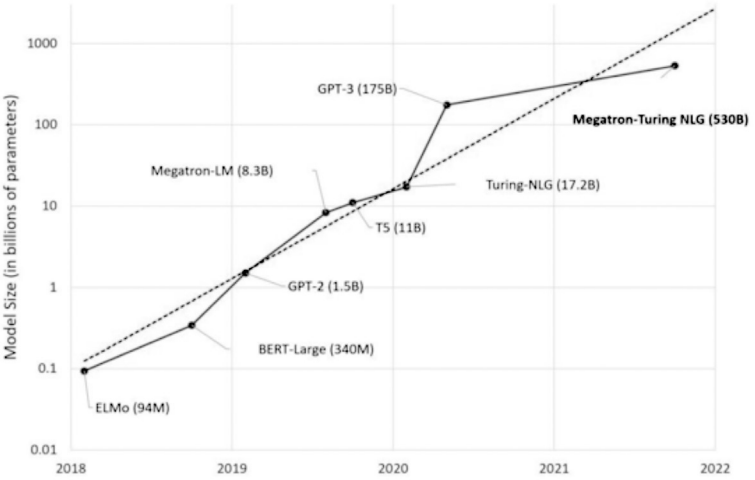


Figure 1: Growth of parameter count in Natural Language Generation (NLG) models

Speed enters all of this. First is the increasing speed of machine operations themselves. Second is the speed at which key decisions are delegated to specific machine AIs, and driven by power competition, both commercial and military. Third is the speed of proliferation of machine AI into new areas of application, and this is where the natural pace of rulemaking is the most insufficient.

Extrema are not boundable

A massive potential outcome space, which describes all non-toy machine learning (ML) systems, renders it impossible to bound what an extreme value is or might be. The more complexity in any system, the broader the range of that system's possible outcomes. This makes the probability distribution of possible outcomes have "fat tails," meaning that across the distribution of possible events, the statistical properties of the entire distribution as a whole come to be dominated by the impact of rare events. As an example, when there are one million buckets with no money in them and one bucket with $100,000,000, the expected gain you get from sticking your hand in a random bucket is $100 — an amount which you cannot actually win and, in any case, is entirely a function of that one solitary outlier value. More critically to our discussion here, for fat tails, the difference between extrema already observed and future extrema are much larger than for distributions with thin tails; the worst flood you have ever seen does not tell what is the worst flood that can happen.

Avoiding the uncharted seamount

Given the above, the mythical prudent man or government would plan for maximum damage scenarios, not for maximum likelihood scenarios. Does this mean that the introduction of autonomy must be incremental? No, insofar as the only way to test is in production and past results are no guarantee of future performance. Does this mean watchdog processes are needed

(even if they, too, are massive, non-interrogable ML)? Yes, with design-space wiggle room here for whether the watchdog's autonomy includes overriding authority for the AI under watch. For the sake of resilience if no other, does this mean retaining whatever mechanism pre-dated the autonomous system now being put into operation? A strong yes if the prior mechanism can be guaranteed to remain in working order while it stands by, else no, expecting some prior mechanism to come to the rescue from unattended cold standby is a false security promise.

Mitigating downsides

As with any other substantive risk management, the key challenge is mitigating downsides. Speed, cost, efficacy, latency, side effects, and more — all figure in. Speaking broadly, planning for the loss of a meaningful asset implies planning for the availability of compensating reserve, the role insurance plays in normal affairs up to and including those where the government is the insurer of last resort. Retaining working alternatives is, in this sense, a kind of insurance. So is deployed diversity — Nature knows better than to fabricate monocultures that fail in lockstep while market forces arguably do not. While it has been repeatedly but ineffectually discussed in the setting of one technical aspect of societal digitization, namely cybersecurity, deploying thoroughgoing autonomy into societally critical roles might suggest the issuance of catastrophe bonds[12] to cover the tail risk of dependence on that autonomy. Lessons learned from managing the tail risk of the nuclear power industry under the Price-Anderson Act[13] should also inform an adroit tail risk strategy for critical autonomous processes.

Accommodation to democracy

While all politics may be local, all technology is global; hence technology policy instantiation inside an autonomous system must somehow accommodate local values. Autonomous technology suppliers sometimes assume a quasi-governmental role. Government vs. autonomy debates previously were often confined to centralized vs. decentralized administrative organization, antitrust regulation vs. "natural monopolies," or the reach of public health measures. No more. The largest tech firms now dwarf small countries[14] in economic size, number of clients,[15] and the amount of personal information stored about those clients. Rule of law observes jurisdictional boundaries, but that limitation more often than not fails to cover technology. As companies and governments deploy more autonomy, the capability set of autonomous systems must include awareness of jurisdictions in the equation. Achieving this in practical terms prompts us to quote Lessig:[16]

> Every age has its potential regulator, its threat to liberty. Our founders feared a newly empowered federal government; the Constitution is written against that fear. John Stuart Mill worried about the regulation by social norms in nineteenth-century England; his book On Liberty is written against that regulation. Many of the progressives in the twentieth century worried about the injustices of the market. The reforms of the market, and the safety nets that surround it, were erected in response.

> Ours is the age of cyberspace. It, too, has a regulator. This regulator, too, threatens liberty. But so obsessed are we with the idea that liberty means 'freedom from government' that we don't even see the regulation in this new space. We therefore don't see the threat to liberty that this regulation presents.

The regulator is code — the software and hardware that make cyberspace what it is. This code, or architecture, sets the terms on which life in cyberspace is experienced, and governs both privacy protections and censored speech. It determines whether information access is general and/or zoned. It affects who sees what or what is monitored. In a host of ways that one cannot begin to see unless one begins to understand the nature of this code, the code of cyberspace regulates.

Subjugating autonomy to democracy is no small challenge. Democracies are inefficient by design, and we need machines to do what they do best. How best can democracy thrive in an automated world? By what principles will we govern "by the people" in tandem with free-running, self-modifying algorithms? We desire clarity in understanding why control decisions are made – particularly when we do not like the outcomes of those decisions. Unless we know we have some visibility or understanding, if not transparency,[17] providing checks and balances[18] sufficient to the task is not possible. US policymakers did not foresee that surveillance would become commercially monetized[19] or that low-end job descriptions might inherently include functioning as an informant.[20] Similarly, no one should expect autonomy to play nice magically. We need to establish a way to safely exercise and test emergent behavior with some degree of public engagement and transparency. Aspects of applied techno-sociological research across critical public service systems and infrastructures must have the principal goal of establishing the design space for watchdog AI systems. All of that is before we use the word "China."

Data as a driver for autonomy

The explosive growth in data volume has led some to suggest that DNA storage alone can accommodate the volume.[21] Even so, much data will remain at its point of collection; there is not enough bandwidth to move it all elsewhere. Lt. Col. Rhett Hierlmeier, who headed up the training center for the F-35, in an interview observed: "Standing outside the cockpit, he peers into the darkened dome and says he believes we will one day fight our enemies from inside one of these things. When I ask what that will take, he says flatly, 'Bandwidth,' which is why 'engineers are focused on things like improving artificial intelligence so planes can act with more autonomy, thus cutting down on communication bandwidth [requirements].'"[22] In this and other examples, we see that data richness is the foremost driver for algorithm autonomy.

If data volume forces distal compute nodes to require autonomy, what does that imply for cybersecurity? Authorities some years back concluded that "[t]he best approach to cybersecurity will emphasize defenses that are robust to unforeseen perturbations, evolvable in response to changing conditions, and self-repairing in the face of damage."[23] This was an early call for a

second watchdog breed-type of autonomy. (Everyone, including those concerned about data interception in transit, will agree that data untransmitted is data unintercepted, which provides yet another driver toward autonomy.)

Operational reality and government responsibility

Unless an algorithm is misapplied, autonomous AI systems will usually perform better than a human at the same task. At the same time, we know that optimality and efficiency work counter to robustness and resilience.[24] We know that complexity tends to conceal interdependence, and unacknowledged interdependence is the source of black swan events. We know that the benefits of digitalization are not transitive (they do not spread to all concerned) but the risks are (and do). We know that because single points of failure require militarization wherever they underlie gross societal dependencies, frank minimization of the number of such single points of failure is a national security obligation. We know that cascade failure ignited by random faults is quenched by redundancy whereas cascade failure ignited by sentient opponents is exacerbated by redundancy. Hence, we know that preservation of uncorrelated operational mechanisms is likewise a national security obligation.[25] Once again, leaving everything up to globalized market forces will almost certainly result in serious downside outcomes for many without clarifying what constitutes acceptable costs.

An early adopter: Autonomy for cybersecurity

The need for speed in each step of the cybersecurity OODA[26] loop is growing more urgent, and that which we must protect is growing more valuable and more complex. Whether or not caused by a litany of accumulated design and implementation failures, it remains true that humans simply cannot keep up with the growing demand. Nor are they good at accepting the consequences of weakness. Cybersecurity tools must include autonomous actors. Most of us have a natural default tendency to seek (and expect) a technical solution to self-imposed problems, but we now have little choice but to center strategy on employing algorithms to do what we cannot ourselves do, which is to protect us from other algorithms. This may be inevitable, if in cybersecurity offense actually enjoys a structural advantage over defense, it might mean that wars of attrition spring up within each new theater of offense, each new dependence made critical simply by the aggregate mass adoption of the underlying technology.

To be clear, while our systems can benefit from greater autonomy in cyber security, we simultaneously must pre-determine the reasonable limits of that autonomy. All models have a tipping point, and such tipping points (vulnerabilities) need watchdog protection from sophisticated adversaries capable of exploiting those tipping points. Adversaries greatly value the ability to undermine our trust in our own data, and to redirect our autonomous agents and thereby inflict friendly fire. A paramount research grade problem here would be a solution for carefully breeding the watchdogs.

The evolution in thinking, negotiating, and training with machines

In the age of autonomy what is worse: getting the right answer for the wrong reasons, or getting the wrong answer for the right reasons? Are we troubled by the implicit de-skilling that comes with substituting autonomous algorithms for practiced, intuitive human judgment, however inferior the latter is? Langewiesche's analysis of the June 2009 crash of Air France Flight 447[27] comes to this conclusion: "We are locked into a spiral in which poor human performance begets automation, which worsens human performance, which begets increasing automation," and further, that "the effect of automation is to reduce the cockpit workload when the workload is low and to increase it when the workload is high." Put differently, as we increasingly become dependent on autonomous systems, we need to anticipate and recognize the point at which an autonomous AI becomes an irreversible necessity.

Once we cross that no-going-back point, we aren't so much flying the plane with AI as we are negotiating with an AI agent in order to fly a plane (or complete another complex task). We are already in the era of negotiation with AI rather than harnessing it as a tool we command and control, but we have yet to fully acknowledge this. In other words, it is undoubtedly essential to train humans and machines as a team. Professional certifications and regulations must ramp up to this reality. This has already begun within limited areas by firms with the resource base and drive to do so, but it is entirely locally driven. And, as is true for other high technology breakthroughs, government regulation is woefully trailing, and desperately needed.

It is possible that, during the training of the man-machine composite, the human expert can help the machine learn and become more effective in complementing human behavior. Humans and machines partnering together have already proven to be superior to machines alone in some strategy games.[28,29] In other areas, human experts have undergone retraining to learn how to better interface with the AI agent to ensure both remain on the same page for operating safely.[30] In such examples, the burden of understanding and adapting to the communication style remains with the human; the ability to reason is the distinguishing human characteristic, though for how long remains a debated question. Given the consequences of getting it wrong, the US should seriously consider the need for a "Reverse Turing Test" whereby nothing can be classified or accepted that does not either recognize that it is interfacing or working with a human and act accordingly, or at a minimum be proven to be totally subservient to the human in the loop. Indeed, this article proposes the following as a general rule that governs use of machine learning: A machine must recognize when it is interacting with a human, and we must have already chosen if and when "I'm sorry, Dave, I'm afraid I can't do that"[31] might actually be proper.

A role for government and our allies

There has been an appropriately increased focus this past year on technology innovation as part of our great power competition with China. While AI is called out as a key tech sector for competition, per se, we must recognize that AI's application within other critical tech sectors,

like biotech, and in critical infrastructure systems and public services will be equally important for our overall competitiveness. The US government (USG), as part of its emphasis on innovation and economic competitiveness, must pursue an understanding of what democratic principles of digital design mean in practice. Digital proving grounds will be needed. Such proving grounds must be able to leverage national labs and other federally funded infrastructure. Integrated research teams must include public and private sector experts alike. Participation must be either compelled or heavily incentivized. There must be no confusion that this effort is a look-ahead to understand and then forestall the distribution of autonomous systems that are inadvertently anti-democratic and/or uncontrollable once deployed. Call it accountability, if you prefer, but think of it as the governance of checks and balances. Any system of trust requires a trust anchor; this effort is to construct one. So long as the autonomous decision-making is not susceptible to coherent explanation, autonomy's implicit authoritarianism[32] means operational countermeasures must be vetted at those proving grounds. Hard questions await, e.g., when may an autonomous system reproduce?

If a probative model can be established, then the USG should look to export the model to like-minded democratic allies around the world. Sharing such proving ground spaces internationally would send clear signals that alternatives to "Made in China" infrastructure and "Controlled in China" data stores are within reach. The policies around autonomy can make clear the distinctions between autocracies and democracies like few other areas of comparison. The US cannot meet the demands of the great power competition before us on our own within the short 9-10-year time frame we face. This is a time to do things *with* our allies, not *to* them.

To be adopted, allies must view the offer we make to them to be real in terms of their economic glide path. We believe the only sure way to demonstrate our commitment is to do here at home what we urge them to do ("do as we do"). If we can gain significant tech translation activity across a few critical economic areas and across several regional partners within the next 3-5 years, we believe that will prove disruptive to China and its 2030 timeline to overtake the US.

Summary of Recommendations — What the US government should establish next.

1. A national priority for dedicated, interdisciplinary, techno-sociological research on autonomous systems, including a requirement for AI-on-AI "watchdog" design and development. This research must cover autonomous system safety and fitness for use as to both industrial accidents and hostile actors. Prudence requires that all autonomous systems be considered dual use by default.

2. A national priority risk management strategy for critical autonomous processes. To motivate the best efforts of the private sector, strict liability for autonomous systems must be put in place and be explicit. Mandatory reporting thresholds for untoward and unanticipated incidents must likewise be explicit, including unarguable clarity for which agencies have the duty to receive and act upon such reports.

3. Regulations and certifications for what is acceptable practice to train humans and machines as a team. This has begun in some industries but needs to be required for critical systems drawing direction from the training of professionals who interact with complex environments, such as lawyers, licensed structural engineers, passenger aircraft pilots, certified public accountants, etc.

4. A national autonomy design criterion that, at a minimum, insists that autonomous systems recognize a human in the loop and that human's authority for interaction. Abiding by such a criterion would grant to the maker of the autonomous system those kinds of legal immunity that are proportionate to the rigor of the criteria followed. A starting point might be airworthiness certificates issued by the Federal Aviation Administration (and some other countries such as Australia).

5. Proving grounds in partnership with industry, which focus on the application of, and experience with, autonomy across tech sectors deemed critical in ongoing competition with China, critical infrastructure, and public service systems. These proving grounds can be topic-specific, and because these partnerships may include both regulator and the regulated, convenors and operators of such partnerships of such proving grounds should, as precedent has shown, be private third parties.[33] These proving grounds:

   a) Can be established across several regions of the country to engage the broadest range of Americans through inclusion, transparency, and communication in relevant work, and

   b) Should be designed and operated to provide common experience in testing and developing new risk strategies and systems using modeling and testing to explore options and develop consensus around solutions. Partnerships among the autonomy industry, government, and insurance industry should lead to new incentive models and policies for buying down the risk in key areas for rapid development, testing, and fielding.

   c) Should include experiments designed to proactively provide baselines for new regulations and certifications in team training of humans and machines.

   d) Should be enabled for next-generation data operations, establishing the necessary practices for the rapid advancement of research and tech translation into application and commercialization while providing protection from economic espionage and theft and securing the privacy of our citizens. This next-generation infrastructure will support the new economy and is as vitally important as the science, technology, and commercial enterprise it seeks to enable.

The closing question: Is autonomy a zero-sum game?

NOTES

1. "Autonomy in Moral and Political Philosophy," *Stanford Encyclopedia of Philosophy,* 2020, plato.stanford.edu/entries/autonomy-moral.
2. Defense Science Board, "Seven Defense Priorities for the New Administration," point 5, "Anticipating intelligent systems and autonomy," December 2016, dsb.cto.mil/reports/2010s/Seven_Defense_Priorities.pdf.
3. George Dyson, *Darwin Among the Machines,* Addison-Wesley, 1997.
4. Peter Bloom, "In finance the war is over, the machines won, the number of real players is under ten, and humans will never again be in the OODA loop," CNAS Catastrophic Risks Workshop, January 12, 2018.
5. As of October 11, 2021, the biggest is the Microsoft-Nvidia "Megatron-Turing Natural Language Generation" model at 530 billion parameters (www.microsoft.com/en-us/research/blog/using-deepspeed-and-megatron-to-train-megatron-turing-nlg-530b-the-worlds-largest-and-most-powerful-generative-language-model); the prior record holder was OpenAI's "GPT-3" at 175 billion parameters, debuting July 22, 2020, (arxiv.org/pdf/2005.14165.pdf).
6. United Nations Rio Declaration, Principle 15: "Where there are threats of serious or irreversible damage, lack of full scientific certainty shall not be used as a reason for postponing cost-effective measures to prevent environmental degradation." www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A_CONF.151_26_Vol.I_Declaration.pdf.
7. So-called adversarial AI is to train one model and then to put that model into action with a second AI, one not trained at all on the subject matter of the first, to attempt to get desirable outcomes by feeding the first one synthesized data.
8. As it is conservative to assume that algorithms will learn to lie to us, it is unsurprising that two law professors have already suggested that price-fixing collusion amongst robot traders will be harder to detect than collusion amongst human ones – bottom line: designing a watchdog is probably harder than designing the system it exists to watch; see Ariel Ezrachi & Maurice Stucke, "When Robots Collude," May 2015, papers.ssrn.com/sol3/papers.cfm?abstract_id=2591874.
9. Sorin Adam Matei & Elisa Bertino, "Can N-Version Decision-Making Prevent the Rebirth of HAL 9000 in Military Camo? Using a 'Golden Rule' Threshold to Prevent AI Mission Individuation," *Policy-Based Autonomic Data Governance,* 2019.
10. Daniel E. Geer, "Application Security Matters," Open Web Application Security Project keynote, April 4, 2012, geer.tinho.net/geer.owasp.4iv12.txt.
11. Rudyard Kipling's poem "If" is a jewel, but this couplet captures autonomy and trust: "If neither foes nor loving friends can hurt you, If all men count with you, but none too much."
12. Federal Reserve Bank of Chicago, "Catastrophe Bonds: A Primer and Retrospective," 2018, www.chicagofed.org/publications/chicago-fed-letter/2018/405.
13. Congressional Research Service, "Price Anderson Act," 2018, crsreports.congress.gov/product/pdf/IF/IF10821.
14. As measured by total 2016 revenue, nine of the top twenty-five economic entities in the world are companies, www.weforum.org/agenda/2016/10/corporations-not-countries-dominate-the-list-of-the-world-s-biggest-economic-entities.
15. Facebook has more users than the combined population of India and China.
16. Lawrence Lessig, "Code Is Law", Harvard Magazine, January 2000, www.harvardmagazine.com/2000/01/code-is-law-html.
17. Article 15 (and others) in the EU's General Data Protection Regulation creates a right to challenge any algorithmic decision with the demand of "Why?" which cannot be answered by an uninterrogable algorithm; At what level of criticality do we require interrogability prior to legal deployment? Does this create a new variety of "informed consent" when a medical algorithm says what must be done but cannot explain why, and what does "informed" in "informed consent" then mean? www.clarip.com/data-privacy/gdpr-article-15.
18. While written with humans in mind, James Madison might well have been speaking to the issue at hand; "The accumulation of all powers ... in the same hands ... may justly be pronounced the very definition of tyranny," The Federalist No. 51, 1788.
19. Shoshana Zuboff, *Surveillance Capitalism,* Public Affairs Press, January 2019.
20. Elizabeth E. Joh, "A Gig Surveillance Economy," Hoover Aegis Series Paper No. 2108, November 10, 2021, s3.documentcloud.org/documents/21101558/a-gig-surveillance-economy.pdf.
21. As this working paper from the DNA Data Storage Alliance notes, global production of data storage devices is entering a period of profound and unfixable shortages; "An Introduction to DNA Data Storage," June 2021, dnastoragealliance.org/dev/wp-content/uploads/2021/06/DNA-Data-Storage-Alliance-An-Introduction-to-DNA-Data-Storage.pdf.
22. Kevin Gray, "The Last Fighter Pilot," Popular Science, December 22, 2015, www.popsci.com/last-fighter-pilot.

NOTES

23. Stephanie Forrest, Steven Hofmeyr, and Benjamin Edwards, "The Complex Science of Cyber Defense," Harvard Business Review, June 24, 2013, hbr.org/2013/06/embrace-the-complexity-of-cybe.
24. "Optimality vs. Fragility: Are Optimality and Efficiency the Enemies of Robustness and Resilience?" joint workshop by the Santa Fe Institute and Morgan Stanley, October 2, 2014; Abstract: "The goals of optimality and efficiency are pervasive in business and government, yet there is suggestive evidence that attempting to optimize a system's performance or to make it more efficient can make it more brittle, fragile, and less robust and resilient."
25. Daniel E. Geer, "A Rubicon," Hoover Aegis Series Paper No. 1801, www.hoover.org/research/rubicon.
26. The OODA loop is the repeating cycle of [observe, orient, decide, act] first developed by U.S. Air Force Col. John Boyd, military strategist.
27. William Langewiesche, "The Human Factor," *Vanity Fair*, 2014, www.vanityfair.com/news /business/2014/10/air-france-flight -447-crash.
28. "The cyborg chess players that can't be beaten," BBC Future, 2015, www.bbc.com/future/article/20151201-the-cyborg-chess-players-that-cant-be-beaten.
29. Nicky Case, "How to Become a Centaur," Journal of Design & Science, 2018, jods.mitpress.mit.edu/pub/issue3-case/release/6.
30. Gregory Travis, "How the Boeing 737 MAX Disaster Looks to a Software Developer," IEEE Spectrum, April 18, 2019, spectrum.ieee.org/how-the-boeing-737-max-disaster-looks-to-a-software-developer
31. "2001" script, 1968, where an autonomous system concludes that its own mission duty trumps human control
32. I do not say why. I only say what.
33. Daniel E. Geer & Richard Danzig, "Mutual Dependence Demands Mutual Sharing," IEEE Security & Privacy, January 2017, and in fuller treatment, Richard Danzig, *Surviving on a Diet of Poisoned Fruit*, Center for a New American Security, July 2014.

The Cyber Defense Review

Professional Commentary

Expeditionary Cyberspace Operations

Paul Schuh

ABSTRACT

As the pace of change in cyberspace operations and the nature of cyberspace forces continues to increase, the demand for innovative solutions to warfighters' needs and improved lethality of the joint force shows no signs of slacking, and the concepts and frameworks established just a few years ago to meet these needs have evolved to keep pace. The Cyber Mission Force is tasked to handle national and combatant commander priorities, working from garrison or deployed when necessary. As the Cyber Mission Force reached full mission capacity, including concomitant changes to their alignment and command and control, additional capability and capacity were required, including, ultimately, calls for additional types of cyberspace forces. In particular, there is a growing need for cyberspace forces that deploy within the physical domains. This article introduces and defines the term Expeditionary Cyberspace Operations (ECO) to standardize terminology for these tactical maneuver units operating across the competition continuum.

THESIS

The conduct of military cyberspace operations (CO) is both enabled and restricted by the nature of the domain, particularly the interconnectivity afforded by the Internet and other global, regional, and local networks. Although cyberspace forces can gain remote access to many targets in and through cyberspace, some targets with military utility are difficult to access from a distance and require maneuver in one of the physical domains to achieve close access of some form. And some systems to which cyberspace forces require close access are not targets at all.

Paul Schuh is the Technical Director of the Policy, Doctrine, & Strategy Division of U.S. Cyber Command (USCYBERCOM), the command Joint Doctrine Lead, and the command terminologist. He served for 20 years in the U.S. Navy as a Surface Warfare Officer and a Cryptologist. After retiring from the Navy, he was a Lead Associate at Booz-Allen Hamilton, supporting all the predecessor organizations of USCYBERCOM, and then transitioned to a DoD civilian position. He helped develop DoD's technical assurance evaluation standard for cyberspace capabilities and became the command's subject-matter expert for technical policy and doctrine. He authored the first detailed Cyber Lexicon in DoD, which became the foundation for portions of joint doctrine for cyberspace operations, for which he is currently the Lead Agent (pwschuh@cybercom.mil). Education: BS Computer Science, The Ohio State University, MS Computer Science, US Naval Postgraduate School, and MS Systems Technology-Joint C3, US Naval Postgraduate School.

In addition to personnel deployed from Cyber Mission Force (CMF) teams, a variety of additional units exist or are being developed that could conduct these close-access missions. The Services are conceiving, resourcing, and fielding elements to conduct CO in support of combatant commands (CCMDs), particularly including U.S. Special Operations Command (USSOCOM), beyond the operations of the 133 CMF teams under the combatant command (COCOM) authority of U.S. Cyber Command (USCYBERCOM). ***But what term should we use to refer to operations where cyberspace forces are required to deploy within the physical domains?*** "Tactical cyberspace operations" has been used colloquially to refer to this activity, but is that the correct term? This article examines the terminology, opportunities, and challenges in the development, deployment, and operations of the cyberspace forces that the Services and USSOCOM are proposing to meet. Additionally, this article introduces the related roles and responsibilities, command and control (C2), training, infrastructure, data, authorities, and capabilities issues.

BACKGROUND

The cyberspace challenges facing the United States (US) have evolved significantly since 2010, when USCYBERCOM was initially established as a subordinate unified command; in 2012, when the Department of Defense (DoD) decided to create the 133 teams of the CMF; in the 2018 elevation of USCYBERCOM to a unified combatant command; and the 2022 elevation of the Cyber National Mission Force Headquarters to a subordinate unified command. USCYBERCOM initially deployed small "expeditionary cyber support elements" forward to Afghanistan and Iraq to facilitate operations against extremists operating in cyberspace and to support physical domain tactical operations while at the same time overseeing the newly assigned and overwhelming task of securing and defending the Department of Defense Information Network (DODIN). The scope of

the USCYBERCOM mission, the number and complexity of its operations, and the policies and authorities under which it operates have grown tremendously since that time. Today, USCYBERCOM conducts operations to execute the following missions:

- Defend forward through persistent engagement to compete with and counter adversaries in competition below the level of armed conflict.
- Execute global operations under various Presidential determinations.
- Provide CO support to CCMDs and forces deployed in crisis response and contingencies.
- Protect the DODIN and support protection of the defense industrial base.
- Counter malign influence, including protecting US elections.
- Acquire and develop CO infrastructure and capabilities,
- Train and exercise the CMF in preparation for wartime operations,
- Execute the Presidentially assigned responsibilities of joint force provider and trainer.

Over the past eleven years, the pace and scope of USCYBERCOM's operations have steadily increased, as did DoD's recognition of both the critical need and growing promise of CO to meet the challenge posed by the Nation's most concerning nation-state threats and other malign actors, including the malicious activities of criminal, individual, and non-state origin in cyberspace. Meanwhile, the demand for tactical CO capacity and operations continued to grow, with increasing CCMD appetite for CO, particularly those integrated with physical domain maneuver forces.

OPPORTUNITIES

With over eleven years of operating experience under expanded responsibilities and authorities, there is potential of CO to better bear in competition below the level of traditional armed conflict and better prepare for its use in crisis, conflict, and war. This opportunity is accompanied by the inexorable convergence of CO, signals intelligence (SIGINT), electromagnetic warfare (EW), military information support operations (MISO), and other operations in the information environment, and by the concomitant need to organize and equip our forces. We must ensure our efforts are well coordinated from a resource perspective and informed by sound development and standardized operating principles. This effort requires a common understanding among the Office of the Secretary of Defense (OSD), the Services, CCMDs, and USCYBERCOM of the terminology and responsibilities that apply to our collective initiatives.

As cyberspace forces are developed and fielded by the Services and deployed by the Services and USSOCOM, we must standardize the associated terminology, examine authorities, develop processes, and clearly assign responsibilities between USCYBERCOM, the Services, and the CCMDs so that CO are conducted under proper authorities; effective C2; sufficient technical

control; and necessary coordination, deconfliction, and synchronization of tactical, operational, and strategic operations. We must ensure initiatives to build new teams of cyberspace forces are mutually informed to meet requirements while avoiding duplication and inefficiency in training, infrastructure and capabilities development, and concepts for effective force employment. This is particularly critical in cyberspace, where any specific operation can have significant impacts on the efficacy and viability of tactics, techniques, and capabilities across the entire joint force and intelligence enterprise and can significantly affect the viability and effectiveness of CO worldwide.

THE CHALLENGE

The goal of any cyberspace operation is maximum effectiveness in achieving its desired objective while protecting against secondary consequences to infrastructure, capabilities, and other operations. This means striking the right balance between distributed CO planning and execution by units under the Services, CCMDs, and maneuver commanders; and the centralized/delegated tasking authorities and technical control essential to enabling and protecting the effectiveness of the Nation's cyberspace forces and capabilities overall.

This challenge has two parts: defining and administering standards for training, qualifications, capabilities development, tradecraft, and operations, and then distributing operating responsibilities in a inherently interconnected domain that overlaps with the physical domains and in which many operations may have global implications for the joint force's overall operating effectiveness. These characteristics are unique to cyberspace. In the physical domains, the employment of a specific weapon or tactic in one area of operations (AO) against a specific target has few immediate implications for the viability of employing it in other AO's against different targets. In cyberspace, using a particular infrastructure, capability, or technique may risk or foreclose its effectiveness across the entire force as adversaries recognize and close exploited vulnerabilities. This means we must apply consistent approaches to ensure that tactical, operational, and strategic CO are effective and responsive to the commander's needs and yet conducted under appropriate authorities and effective technical control to ensure the protection of other operations and the overall capability of the force, and prevent or mitigate unintentional effects.

ISSUES

As understanding and experience in CO continue to evolve, and as the Services and USSOCOM invest in and deploy additional cyberspace force elements, several things must be done:

- Clarify the terminology related to CO support to tactical maneuver elements in the physical domains (this article).
- Clearly understand USCYBERCOM's role and authority in conducting CO at all levels of warfare.

- Better synchronize diverse force, capability, infrastructure, and training initiatives.
- Delineate responsibilities among USCYBERCOM, the Services, USSOCOM, and executing commands.

TERMINOLOGY

DoD joint doctrine, in Joint Publication 1, *Joint Warfighting*, describes three levels of warfare:

- **The tactical level of warfare** is where battles and engagements are planned and executed to achieve military objectives assigned to tactical units or task forces. (Note that this definition is focused on the units involved and the objectives sought, not on the unit's location.)
- **The operational level of warfare** is where campaigns and major operations are planned, conducted, and sustained to achieve strategic effects within a theater or another operational area.
- **The strategic level of warfare** is where a nation or group of nations uses national resources to achieve national or multinational strategic objectives.

Based on these definitions, a "tactical cyberspace operation" would be "a cyberspace operation conducted by tactical cyberspace forces units to achieve tactical effect." But that doesn't limit the scope of the term to only those tactical units that deploy with physical domain maneuver units. A combat mission team (CMT) operating remotely from the US will fit the same definition if it achieves tactical-level objectives, even if it is maneuvering to the target virtually, not physically. The distinction between operational and strategic CO depends upon the level of the intended objective. Similarly, strategic cyberspace operations could be defined as "cyberspace operations conducted using national resources and infrastructure to achieve national or multinational strategic objectives to gain advantage in competition and establish conditions to prevail in war." Like tactical CO, strategic CO can be conducted from any location, access permitting.

USE CASES

Consider a CO to support a particular maneuver engagement against an enemy's weapons systems or units within a particular geographic AO; in close proximity to physical domain forces in contact; using the organic resources of a locally deployed CO unit; with effects limited in duration and conducted for tactical impact. This is easily recognized as a tactical CO. Now consider a different example – a CO against a particular network or entity for a local tactical effect, but the execution of which depends on national assets, data, infrastructure, and capabilities; executed remotely across infrastructure far removed from the supported tactical operation; to create effects against a key node geographically far removed from the theater of the

desired tactical outcome. This is also a tactical CO but would require authorities not held by a local command, capabilities not directly available to the local commander, and execution under policy and technical control factors beyond tactical considerations. Conversely, an operational or strategic CO might involve dispersed global or localized operations that leverage forward-deployed forces in close physical proximity to an access point. The bottom line is that the location of the operation does not determine the level of the operation.

This spectrum of operations means that a unit of an Army Cyber Warfare Battalion or an Air Force Mission Defense Team must train to meet both the deployment and sustainment standards of their Service, as well as the CO technical, policy, and interoperability standards specified by CDRUSCYBERCOM. A unit of the Navy's Fleet Offensive Cyber Teams or a Marine Corps cyber mission element (CME) must carry equipment compatible with shipboard installation and maintenance and follow procedures that are fully consistent with tactics, techniques, and procedures specified by CDRUSCYBERCOM for gaining, maintaining, and sharing target accesses, which may have continued utility beyond the scope of the Team's deployment for later operations at the tactical, operational, or strategic level.

To the extent that units of the CMF are fully tasked with theater-level and national-level objectives, these units of cyberspace forces manned, retained, and/or fielded by the Services and USSOCOM will increasingly fulfill roles requiring deployment within the physical domains. Examples include deploying for the following objectives:

- Gain access through a low-power, point-to-point radio frequency (RF) link.
- Gain access through physical connection (tapping) to wired communications links.
- Gain access through hands-on keyboards or the insertion of portable media.
- Hunt for cyber threats on allied/partner networks.

PROPOSED DEFINITION

To summarize, the opposite of remote operations is not tactical operations. The opposite of remote is "proximal" or better "close access" or even better "expeditionary." To specify the training, equipping, and qualification standards required for units of cyberspace forces to deploy with forces maneuvering in the physical domains, as well as the policies and procedures required to standardize their tasking and their mission reporting, a more specific term than tactical is required: one that evokes its intended meaning.

The proper term for this type of deployed, "on-site" CO support, whether accompanying physical domain maneuver units or as stand-alone cyberspace forces, is ***expeditionary cyberspace operations (ECO)***. This term more precisely captures the essence of this activity, which is not just tactical and may even be strategic. In the DOD Dictionary of Military and Associated

Terms, the term expeditionary force is described as "organized to achieve a specific objective in a foreign country." Note that this term originated when forces had to be physically present in a foreign country to achieve their objectives. Still, its meaning endures to this day and captures the spirit and intent of the missions these CO units are intended to undertake.

Therefore, the *definition of expeditionary cyberspace operations* should be "cyberspace operations conducted by personnel or units of cyberspace forces deployed within the physical domains." ECO can describe not just external CO missions, i.e., offensive cyberspace operations (OCO) and defensive cyberspace operations response actions (DCO-RA), but also internal CO missions (defensive cyberspace operations-internal defensive measures (DCO-IDM) and DODIN operations. In fact, DCO-IDM hunt forward operations (HFO) are usually expeditionary.

MANNING FOR ECO

Any sufficiently trained, qualified, equipped, and appropriately ordered unit (or individual), including portions of the CMF, could undertake ECO. But because operational and strategic level taskings consume most of the CMF capability and capacity, units from groups 7 and 10 from the December 2019 SecDef *Cyberspace Operations Forces* (COF) Memo are the cyberspace forces likely to undertake many of these missions. These "non-COF" cyberspace forces are being developed specifically to undertake ECO and are manned by Service-retained (group 7) or USSOCOM-assigned (group 10) personnel. C2 of specific forces doing ECO will not be one-size-fits-all but will depend upon their assigned mission, including who has operational control (OPCON), tactical control (TACON), and the type of physical domain maneuver element they support.

TRAINING FOR ECO

As with other warfighting disciplines, effectiveness in the highly technical CO field is a direct function of individual and collective skills and training. USCYBERCOM will develop and direct training standards for all cyberspace forces, including standards guiding the training of cyberspace forces for ECO. USCYBERCOM will work with the Services and OSD to identify opportunities to gain efficiency in developing and administering CO training across the force. To maintain the capability to conduct Presidentially directed joint force trainer duties, CDRUSCYBERCOM must be able to establish, maintain, inspect, and certify minimum training standards for all cyberspace forces conducting ECO. This is done based on the position-specific qualifications documented in the Joint Cyberspace Training and Certification Standards (JCT&CS) used for the CMF. Units assigned to conduct ECO may propose and contribute to developing new, ECO-specific JCT&CS standards. Whenever possible, proposed new standards should be universal to all ECO missions, not specific to one Service or CCMD.

EQUIPPING FOR ECO

There have already been interoperability issues between CO capabilities procured by the Services for similar missions and effects. The Joint Cyber Warfighting Architecture (JCWA) Program is creating standards for Service- and USSOCOM-developed deployable cyberspace capabilities. Various JCWA portfolio interface control documents (ICDs) will establish interoperability requirements for cyberspace capabilities used for ECO, including data exchange formats. Capabilities like the deployable mission support system (DMSS) kits for cyberspace protection teams (CPTs) have already begun this standardization. The Services should procure infrastructure to support ECO under standards and policies defined in conjunction with USCYBERCOM, who will be DoD's lead and approval authority. USCYBERCOM, in conjunction with the Services, will define data standards, governing policies, and cyberspace capability development policies. Decentralized development of cyberspace capabilities to support ongoing operations will be the norm, but it will be subject to technical control and governance of USCYBERCOM.

EXISTING AUTHORITIES

Conduct of ECO, like any military operation, falls to those units with an assigned ECO mission and an execute order (EXORD) to undertake a specific operation. Their specific tasking may be covered inside a larger, all-domain operational order (OPORD) or in a stand-alone order to conduct CO in support of another named operation. In general, ECO are subject to the same constraints and restraints as other CO. This includes national policy, DoD policy, and Chairman's EXORDS that apply to all CCDRs. Further, external mission ECO remain subject to the requirement for interagency deconfliction for cyberspace attack and exploitation actions.

All ECO-capable units derive their authority to operate from their operational chain of command. Any combatant commander can conduct CO under specific circumstances. However, only CDRUSCYBERCOM is assigned specific responsibilities for CO in the Unified Command Plan (UCP); represents DoD in the interagency deconfliction process; is under order to secure, operate, and defend the DODIN; and routinely deploys forces to defend non-DODIN blue cyberspace. Consequently, the US military must consider how to best characterize and assign responsibilities and C2 for tactical, operational, and strategic CO to ensure maximum effectiveness while avoiding unintended consequences.

NEW AUTHORITIES

As the Services continue to develop cyberspace forces that fall under the "non-COF" designation, USCYBERCOM should maintain centralized tasking authority for all CO, including ECO, to maintain cyberspace situational awareness and to aid in required operational deconfliction. In the same manner that National Security Agency (NSA) delegates SIGINT operational tasking authority (SOTA), CDRUSCYBERCOM could delegate *cyberspace operations tasking authority* ("COTA") to tactical commanders in a manner that focuses their activities on mission-relevant

targets and limits risk to other similar or associated CO. COTA would be the authority for a military commander to operationally direct, and levy CO requirements on, designated units.

Likewise, in the same way that NSA exercises SIGINT technical control (SIGINT TECHCON), CDRUSCYBERCOM could exercise "*CO TECHCON*." This control over the policies and standards that underpin the CO would not be delegated. CDRUSCYBERCOM should retain control over the uniform techniques, standards, and support mechanisms by which CO, including ECO, are conducted, by which CO operational and mission reporting is produced, and how mission-relevant information is collected, processed, and disseminated.

SUMMARY

Expeditionary Cyberspace Operations are happening now and will occur more in the future. Establishing the correct terminology and providing its definition are just two short steps on a long journey to make the expeditionary operations of cyberspace forces part of a comprehensive framework of fully deconflicted, mutually supporting, and globally integrated CO.

DISCLAIMER

The views expressed are those of the author and do not reflect the official policy or position of U.S. Cyber Command, the Department of Defense, or the U.S. Government.

Countermeasures as Lightning, not a Lightning Bug:

Illuminating the Legal Doctrine

Lieutenant Colonel Mark A. Visger
Professor Zhanna L. Malekos Smith

Mark Twain famously observed that the difference between the "right word and the almost right word is the difference between lightning and a lightning bug." Similarly, here, the term 'countermeasures' has a particular textual meaning under international law. It is not an unfettered privilege that can be conjured at any whim—especially in the cyber domain. Definitionally, countermeasures are a limited set of responses available to an injured State responding to an aggressor State's behavior; further, these responses would otherwise be unlawful but for the aggressor State's "unfriendly" and illegal actions.

In a previous *The Cyber Defense Review* article, Dr. Nori Katagiri outlined challenges to implementing countermeasures in cyberspace from a perspective of active defense.[1] For purposes of his article he defined countermeasures as "a set of responses toward verified attackers within a reasonably short period of time."[2] He also discussed the challenges of implementing an active defense approach from a strategic and political perspective. Yet "countermeasures," as described by Dr. Katagari (i.e., an active defense cyber strategy, which we will refer to as "active defense perspective" for this paper), are quite different from "countermeasures" as traditionally defined under international law. As a legal matter, countermeasures are responses to unfriendly state actions that would otherwise be unlawful but for the responsible State's misconduct. As articulated in Tallinn Manual 2.0, an "injured State" engages in countermeasures in order to induce the "responsible State" to cease its wrongful behavior.[3]

This article explains why the legal countermeasures doctrine addresses a different set of problems than Dr. Katagari's active defense perspective. In fact, the legal doctrine will not be invoked to justify action except in a narrow subset of active defense operations because international law limits countermeasures in terms of purpose, duration, and scope.[4]

Lieutenant Colonel Mark A. Visger, an Academy Professor at the Army Cyber Institute, leads the Cyber Law and Policy Research Team. He has taught courses in Cyber Law, International Law, National Security Law, Constitutional and Military Law, as well as Computing Fundamentals.

Further, while the legal doctrine of countermeasures may sometimes justify active defense responses, the doctrine often will not be needed for an active defense cyber operation to remain in compliance with international law. Law and strategy are not one and the same. Law can undergird strategy and strategy can fortify law, but to treat them interchangeably could, as Mark Twain noted, produce an unpleasant shock.

We turn now to examining the term "countermeasures" and its distinct meaning under international law. The legal doctrine shares some commonalities with the active defense perspective advocated by Dr. Katagiri, which may cause readers to muddle the legal doctrine with the policy and strategy doctrine.

COUNTERMEASURES WITHIN THE INTERNATIONAL LEGAL SYSTEM

In order to place the legal countermeasures doctrine in proper context, it is important to review the overall framework of international law, which differs from traditional understandings of what constitutes law, particularly when it comes to enforcement of international law. At its heart, countermeasures are a legal enforcement mechanism. They function as a way to compel another State to comply with international law.

Characteristics Unique to International Law

International law is unique in several respects. First, with some exceptions, it primarily governs Nation-States in their interactions with other Nation-States, and not between nations and individuals (e.g., treaty obligations between Country X and Country Y). Second, with some modern era exceptions, Nation-States are sovereign entities and there is no higher-level sovereign entity to govern these sovereign States and enforce international legal obligations. International courts and other international bodies exist, but their reach is limited because States must willingly submit to their jurisdiction before any legal action

Professor Zhanna L. Malekos Smith, an adjunct fellow with the Strategic Technologies Program at the Center for Strategic and International Studies (CSIS) in Washington, D.C., an assistant professor in the Department of Systems Engineering at the U.S. Military Academy at West Point, a fellow with the Army Cyber Institute, and an affiliate faculty member with the Modern War Institute.

may commence. As a result, international law is largely self-enforcing among the Nation-States themselves—which leads to significant enforcement challenges. Despite enforceability constraints, most nations recognize the value of a rules-based international order and seek to comply. This dynamic is reflected in Louis Henkin's famous statement: "Almost all nations observe almost all principles of international law and almost all of their obligations almost all of the time."[5]

Recognizing the self-enforcing nature of international law between States is key to understanding countermeasures. Moreover, because there are no police or prosecutors to enforce legal claims between States, aggrieved States are on their own to seek redress. Prior to the treaty prohibitions on use of force in the UN Charter in 1945, military action was routine in enforcing international law obligations. Without this bludgeon (particularly for stronger nations), countermeasures are one of the few enforcement tools remaining. As an example, if country X is violating its treaty obligations to allow country Y to traverse a maritime strait, country Y may not honor treaty obligations to provide favorable trading conditions to country X, thereby economically punishing country X and causing it to re-open the strait.

Evolving International Legal Norms in Cyberspace

Our understanding of how international law is mapping onto cyber operations remains in its infancy. However, in 2015 the UN's Group of Governmental Experts (GGE) achieved consensus on eleven non-binding norms of responsible state behavior which now guide international conduct in cyberspace. In 2019, to help promote inclusivity and participation by all States in discussing international cyber stability, the UN First Committee ordained the Open-Ended Working Group (OEWG).[6] In May 2021, this agreement was endorsed again by all UN member States at the end of the UN's Open-Ended Working Group. "The OEWG and GGE work together to create and reinforce this framework"

explains cyber strategy expert, James Lewis of the Center for Strategic and International Studies. Focusing on the US perspective on promoting stability in cyberspace, the newly published 2022 National Security Strategy champions the 2015 UN General Assembly's endorsed framework for cybersecurity:

> As an open society, the United States has a clear interest in strengthening norms that mitigate cyber threats and enhance stability in cyberspace. We aim to deter cyber attacks from state and non state actors and will respond decisively with all appropriate tools of national power to hostile acts in cyberspace, including those that disrupt or degrade vital national functions or critical infrastructure. We will continue to promote adherence to the UN General Assembly-endorsed framework of responsible state behavior in cyberspace, which recognizes that international law applies online, just as it does offline.[7]

In summary, the ability to sustain a framework for responsible state behavior in cyberspace is powered by three distinct engines. First, norms—reaching a consensus on how States should act in cyberspace; second are confidence-building measures to enhance accountability, communication, and trust amongst States, and lastly, capacity building to enable States in both the technical and political sense to adhere to a framework in a "rules-based environment."[8]

Contours of the Countermeasures Legal Doctrine

Countermeasures are unfriendly and facially contrary to international law, yet they facilitate States seeking to enforce their legal rights under certain conditions. Again, because international law is largely self-enforcing, enforcement mechanisms become critical for States to protect their legal rights.

In addition to countermeasures, another significant mechanism for a wronged State is retorsion—an unfriendly but lawful act.[9] The difference between countermeasures and retorsion is simple—an act of retorsion does not violate international law. According to Professor Jeffrey Kosseff of the US Naval Academy, "[r]etorsion is both flexible and limited. It is flexible because, unlike other responses, it is subject to relatively few operational requirements. It is limited because it may only consist of actions that comply with international law."[10] Due to the inherent limits on retorsion, countermeasures appear to be a better enforcement mechanism. While countermeasures can be used skillfully to induce a State to comply with the law, they face legal limitations on when and how they can be used. Cyber countermeasures operate under strict criterion based on:

1. A requirement to notify and offer to negotiate;
2. The countermeasure response must be proportionate to the initial wrongful act; and
3. Some existing legal frameworks or agreements restrict usage of countermeasures (for example, a countermeasure action cannot violate fundamental human rights).

Another challenge to employing countermeasures is that they are not available to non-state actors and cannot be applied by States against non-state actors who are not acting for a State, or otherwise receiving state support for such actions.* If a State has effective control over the cyber operation waged by the non-state actor, responsibility could be imputed under the doctrine of State responsibility. For example, in a lawsuit brought by Nicaragua against the US over their support of the Contra rebels, the International Court of Justice evaluated whether an "armed attack" waged by non-state actors (the Contras) could be imputed to the US, specifically whether the US "had effective control of the military or paramilitary operation[.]"[11] Thus, private actors engaged in hostile cyber operations adds another wrinkle to the legal analysis. States seeking to use countermeasures must conclude that the initial cyberattack violated international law and that the attack was attributable to a state actor, and not private individuals such as "patriotic hackers."

These limits will likely restrict a State's ability to utilize the doctrine in an active defense cyber operation. When considering whether to deploy countermeasures, it is best to recall the following cautionary statement: "[Countermeasures] should be used with a spirit of great moderation and be accompanied by a genuine effort at resolving the dispute."[12]

WHAT IS AN INTERNATIONALLY WRONGFUL ACT IN CYBER? A NECESSARY PRECONDITION.

The foregoing discussion demonstrates that countermeasures will only be necessary to counter a cyber operation that violates international law. Otherwise, a State engaged in a cyber active defense response that does not violate the law would not need to invoke the doctrine as the response more accurately would constitute an act of retorsion. In fact, there are likely to be a wide variety of potential cyber operations, including active defense responses, which would comply with international law. Such operations would not require the legal justification that the countermeasures doctrine provides. Further, to claim a countermeasures justification, the initial cyber operation which prompted the active defense response must itself violate international law. Which raises the question—what peacetime cyber operations violate international law?

To answer this question, three international law prohibitions may be implicated by a peacetime cyber operation:

1. Violating a state's sovereignty;
2. Coercively intervening into a state's internal affairs; and
3. Use of force. In addition, one key category of activity, espionage, does not constitute a per se violation of international law.[13]

* Note that a State may have a legal obligation to exercise due diligence to prevent non-state actors from engaging in malicious cyber operations against information communication technologies. Violation of this legal obligation may serve as a basis for invoking countermeasures, although the exact contours of this legal obligations is not clear.

These four doctrines are each discussed below.

1. Sovereignty – Maybe a Violation of International Law

This doctrine arises from the core international law principle of sovereignty—the idea that a State has "supreme, absolute, and uncontrollable power."[14] In Tallinn 2.0, the International Group of Experts stated that this supreme authority extends to "cyber infrastructure, persons, and cyber activities located within [a State's territory]."[15] With this foundation, a State violates the sovereignty of another State when the violator interferes with the exercise of sovereign authority. The Tallinn 2.0 experts specified two possible bases for violation of sovereignty in cyberspace—(1) "the degree of infringement upon the target State's territorial integrity"(through damage, loss of functionality or other infringement of cyber infrastructure or cyber activities within the target State's territory); or (2) "interference or usurpation of inherently governmental functions" of the target States.[16] Unfortunately, while the Tallinn 2.0 experts included a list of non-exclusive factors to consider in judging whether a sovereignty violation has occurred, the exact contours of what activities constitute a sovereignty violation remain unclear.

To confuse matters further, not all nations accept the proposition that a violation of sovereignty violates international law. The UK strongly asserts that sovereignty is but a principle underlying the international legal system, not a rule that can be violated. In May 2022 the former UK Attorney General, Suella Braverman, reaffirmed that the UK regarded sovereignty as an international relations construct and not a rule of international law.[17] Under this sovereignty-as-principle approach, violations of sovereignty do not, standing alone, violate international law. Similarly, the former chief legal advisor to U.S. Cyber Command, then-Colonel Gary Corn, espoused this position in statements and publications made in a personal capacity.[18] The US official position on the matter has been studiously neutral, with hints of sympathy for the British position.[19] Many States take the opposite position that violating sovereignty violates international law, so there is no consensus on this issue.

2. Coercive Intervention

The second doctrine potentially implicated by cyber operations is the prohibition of coercive intervention in the affairs of another State. This prohibition generally protects activities that fall within a State's exclusive control, the domaine réservé. States coercively interfering in another State's domaine réservé violate this prohibition. Focusing on the historical context of this concept, in 1986 the International Court of Justice held in Nicaragua v. United States that acts of coercion amount to intervention, by a State forcing another State to follow a course of action that it would not otherwise have done.[20] As a result, the court ruled that American support to the Contra rebels breached this rule. Essentially, in evaluating the risk of coercive effects in cyber operations, the Tallinn 2.0 experts focused on the removal of choice, stating that coercion "refers to an affirmative act designed to deprive another State of its freedom of choice, that is, to force that State to act in an involuntary manner or involuntarily refrain from acting in a particular way."[21]

3. Unlawful Use of Force

Article 2(4) of the UN Charter prohibits States from employing a "threat or use of force" against another member State: "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the Purposes of the United Nations."[22] "Use of force" is nowhere defined, and ambiguity as to what amounts to a use of force in cyberspace remains unsettled in the international legal community. The Tallinn Manual seeks to clarify by stating that "[a] cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force,"[23] and listing a number of criteria to consider in this determination. The Tallinn Manual also defines 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."[24] Such statements are helpful, however, they are not a bright-line rule for what would meet the use of force threshold.

States suffering an armed attack in violation of Article 2(4) have the inherent right to use force in self-defense under Article 51 of the UN Charter, which is another enforcement mechanism for the limited subset of scenarios that justify use of force.

4. Not a Per Se International Law Violation: Cyber Espionage

It is important to define the final category of cyber operations–traditional espionage activities. First, espionage is implicitly recognized as lawful under international law. Peacetime espionage, according to international relations theorist Roger Scott, "is not prohibited by international law as a fundamentally wrongful activity."[25] As to wartime espionage, the Lieber Code of 1863, adopted that same year by the US Army, recognizes spies as a condition of war (*Jus in bello)* and has become part of the foundational basis for other nations' treaties and military codes.[26]

Dr. Catherine Lotrionte of the Atlantic Council describes "espionage [as] one aspect of a nation's intelligence work, encompassing the government's efforts to acquire classified or otherwise protected information in order to deal with threats from actual or potential adversaries."[27] Although States collect economic intelligence – a subset of traditional espionage – the US has urged that commercially-motivated espionage, also known as industrial espionage, should be unlawful during peacetime under international law. The US distinguishes economic espionage and economic intelligence because the former entails "providing such information to the collecting State's own private entities to gain economic advantages."[28] Under US domestic law, the Economic Espionage Act adds clarity by defining acts of economic espionage as: "knowingly (1) performing targeting or acquisition of trade secrets, or (2) benefiting any foreign government, foreign instrumentality, or foreign agent."[29] The FBI has classified industrial espionage as the theft of trade secrets, as seen in indictments of Chinese state actors for targeting US companies and stealing trade secrets and intellectual property.[30] As a matter of public policy, the US does

not conduct economic espionage, but does collect economic intelligence to support national security motivated espionage. The People's Republic of China, however, has rejected this 'western' distinction, which remains a lingering point of contention in US-China relations.

Tallinn Manual 2.0 experts generally agree that merely conducting cyber espionage operations in peacetime, absent physical damage or injury to the functionality of the targeted State's cyber infrastructure, is not a breach of sovereignty, or per se violation of international law.[31]

Closing Thoughts on Cyberspace Operations and International Law Violations

This review of international law illustrates the limited circumstances wherein cyber operations may violate international law. To illustrate these limits, Michael Schmitt, lead editor of the Tallinn Manual 2.0, concluded that he did not consider the 2020 SolarWinds hack to be in violation of international law.[32] If correct, countermeasures would not be a lawful response to SolarWinds. This would not foreclose active defense responses to SolarWinds, so long as those defense actions themselves do not violate international law as described above. Many cyberattacks do not violate international law—either because they are not legally attributable to a State, or because they fall short of breaching the aforementioned standards.

An International Law Perspective on Active Defense Cyber Operations

It is important in concluding to offer parting thoughts on Dr. Katagiri's article from a legal perspective. His article recommends three considerations in employing countermeasures as active defense: 1. Limited aim of defense and deterrence; 2. Challenges in defending critical infrastructure; and 3. Compliance with rules of behavior.

The first point advocates active defense countermeasures not for preemption, but solely "for defense and deterrence through retaliation and punishment." As discussed above, legal countermeasures are not a form of deterrence. Deterrence by denial is denying your adversary the ability to benefit of taking any course of action that would harm your interests and/or position. Deterrence by cost imposition is influencing your adversary's cost-benefit calculus such that the perceived cost outweighs the benefit.[33] By contrast, lawful countermeasures seek only to induce the offending State to cease its wrongful behavior. Yet Dr. Katagiri's more expansive definition merits consideration. States engaged in active defense cyber operations may conclude that it is inappropriate to wage such operations where preemption is the primary objective. In such cases, Dr. Katagiri's analysis adds helpful considerations in assessing the role of active defense activities in both policy and strategy.

Dr. Katagiri's second point flags challenges associated with labeling protected critical infrastructure, which may warrant stronger active defense responses. Specifically, he outlines the differences in US, Russian, and Chinese approaches to identifying critical infrastructure. These differing approaches create escalatory risk because hackers, whether state-sponsored or not, may not recognize what constitutes critical infrastructure.

Because merely attaching the words "critical infrastructure" to an entity does not mean that it is "off limits" from targeting under international law. One must still examine the underlying impact and effects of the cyber operation in question in order to determine whether it violates international law. In fact, the term critical infrastructure appears nowhere in the Tallinn 2.0 discussion of countermeasures. A state designation of critical infrastructure, at most, may bolster a claim that a legal line has been crossed, but without more, it is not legally conclusive.

Finally, Dr. Katagiri recommends that countermeasures comply with existing norms of behavior in the international community, and we as lawyers concur. We urge precision, however, in how those rules of behavior are expressed–and clearly communicating whether limitations are legally adopted, or adopted as a matter of policy. Some legal doctrines Dr. Katagiri cites apply only in an armed conflict context. The US uses an approach consistent with Dr. Katagiri's recommendation by ensuring all military operations comply with the Law of Armed Conflict, regardless of whether there is armed conflict. As a matter of policy, the US adopts this approach, but this is not required by law. Rather, the Law of Armed Conflict is only triggered when armed conflict exists. Similarly, as constraints are placed on active defense cyber operations, States should clarify whether such limitations are legally mandated, or voluntarily followed as a matter of policy.

CONCLUSION

This article examined why it is important to keep the countermeasures legal doctrine separate and distinct from cyber operations employing active defense strategies. Ultimately, the legal doctrine applies only in a narrow set of circumstances. Active defense cyberspace operations will not frequently trigger this legal doctrine. More often than not, active defense cyber operations will comply with international law without resorting to countermeasures as a legal justification. We also have underscored the significant ambiguity in international law as applied to cyber operations. For this reason, precision of thought in understanding the strategic value of countermeasures in cyber operations and their legal basis under international law makes a world of difference–just like the difference between lightning and a lightning bug.

DISCLAIMER

Views expressed in this publication are solely those of the authors and not those of the U.S. Military Academy, the Department of Defense, CSIS, or the U.S. Government.

NOTES

1. Nori Katagiri, "Three Conditions for Cyber Countermeasures: Opportunities and Challenges of Active-Defense Operations, *The Cyber* D*efense Revie*w 7, no. 3 (Summer 2022): 79.
2. Ibid., 81.
3. NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual 2.0 on the International* Law *Applicable to Cyber Operations,* Michael N. Schmitt, ed. (Cambridge: Cambridge University Press, 2017): 111-12. The Tallinn Manual 2.0 defines cyber operations as "employment of cyber capabilities to achieve objectives in or through cyberspace[.]" Ibid., 562.
4. Jeff Kosseff, "Retorsion as a Response to Ongoing Malign Cyber Operati*ons," 12th International Conference on Cyber Conflict* (2020): 11 https://ccdcoe.org/uploads/2020/05/CyCon_2020_1_Kosseff.pdf.
5. Louis Henkin, How Nations Behave (Columbia Univ. Press, 1979), 47.
6. James Lewis, *Cyber Stability Framework: Norms of Responsible State Behavior, International Law, CBMs* (2020), available at https://www.youtube.com/watch?v=MZlsGOC185M.
7. The White House, *2022 National Security Strategy,* (October 12, 2022), https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.
8. James Andrew Lewis, "Creating Accountability for Global Cyber Norms," *CSIS* (February 23, 2022) https://www.csis.org/analysis/creating-accountability-global-cyber-norms.
9. Kosseff, Retorsion, 10.
10. Ibid.
11. Nicaragua v. U.S. (Military and Paramilitary Activities), 1986 I.C.J. 195.
12. U.S. v. France (Air Services Agreement of March 27, 1946), 18 RIAA 416, 445 (1979).
13. NATO, Tallinn Manual 2.0, 168.
14. Black's Law Dictionary (6th edition, 1991): 1396.
15. NATO, Tallinn Manual 2.0, 13.
16. Ibid., 20.
17. Suella Braverman, *International Law in Future Frontiers* (2022), https://www.gov.uk/government/speeches/international-law-in-future-frontiers.
18. Colonel Gary Corn and Robert Taylor, "Sovereignty in the Age of Cyber." *AJIL Unbound* 111 (August 21, 2017): 207.
19. Honorable Paul C. Ney, Jr., *DoD General Counsel Remarks at U.S. Cyber Command Legal Conferenc*e (2020), https://www.defense.gov/News/Speeches/speech/article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/.
20. Nicaragua v. U.S.
21. NATO, Tallinn Manual 2.0, 317. As an example of how coercive intervention applies to misinformation campaigns against elections, see Craig Forcese, "The 'Hacked' US Election: Is International Law Silent, Faced with the Clatter of Cyrillic Keyboards?" *Just Security Blog* (December 16, 2016), https://www.justsecurity.org/35652/hacked-electioninternational-law-silent-faced-clatter-cyrillic-keyboards.
22. United Nations Charter, Art. 2(4) (1945).
23. NATO, Tallinn Manual 2.0, 330.
24. Ibid., 415.
25. Robert D. Williams, "Spy Game Change: Cyber Networks, Intelligence Collection, and Covert Action." *George Washington Law Review,* 79, no. 4 (2011): 1162.
26. American Red Cross, "The Lieber Code, Limiting the Devastation of War" (2017), https://silo.tips/download/the-lieber-code-limiting-the-devastation-of-war.
27. Catherine Lotrionte, "Countering State-Sponsored Cyber Economic Espionage Under International Law." *North Carolina Journal of International Law and Commercial Regulation,* 40 (2014): 463-64.
28. Ibid.
29. U.S. Economic Espionage Act, U.S. Code 18 (2018), § 1831.

NOTES

30. U.S. Department of Justice, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," (May 19, 2014), https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor; "Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax," (February 10, 2020), https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking.
31. NATO, Tallinn Manual 2.0, 168.
32. Michael Schmitt, "Top Expert Backgrounder: Russia's SolarWinds Operation and International Law," *Just Security* (December 21, 2020), https://www.justsecurity.org/73946/russias-solarwinds-operation-and-international-law.
33. Erica Lonergan and Mark Montgomery, "What is the Future of Cyber Deterrence?" *SAIS Review*, vol. 41 no. 2 (Summer-Fall 2021): 62. For an excellent overview of deterrence in the cyber context featuring the late former Secretary of Defense, Ash Carter, see *How deterrence is changing, explained by Defense Secretary Ash Carter.* https://www.youtube.com/watch?v=Wp4fKplfGRc.

The Cyber Defense Review

Research Articles

Gaining Competitive Advantages in Cyberspace

through the Integration of Breakthrough Technologies in Autonomy, Artificial Intelligence, and Machine Learning

Lieutenant Colonel Nathaniel D. Bastian, Ph.D.

ABSTRACT

Cyberspace has characteristics that differ from air, land, maritime, and space domains, which affect how the Joint Force operates and defends it. Fast-moving innovations are transforming the character of warfare in cyberspace, requiring novel technology integration. Effective integration of breakthrough technologies in autonomy, artificial intelligence, and machine learning into cyberspace can enable competitive advantages to be gained that enhance the combat power of joint forces conducting multi-domain operations. These technologies help shorten the sensor-to-shooter pathway to accelerate and optimize decision-making processes. These technologies also permit the enhancement of cyber situational understanding from the ingest, fusion, synthesis, analysis, and visualization of big data from varied cyber data sources to enable decisive, warfighting information advantage via the display of key cyber terrain with relevance in the commander's area of operations at the tactical edge. These technologies engender actionable information and recommendations to optimize human-machine decision-making via autonomous active cyber defense to effectively execute command and control while informing resourcing decisions. Competitive advantages gained allow key actions to be taken to generate, preserve, and apply informational power against a relevant actor while also permitting maneuver through the information environment.

INTRODUCTION AND BACKGROUND

Cyberspace has characteristics that differ from the air, land, maritime, and space domains. These characteristics affect how the Joint Force operates and defends cyberspace infrastructure, information, information systems, and data.[1] Joint forces have integrated and synchronized cyberspace capabilities along with the

LTC Nathaniel D. Bastian, Ph.D., is an Academy Professor at the United States Military Academy at West Point. He serves as Chief Data Scientist and Senior Research Scientist at the Army Cyber Institute (ACI) within the Department of Electrical Engineering and Computer Science, as well as Assistant Professor of Operations Research and Data Science with a dual faculty appointment in the Department of Systems Engineering and the Department of Mathematical Sciences. He leads the ACI's Data and Decision Sciences Division, directs the ACI's Intelligent Cyber-Systems and Analytics Research Lab and the ACI's Internet of Things Research Lab, and co-directs the ACI's Cyber Modeling and Simulation Research Lab. He has co-authored 80+ refereed publications, received $4M+ in externally-funded research monies from DEVCOM, NSA, AFRL, OUSD(R&E), DARPA, and NSF, served as a Visiting Research Fellow at the Johns Hopkins University Applied Physics Lab, and served as Distinguished Visiting Professor at the NSA.

authorities to conduct effective cyberspace operations as part of an overall combined arms strategy in support of Multi-Domain Operations (MDO) and Joint All-Domain Command and Control (JADC2). Cyberspace operations provide the commander the capability to process and manage operationally relevant actions, allowing simultaneous and linked maneuver, in, through and across multiple domains and the information environment, while engaging adversaries and populations directly across time, space, and scale.[2]

The information environment (IE) is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information.[3] To manage the complexity of the cyberspace domain, the military divided it into separate layers, to include physical, logical, and cyber-persona.[4] Connections between the layers of cyberspace generate a portion of the IE that is divided into three dimensions – physical, informational, and cognitive; each dimension is associated with a specific layer of cyberspace[5] in which the latest technology can be integrated.

Fast-moving trends are rapidly transforming the character of warfare in cyberspace, which include significant advances in science and technology. These new discoveries and innovations are occurring at a breakneck pace. While the nature of war may remain constant, its speed, automation, effects, and increasingly integrated multi-domain conduct are changing, requiring novel technology integration. However, which breakthrough technologies and in what ways can their subsequent integration engender competitive advantage gains in cyberspace? Effective integration of breakthrough technologies in autonomy, artificial intelligence, and machine learning into cyberspace can enable competitive advantages to be gained to help provide joint commanders a full range of physical, virtual, lethal, and nonlethal capabilities tailored to enhance the combat power of joint forces conducting MDO. First,

these technologies can help shorten the sensor-to-shooter pathway to accelerate and optimize decision-making composed of a complex sequence of operations to be performed in varied cyberspace environments and situations. Second, these technologies permit the enhancement of cyber situational understanding from the ingest, fusion, synthesis, analysis, and visualization of big data from varied cyber data sources to enable decisive, warfighting information advantage via the display of key terrain in cyberspace with relevance in the commander's area of operations at the tactical edge. Third, these technologies help engender actionable information and recommendations to optimize (accelerate, augment, and improve) human-machine decision-making via autonomous active cyber defense to effectively execute C2 while informing resourcing decisions.

To define these technologies, autonomy is the ability of a system to respond to situations by independently composing and selecting among different courses of action to accomplish goals based on knowledge and a contextual understanding of the world, itself, and the situation. Moreover, autonomy can best be expressed as a state of technological activity in which human interaction is limited or completely removed. Artificial intelligence (AI) is generally defined as a set of symbolic and/or non-symbolic techniques that enable machines to perform tasks that normally require human intelligence.[7] As a subset of AI, machine learning (ML) entails statistical/probabilistic algorithms that learn patterns in data as opposed to the use of symbolic representations of human knowledge.[8]

Shortened Sensor-to-Shooter Pathway for Accelerated and Optimized Decision-Making

One competitive advantage to be gained in cyberspace is that breakthrough autonomy AI, and ML technologies can help increase the automation of operational processes/functions and data processing while improving situational awareness.[9] The effective integration of these breakthrough technologies can enable the timely and optimized combination of software, sensors, systems, and humans to allow a complex sequence of operations to be performed in varied cyberspace environments and situations.[10] Currently, the Joint Force lacks a digitized network lethality backbone at scale, where warfighters must manually assess sensor data, identify targets, and then choose the weapon of choice to inform the commander's engagement decisions. Further, there is no digitized collaboration between platforms and C2 nodes, and there is no ability for commanders to leverage sensor data across the formation from multiple inputs to make informed, collaborative, and optimized decisions. Moreover, these sensor-to-human-to-shooter networks often have long processing times between target identification and target engagement, which has the potential to hinder successful execution of MDO significantly. Cyberspace infrastructure, however, is network-agnostic as it supports all users.[11] Cyberspace operations, in conjunction with autonomy, AI, and ML technology-enhanced cyberspace infrastructure, make it possible to shorten the sensor-to-shooter pathway to accelerate and optimize decision-making in terms of the best available shooter to respond with.

For example, the U.S. Army's Program Executive Officer for Intelligence, Electronic Warfare, and Sensors (PEO IEW&S) has the Tactical Intelligence Targeting Access Node (TITAN) modernization program within its Project Manager for Intelligence Systems & Analytics (PM IS&A) that is developing and integrating autonomy, AI, and ML technologies into cyberspace operations to automate target recognition, identification, and geolocation from multiple sensors to fuse the common intelligence picture and make target recommendations that reduce sensor-to-shooter timelines.[12] TITAN is a scalable and expeditionary intelligence ground station that supports commanders across the JADC2 battlefield framework with capabilities tailored to echelon. The capability ingests space and high altitude, aerial and terrestrial layer sensors and integrates an AI system, known as Prometheus,[13] to rapidly fuse and synthesize the sensor feeds into meaningful information to then provide target nominations directly to fires command and control networks as well as multi-discipline intelligence support to targeting and situational awareness in support of mission command.[14] Once targets are nominated, an AI-enabled targeting system known as FIRES Synchronization to Optimize Responses in Multi-Domain Operations (FIRESTORM), which is a science and technology effort led by the U.S. Army Combat Capabilities Development Command (DEVCOM) Armament Center, then ingests the sensor data (radio data link feeds, etc.) of adversary threats from Prometheus, uses One World Terrain to map the battlefield (navigational and terrain-specific, weather conditions, target coordinates, and precisely identified enemy location information), and optimally recommends the best weapon system to engage specific targets.[15]

In this example, the primary competitive advantage gained in cyberspace is saving the Joint Force commander's time for decision-making (reduced from 20 minutes to 32 seconds)[16] while providing actionable, effective, and efficient recommendations to deliver the right effects in near real time. Specifically, an integrated and scalable intelligence, surveillance, and reconnaissance (ISR) targeting and tasking capability shortens the sensor-to-shooter pathway by receiving multi-intelligence sensor feeds and directly down links them from strategic to tactical (process), uses on-board autonomy, AI and ML technologies to conduct target detection and mensuration to feed the intelligence common operating picture (exploit). This provides targetable data to decision-makers and fires C2 platforms for effect (disseminate), and finally uses an AI-enabled decision aid for weapon-target matching (optimize) to determine the best firing system to respond to the given threats (based on the terrain, available weapons, proximity, and number of other threats) while providing critical target deconfliction and an updated common operating picture (COP) for enemy and friendly situations.[17] Overall, the integration of breakthrough technologies leads to reduced target engagement time, accelerated and coordinated response of assets across multiple domains, faster determination of information relevant/important to the mission, and reduced decision cycle time and data overhead that enable success for Joint forces conducting MDO. Information-centric technologies, where network connections are ad hoc and information exchange and interconnectivity fluctuate at speeds beyond human capacity,[18] allow competitive advantages to be gained in cyberspace in the form of networked

lethality. Knowledge, capabilities, and network-centric processing technologies that use autonomy, AI and ML seamlessly integrate networked sensors, target acquisition assets, effects assets, and warfighters to enable delivery of responsive and decisive effects on targets at all echelons.

*Enhanced Cyber Situational Understanding through Advances in Big Data Analytic*s

Another competitive advantage gained in cyberspace leverages advances in big data analytics to enhance cyber situational understanding by permitting the depiction, perception, and understanding of relevant cyberspace impacts that help enable the delivery of effects by tactical maneuver commanders in support of MDO. Many of these advances in big data analytics focus on ingesting, fusing, synthesizing, analyzing, and visualizing big data from varied cyber data sources that present significant volume, velocity, variety, veracity, and visualization issues.[19] Sample cyber data sources include host-based alerts, intrusion alerts, signature updates, vulnerability scans, network traffic (network flow, system logs, packet capture), network device status, security logs, powershell logs, and many more. Most of these advances in big data analytics stem from the research, development, and integration of breakthrough technologies in autonomy, AI and ML that use novel algorithms, methods, architectures, and computing mechanisms to ingest and tag massive data sets at the speed of cyber, to collect data with seemingly unbounded storage capacity with easy query and retrieval, to bring analytic tools to analysts at the tactical edge, and to rapidly generate visualizations that display key cyber terrain for improved decision-making while increasing operational efficiency.[20]

One advancement in big data analytics leverages a ML technology known as deep learning (DL), which is a subfield of ML that uses neural network algorithms with a sophisticated, multi-layer computational architecture to learn hierarchical representations of data. In a network intrusion detection system setting, for example, traditional ML techniques require the extraction of features from raw network traffic; typically, cyberspace subject matter experts analyze the network traffic and extract optimum features that are then used to train ML models useful to detect cyber-attacks. This approach, however, is resource-intensive, not scalable or generalizable across varied cyber data sources, and can result in information loss during data pre-processing.[21] Research scientists from the Army Cyber Institute (ACI) at West Point and the U.S. Army DEVCOM Army Research Laboratory (ARL) recently developed and applied a novel DL algorithm leveraging a one-dimensional convolutional neural network (1D-CNN) architecture that achieves an accuracy of 99% for network intrusion detection using only the bytes of the raw network traffic (i.e., packet capture data).[22] Follow-up research and development from the ACI/ARL team led to another advance in big data analytics known as transfer learning, which seeks to create DL models for a target domain that are pre-trained on some source domain (i.e., take information from one task and use it advantageously to learn a related task), to create and distribute the DL technology to tactical edge, computationally constrained environments.[23] They were able to conduct transfer learning successfully by transferring all

main layers of the pre-trained 1D-CNN model combined with an edge retrained random forest ML model to obtain over 96% accuracy on the tactical network intrusion detection task with only 5,000 training samples on an AI-enabled edge device with an edge training time of only 67 seconds.[24] The ability to use such breakthrough DL technology to accurately and efficiently detect indicators of compromise at the tactical edge enables enhanced cyber situational understanding via integration of command post, cyberspace big data analytic tools that allow maneuver commanders and cyber defenders to depict and understand cyber terrain, make informed decisions, and remain effective and agile in MDO.

These advances in big data analytics that leverage breakthrough technologies in autonomy, AI and ML can be uniquely integrated across the Cyber Mission Force to immediately enhance cyber situational understanding and help gain competitive advantage in cyberspace. For instance, the U.S. Army's Program Executive Officer for Enterprise Information Systems (PEO EIS) has the Cyber Analytics and Detection (CAD) modernization program within its Project Manager for Defensive Cyber Operations (PM DCO) that aims to provide a "cyberspace analytics capability that offers interfaces and visualizations accessible by cyberspace defenders at all levels to facilitate counter-reconnaissance activities aimed at discovering the presence of advanced or sophisticated cyber threats and vulnerabilities."[25] The CAD program manages the Army's Big Data Platform (BDP), which is a data operating system used as the foundation for the cyber data fabric at Army Cyber Command (ARCYBER). ARCYBER's cloud-enhanced BDP, known as Gabriel Nimbus, is used at enterprise and strategic level operations, but they also have lighter versions of the BDP that are used at operational and tactical levels. Thus, the BDP's open-system architecture can easily integrate these advances in big data analytics to enhance cyber situational understanding[26] at the enterprise, strategic, operational, and tactical levels. Moreover, the U.S. Army's Program Executive Officer for Command Control Communications-Tactical (PEO C3T) has the Cyber Situational Understanding (Cyber SU) modernization program within its Project Manager for Mission Command Cyber (PM MC Cyber) that ingests data from PM DCO and other Army program offices to "enable visualization, analysis, and understanding of cyber and electromagnetic activities"[27] at the tactical edge. The Cyber SU product allows for integration of breakthrough technologies in autonomy, AI and ML that create advances in big data analytics to facilitate "informed planning, timely decision making, and mission accomplishment in the cyber-contested operating environment."[28] This enhanced cyber situational understanding allows direct gains in cyberspace competitive advantage such as network awareness (asset identification, vulnerability and incident management, etc.), threat awareness (adversary dispositions/actions, insider threat, etc.), and mission awareness (operational assessment, cyberspace mission impacts, etc.). Further, an AI-enhanced cyber situational understanding capability provides the ability to identify and display risk to system and equipment dependencies that have direct impact on combat missions when faced with a threat. Hence, these technologies are the pivot around which big data will be turned into actionable insight and knowledge and, ultimately, a decisive, warfighting information advantage needed to gain and maintain decision dominance.

Optimized Human-Machine Decision-Making via Autonomous Active Cyber Defense

A final competitive advantage gained in cyberspace is that these technologies can help realize autonomous active cyber defense that augments cyber defenders in their threat assessment and interpretation of vast amounts of cyber data to produce actionable information and recommendations to decision-makers to effectively execute C2 and inform optimal resource allocation decisions in terms of prioritization of incident response. Breakthrough technologies in autonomy, AI, and ML have the ability and capacity to make independent decisions and act upon these decisions rapidly, while at the same time, can work as part of a cyberspace operations team that includes humans.[29] Many of these technologies can collaborate with humans who will retain control and final decision-making authority while enhancing mission awareness of the cyber terrain and reducing the risk to personnel during operations. Thus, the integration of these technologies has the potential to impact the speed of the decision cycle decisively. Given that autonomous active cyber defense capabilities can detect, evaluate, and respond before a human operator alone can understand and react,[30] they should be used to optimize human-machine decision-making for the "collection of synchronized, real-time capabilities to discover, define, analyze, and mitigate cybers threats and vulnerabilities."[31] This includes technologies that learn and manage network topologies,[32] identify and manage trusted users, detect network anomalies, identify threats, and undertake mitigation and response action.[33]

As an example, the Joint Force Headquarters-Department of Defense Information Network (JFHQ-DODIN) has the mission to secure, operate, and defend the DODIN by integrating intelligence information, network operations, security actions, defensive cyberspace actions, and assessment and inspection results for informed decision-making.[34] The integration of breakthrough technologies in autonomy, AI, and ML can help optimize human-machine decision-making for threat-informed operational prioritization that allows JFHQ-DODIN leadership to optimally assess, track, report and align readiness of cyber terrain with assigned forces and prioritized essential tasks. Researchers from the University of South Florida in collaboration with the ACI recently developed a novel AI technology, known as Deep VULMAN, for optimizing the dynamic cyber vulnerability management process.[35] This technology can be directly leveraged by JFHQ-DODIN via its Network Operations Centers, Cyber Security Service Providers, Cyber Protection Teams, etc. for threat-informed resource allocation decision-making. Typically, these cyber defenders scan the network with a vulnerability scanner to find vulnerabilities reported in the National Vulnerability Database, and the generated vulnerability report contains the vulnerabilities found in the network along with attributes such as a common vulnerability exposure (CVE) code, host name, description, common vulnerability scoring system severity (CVSS) rating, and more. These forces then must assign resources to mitigate the vulnerability instances by taking actions such as applying patches, disabling services, etc. The Deep VULMAN AI-based technology overcomes limitations in current approaches to vulnerability management using advanced techniques for sequential decision-making under uncertainty, including deep reinforcement learning and integer programming, to autonomously

recommend optimal, robust vulnerability triage and mitigation plans/policies.[36] This example of optimized human-machine decision-making via autonomous active cyber defense for dynamic cyber vulnerability management directly leads to gains in cyberspace competitive advantage in that the number of JFHQ-DODIN resources to be allocated over time is optimized and important vulnerabilities are identified and prioritized for mitigation, given the optimized allocation of resources. As such, these technologies uniquely provide the ability for cyber defenders to ensure mission continuity and success.[37]

Additional competitive advantages in cyberspace can be gained through improved interaction between human cyber operators and their tools. Breakthrough technologies in autonomy, AI, and ML can be integrated to improve cyber operators' ability to meet the increasing size, speed, and complexity of the cyber battlefield. Specifically, the Cyber Mission Force lacks validated, scalable capabilities to document and model cyber workflows and infer operator intent in real time; these capabilities are necessary to augment workflows effectively. Traditional methods to model workflow manually and elicit expert operator knowledge are often time/labor intensive, and they produce static workflow models of current practices and tactics, techniques, and procedures (TTPs); these can become obsolete as cyber-attacks and tools are constantly evolving. Automated techniques that integrate these breakthrough technologies can learn and log new workflows, which can then be incorporated on an ongoing basis into an adaptive decision support system for autonomous active cyber defense to keep pace in this domain. Without such methods, shallow and stale models of cyberspace operations impair operational, training, and technology development and acquisition decisions. Enormous opportunities exist to rapidly advance human-AI capabilities by adopting and automating digital methods and cyber analytics that can leverage high-granularity, human-computer interaction (HCI) data to augment the cognitive capabilities of cyber operators. To advance the state of the art and enable cyberspace decision-support capabilities, these breakthrough technologies can be integrated to capture cyber operator performance and workflows in complex information environments. Moreover, a cybernetic control signal (i.e., a virtuous feedback loop between human and machine) that leverages these HCI data streams along with integrated autonomy, AI, and ML technologies to improve the definition, resolution, and performance of the conjoined cyber operator system can be implemented for optimized human-machine decision-making. Cyberspace competitive advantages can be gained using these technologies to automate and accelerate aspects of knowledge elicitation and mature digital recording into an assistive automation capability to provide decision support to cyber operators with expert TTPs that is responsive to current workflows and situation. This broadly mitigates risks associated with the adoption of complex and unproven technologies.

CONCLUSIONS AND RECOMMENDATIONS

As highlighted above, the effective integration of breakthrough technologies in autonomy, AI, and ML into cyberspace support to operations in the IE gain competitive advantages across the cyberspace layers and respective IE dimensions. This allows actions to be taken by the commander to generate, preserve, and apply informational power toward a relevant actor while permitting maneuver through the IE.

Given that ongoing research and development in new breakthrough technologies is leading to major advancements at an exponential pace, how can the operational, science and technology, and acquisition and sustainment cyberspace communities actively identify and exploit the next technological innovations that come our way? This is where strategic, active partnerships among industry, academia, and government organizations must be established, maintained, and leveraged through a mission-focused, robust ecosystem of diverse cyberspace technology innovators focused on technology development, assessment and deployment. Industry organizations, including startups, large system integrators, global companies and more, represent a vital part of the ecosystem with now direct links to military organizations in which emerging requirements can be directly communicated so that new breakthrough technologies in autonomy, AI, and ML can be rapidly integrated and deployed more quickly. Academic organizations, including universities, research institutions, federally funded research and development centers (FFRDCs) and university-affiliated research centers (UARCs) within the ecosystem can learn about emerging cyberspace technology needs and challenges, enabling them to scale research efforts and build novel technology solutions through direct access to military-relevant use cases and problem sets. Finally, government entities within the ecosystem can establish airtight collaborations with these world-class innovative partners from industry and academia to remain knowledgeable about the latest innovations to exploit.

Although the character of warfare in cyberspace is rapidly transforming due to continued technological advances, the persistent and sustained identification, exploitation, and integration of new breakthrough technologies in autonomy, AI, and ML will continue to ensure competitive advantage gains in cyberspace across the Joint Force leading to success in conducting MDO.

NOTES

1. Joint Publication 3-12, U.S. Department of Defense, *Cyberspace Operations* (Washington, DC: United States Department of Defense, 2018), I-2.
2. Ibid., I-7.
3. Joint Publication 3-13.1, U.S. Department of Defense, *Information Operations* (Washington, DC: United States Department of Defense, 2012, incorporating change 1, 2014), I-1.
4. Joint Publication 3-12, U.S. Department of Defense, I-3.
5. Joint Publication 3-13.1, U.S. Department of Defense, I-2.
6. Alexander Kott, *Intelligent Autonomous Agents are Key to Cyber Defense of the Future Army Networks* (West Point, NY: *The Cyber Defense Review*, vol. 3, issue 3, 2018,57-70), 58.
7. Nathaniel Bastian, *Building the Army's Artificial Intelligence Workforce* (West Point, NY: The Cyber Defense Review, vol. 5, issue 2, 2020, 59-63), 59.
8. Fernando Maymí and Scott Lathrop, *AI in Cyberspace: Beyond the Hype (*West Point, NY: *The Cyber Defense Review*, vol. 3, issue 3, 2018, 71-81), 77.
9. TRADOC Pamphlet 525-8-6, Department of the Army, *The U.S. Army Concept for Cyberspace and Electronic Warfare Operations 2025-2040* (Fort Eustis, VA: U.S. Army Training and Doctrine Command, 2018), 19.
10. Alexander Kott, 63.
11. Joint Publication 3-12, U.S. Department of Defense, I-5.
12. Nathan Strout, "What the Army's TITAN Program Means to Multidomain Operations," *C4ISRNET,* June 9, 2020, https://www.c4isrnet.com/battlefield-tech/it-networks/2020/06/09/what-the-armys-titan-program-means-to-multi-domain-operations/.
13. Nathan Strout, "Inside the Army's Futuristic Test of its Battlefield Artificial Intelligence in the Desert," *C4ISRNET*, September 25, 2020, https://www.c4isrnet.com/artificial-intelligence/2020/09/25/the-army-just-conducted-a-massive-test-of-its-battlefield-artificial-intelligence-in-the-desert/.
14. Nathan Strout, "Army's TITAN Program."
15. George Seffers, "Soldiers and Commanders to Assess FIRESTORM AI Technology," *SIGNAL*, June 8, 2021, https://www.afcea.org/content/soldiers-and-commanders-assess-firestorm-ai-technology.
16. Ibid.
17. Nathan Strout, "Assess FIRESTORM AI Technology."
18. Marc Chalé and Nathaniel Bastian, "Generating Realistic Cyber Data for Training and Evaluating Machine Learning Classifiers for Network Intrusion Detection Systems" (*Expert Systems with Applications,* vol. 207, issue 117936, 2022, 1-18), 1.
19. Tariq Mahmood and Uzma Afzal, *Security Analytics: Big Data Analytics for Cybersecurity – A Review of Trends, Techniques and Tools* (2013 IEEE 2nd National Conference on Information Assurance, 2013, 129-134), 130-131.
20. Rudy Guyonneau and Arnaud Le Dez, "Artificial Intelligence in Digital Warfare: Introducing the Concept of the Cyber-teammate" (West Point, NY: *The Cyber Defense Review,* vol. 4, issue 2, 2019, 103-115), 105-106.
21. Michael De Lucia, Paul Maxwell, Nathaniel Bastian, Ananthram Swami, Brian Jalaian, and Nandi Leslie, *Machine Learning for Raw Network Traffic Detection* (2021 SPIE AI and ML for MDO Applications III, vol. 11746, issue 117460V, 2021, 1-11), 1.
22. Ibid.
23. David Bierbrauer, Michael De Lucia, Krishna Reddy, Paul Maxwell, and Nathaniel Bastian, "Transfer Learning for Raw Network Traffic Detection" (*Expert Systems with Applications*, 1-10, Under Review), 3.
24. Ibid., 7-9.
25. PEO Enterprise Information Systems, "Cyber Analytics and Detection," https://www.eis.army.mil/programs/cad.
26. TRADOC Pamphlet 525-8-6, Department of the Army, 24.
27. PEO Command Control Communications-Tactical, "Mission Command Cyber," https://peoc3t.army.mil/mc/mcc.php.
28. Ibid.
29. Rudy Guyonneau and Arnaud Le Dez, 108-109.
30. Alexander Kott, 61-62.
31. TRADOC Pamphlet 525-8-6, Department of the Army, 25.

NOTES

32. Ibid.
33. Rudy Guyonneau and Arnaud Le Dez, 111.
34. Defense Information Systems Agency, "Director," https://www.disa.mil/about/our-leaders/director.
35. Soumyadeep Hore, Ankit Shah, and Nathaniel Bastian, *An Artificial Intelligence-Enabled Framework for Optimizing the Dynamic Cyber Vulnerability Management Process* (39th International Conference on Machine Learning, PMLR 162, 2022, 1-21), 1.
36. Ibid., 2.
37. TRADOC Pamphlet 525-8-6, Department of the Army, 25.

Conventional Retaliation and Cyber Attacks

Sarah Chen
Dr. Jennifer Taw

INTRODUCTION

On July 27, 2021, President Joe Biden warned, in a speech at the Office of Director of National Intelligence, that "I think it's more than likely we're going to end up, if we end up in a war - a real shooting war with a major power - it's going to be as a consequence of a cyber breach of great consequence and it's increasing exponentially, the capabilities."[1]

Most analysts view the president's hypothetical scenario as unlikely for two reasons. First, attributing cyberattacks is often challenging, making retaliation difficult, if not impossible. Cyberattacks are commonly anonymous, hard to trace, and may be triggered long after they were set up. Moreover, they are often carried out not by states but by criminal entities, hacker groups, or other non-state actors, which sometimes but not always are affiliated with or sponsored by states. The practical and political window for overt retaliation closes if a cyberattack cannot be directly and timely attributed to a state. Second, and importantly, most cyberattacks do not have strategic effects. The preponderance of cyberattacks are either distributed denial-of-service (DDOS) attacks (meant to disrupt, blackmail, or extort), or they are efforts to collect information through a combination of hacking and malware. Even attacks attributable to a state usually fall below the threshold for conventional retaliation.

Yet we explain here why improvements in attribution capabilities, combined with cyberattacks' increasing potential to kill people, threaten military readiness, and wreak economic destruction are making it more likely that a cyberattack will trigger a conventional response. This is significant because, as foreseen by President Biden, it means that a cyberattack could be not only an element of war but a precipitating act of war.

Sarah Chen is a Rhodes Scholar pursuing a MSc in Social Science of the Internet at Oxford. She recently graduated from Claremont McKenna College with a dual degree in International Relations and Philosophy, Politics, and Economics. Her academic interest area is in cyberspace conflict and wargaming. During her undergraduate years, she worked on games with the Center for Naval Analyses, the Gould Center for Humanistic Studies, and the Office of the Director of National Intelligence.

This article summarizes how some states already anticipate this possibility, and reviews the conventional wisdom on the relationship among cyberattacks, retaliation, and escalation, with special attention to attribution. We then show accurate attribution is easier now, and that cyberattacks with strategic impact are somewhat more likely. We conclude with recommendations for considering this new level of cyber conflict.

STATES ANTICIPATE STRATEGIC CYBERATTACKS

Article 51 of the UN Charter allows the use of force "only in response to a certain kind of attacking force, specifically, an 'armed attack.'"[2] With respect to this, however, legal experts rely on effects-based analysis more than a definition-based one, looking at the "violent consequences of an attack which does not consist of the use of kinetic force" to determine whether it is equivalent to an armed attack.[3] A cyberattack that causes deaths or significant strategic outcomes - that, in effect, has an outcome equivalent to a conventional armed attack - arguably meets this standard.

The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, published in 2017, is intended to assist in applying international law when interpreting cyber actions and developing appropriate responses. The manual, relied on by multiple individual states' doctrines on cyberspace, states that use of force, while generally forbidden, can be appropriate and justified in self-defense, depending on the context. The manual offers a framework for judging a cyberattack that includes the following criteria: severity, immediacy, directness, invasiveness, measurability of effects, military character, state involvement, presumptive legality.[4]

Many states have begun to identify circumstances appropriate for response to a cyberattack with non-cyber retaliation. Since 2011, US leaders, for example, have reserved the right to respond to hostile acts in cyberspace with "all necessary means – diplomatic, informational, military, and economic" although the US will

Jennifer Morrison Taw is Associate Professor of Government and International Relations at Claremont McKenna College, where she teaches International Relations, Security Studies, War, and U.S. Foreign Policy. Her publications include Mission Revolution: The U.S. Military and Stability Operations (Columbia University Press, 2012); "Preventive Force: The Logic of Costs and Benefits," Chapter 2 in Fisk, et. al, Preventive Force: Drones, Targeted Killing, and the Transformation of Contemporary Warfare (New York University Press, 2016); and "Colombia: A Case Study," chapter in Fair, et. al, Policing Insurgencies: Cops as Counterinsurgents (Oxford University Press, 2014). Taw is also coauthor of World Politics in a New Era, 6th edition, with Spiegel, et al., (Oxford University Press, 2014). Prior to teaching, Jennifer worked for ten years at RAND, where she focused on counterinsurgency, counterterrorism, peace operations, and special operations forces.

"exhaust all options before military force whenever [it] can."[5] In a 2015 hearing, then-Deputy Secretary of Defense Robert Work stated that the US "reserves the right to respond to malicious cyber activity at a time, place, and manner of its choosing."[6]

In the German federal government's March 2021 position paper, "On the Application of International Law in Cyberspace," officials note the potential of cyberattacks with kinetic outcomes severe enough to trigger responses under international law. Cyber operations could "constitute an armed attack whenever they are comparable to a traditional kinetic armed attack in scale and effect."[7] German government officials lay out four response possibilities: retorsion, countermeasures, measures taken based on necessity, and self-defense. With self-defense, states can "resort to all necessary and proportionate means in order to end the attack" when a cyberattack is comparable to an armed attack. They also state that "there is no general obligation under international law as it currently stands to publicize a decision on attribution and to provide or to submit for public scrutiny detailed evidence on which an attribution is based."[8] That is not to say that accusations should not be substantiated, however, the German report concludes that the state should have discretion whether to publicize attribution.[9]

The French government, in its cyber operations declaration, reserves the right to respond to cyberattacks and provides criteria for assessing whether or not a cyber operation is comparable to an armed attack: substantial loss of life, physical or economic damage, impact on critical infrastructure, number of victims, technological or ecological catastrophe.[10] The French add that, even if one cyberattack falls short of reaching a certain threshold of damage, multiple attacks and their effects can be aggregated (for instance, if an attack cripples electronic infrastructure in one area of the country and a different attack, sponsored by an actor working in conjunction with the first, damages water supply access in another

area jointly impacting a large number of citizens). Self-defense from such attack(s) can include conventional force and can also be preemptive. Like Germany, France prefers that each state decide if and when to share public attribution, and also what evidence is needed to support an accusation, and underscores that absence of public attribution is not necessary to justify a state's response to a cyberattack.[11]

While it has similar self-defense guidelines, the Netherlands categorizes attribution as technical, political, or legal, wherein states need only to disclose evidence for legal issues when an attacking state violates international law.[12] Dutch policy also holds that, if self-defense is required, there must be adequate and convincing proof of the actor's guilt and states must still meet requirements of necessity and proportionality: "the intention is to end the attack, the measures do not exceed that objective and there are no viable alternatives. The proportionality requirement rules out measures that harbor the risk of escalation and that are not strictly necessary to end the attack or prevent attacks in the near future."[13]

NATO Secretary-General Jens Stoltenberg wrote in 2019 that "a serious cyberattack could trigger Article 5 of our founding treaty" that triggers the collective defense agreement, placing cyberattacks in the same domain as any physical attack.[14] Stoltenberg cited the 2017 WannaCry virus's effect in the United Kingdom as an example of a major cyberattack: ransomware that shut down multiple hospitals and cost over £90 million.[15] Article 5 specifies that if an "armed attack" occurs against a NATO ally, then each member will assist the ally with "such actions as it deems necessary, including the use of armed force."[16] While Article 5 has yet to be triggered by a cyberattack, and while there is no consensus on the definition of the term 'armed' cyberattack, a kinetic response to a cyberattack—backed by a multilateral alliance—seems clearly possible. Eneken Tikk, a research lawyer at the Cyber Policy Institute, observes, however, that Article 5 poses a high threshold, for example, attacking critical infrastructure with effect comparable to an armed attack; below this threshold, he observes that even an attack resulting in casualties may not qualify.[17]

In 2010, anticipating this debate in NATO, Mark Rasch, former head of the U.S. Justice Department's computer crimes unit, suggested that Article 5's chief purpose is "to act as a massive deterrent...by establishing the rules of cyber war engagement, NATO is 'throwing down the gauntlet'."[18] Yet NATO eleven years later openly affirmed that cyberattacks could trigger Article 5, reiterating this in the response to the Russia-Ukraine conflict, and further declared that "the Alliance is determined to employ the full range of capabilities at all times to actively deter, defend against, and counter the full spectrum of cyber threats, including those conducted as part of hybrid campaigns, in accordance with international law."[19] NATO made the case that "ransomware incidents and other malicious cyber activity targeting our critical infrastructure and democratic institutions... might have systemic effects and cause significant harm."[20]

This brief review of NATO's and NATO members' anticipation of strategic cyberattacks demonstrates the seriousness with which many major military powers are planning for such

eventualities, and considering circumstances that would justify conventional responses. Notably, such policies and deliberations serve not only to prepare and plan for strategic cyberattacks, but also to deter against them by forewarning a conventional response to certain types of attacks, based on the targeted victim, and the level of impact.

LITERATURE REVIEW

In 2012, Thomas Rid published his article "Cyber War Will Not Take Place,"[21] and defined an act of war as being instrumental and political, with the potential to be lethal. He argued that, given that most cyberattacks were primarily acts of sabotage, espionage, or subversion, they were "tactical in nature" and only rarely might "have operational or even strategic effects."[22] Rid further observed that not a single cyberattack had met all three criteria.[23] A year later, John Stone responded with his own article, "Cyber War Will Take Place!" Stone wrote that "cyber war is possible in the sense that cyberattacks could constitute acts of war." Stone recognized, long before the crippling effects of large-scale attacks like NotPetya, that the application of force for an act of war "can break things, rather than kill people, and still fall under the rubric of war."[24]

More in keeping with Rid than with Stone, Martin Libicki in 2020 wrote "Correlations Between Cyberspace Attacks and Kinetic Attacks," in which he drew several conclusions: "a kinetic retaliation to a cyberattack is possible but cannot yet be deemed a likely consequence" and "rarely do events in cyberspace – much less escalation in cyberspace – lead to serious responses at all."[25] He continued, "while there could be cyberattacks consequential enough to induce echoes in the physical world, none have reached that threshold and it may well be that none could reach that threshold."[26]

In both theory and practice, the most common response to a cyberattack is also cyber, whether as defense or retaliation. Interestingly, even in this context, the expectation is that a cyberattack will be met with an equivalent response, rather than escalation. There are practical reasons for this, but it is also related to policymakers' and the public's perceptions. Jacqueline Schneider analyzed the Deterrence and Escalation Game in Review (annually conducted (2011-2016) with US foreign policy decision makers), concluding that decision makers "curtail their own use of cyber operations for fear of escalation, while not responding to similar adversary actions in cyberspace."[27] Similarly, Benjamin Jensen and Brandon Valeriano in 2017 looked at whether or not cyber operations resulted in a desire for an escalatory response.[28] US, Russian, and Israeli participants in a simulation and survey experiment were assigned to four groups and presented with a triggering incident (half had a cyber-based incident and half did not) and given the ability to respond (half were given the option of a cyber response and half were not). Jensen and Valeriano found that all three nationalities "preferred de-escalation more than escalation even when they had cyber options with which to respond. Escalation was not the norm."[29] Respondents across all four scenarios opted 40-50% for de-escalation, 30-50% for a proportional response, and less than 10% of advocated escalation.[30]

When retaliation to a cyberattack is going to occur, however, Aaron Brantly lists certain requirements for success: the state must identify the perpetrator, retaliate in a timely and proportionate manner, and employ a cyberweapon tailored for the specific target.[31] Timeliness is important because perpetrators expecting a delayed response may assume that "the risk of punishment for an attack is ... so temporally distant as to be discounted to the point of irrelevance."[32] Avoiding escalation renders proportionality critically important. Specificity and prompt response prevent "bleed" or "escape" by preventing a cyberweapon like malware or a virus from hopping to unintended servers or sectors.

This logic presumes that assured proportionate response will deter cyberattacks. Whether this is true is complicated by the aforementioned challenges of attribution. Unlike kinetic weapons and military movements, which are physical and often overt actions, cyberattacks are invisible and can remain undetected, and their effects may be attributed to other causes. When they *are* recognized as cyberattacks, it may be hard to trace their perpetrators or even to identify their scope. As Charles Glaser notes, cyberattacks are inherently covert,[33] requiring secrecy to increase success, reliant on finding vulnerabilities and 'zero-day' exploits.

These characteristics often muddle attribution. For instance, an attack could originate from servers in a state without that state's awareness; a non-state organization might utilize the servers or another actor could route through them.[34] In "Crisis and Escalation in Cyberspace," Martin Libicki describes how a state can plausibly deny responsibility for a cyberattack traced to its territory, claiming it was a non-state actor or a false-flag operation.[35] Without surety, a state victim of a cyberattack cannot retaliate, rendering perpetrators non-deterrable, thinking they can cover their tracks. Former U.S. Deputy Secretary of Defense Bill Lynn noted that traditional deterrence models are less effective in cyberspace due to the difficulty in identifying attackers; he holds deterrence must instead "be based more on denying any benefit to attackers than on imposing costs through retaliation."[36]

In "Cyber Deterrence," Jonathan Welburn, Justin Grana, and Karen Schwindt suggest, to the contrary, that deterrence can be effective if the defender signals – without specificity – that it has the cyber capacity to defend/retaliate against a cyberattack. In their model, Welburn et.al assume that: "1. The defender can only imperfectly attribute attacks. 2. The attacker has uncertainty over the defender's retaliatory and defensive capability. 3. The defender can signal its capability not by revealing its true capability, but through costless and unverifiable cheap talk."[37] The authors map out this model utilizing game theory and show that "it is never in the best interest of the defender to perfectly signal its retaliation capability."[38] However, if it can convince the attacker that it is signaling a strong, true capability without revealing its actual hand, this increases deterrence. Welburn et. al. also propose a model of "anti-deterrence," incentivizing an attacker to attack when the defending state has heightened readiness and in such a way that the attacker tips its hand, increasing the likelihood of correct attribution.[39] Their conceptualization of deterrence in a cyber context highlights the differences from classic

deterrence: in the cyber realm, they suggest, states must coopt uncertainty, signaling indirectly, vaguely, and without technical proof.

Considering the foregoing, it might seem unlikely that a cyberattack could be expected to trigger a conventional response. But some of the conditions have changed since these analyses were conducted. As will be discussed, attribution technology and capabilities are improving, thus facilitating retaliation and, of course, deterrence, by obviating the comfort perpetrators may have that they will not be identified. Secondly, while the preponderance of cyberattacks remains tactical, the potential for strategic cyberattacks is increasing and it is, therefore, worthwhile to consider when a cyberattack could become a precipitating cause of war.

Stone and Rid classify a cyberattack as an act of war if it corresponds to a strategic economic attack, a strategic military attack, or a lethal civilian attack, thus potentially justifying a conventional response. While in their 2018 article "Determinants of the Cyber Ladder," Nadiya Kostyuk, Scott Powell, and Matt Skach saw cyber capabilities as unready to deal an existential blow to a major power,[40] they offered a useful escalation ladder for conceiving of the requirements of doing so. In their model, an act of war would involve a "major damaging attack – targeted military interference and overt disabling and/or destruction of military targets or infrastructure; catastrophic attacks – permanent damage to civilian infrastructure (mass destruction of critical data, infrastructure control, software, banking infrastructure); and existential attacks" equivalent to "limited contingency operations, major military operations, and nuclear war."[41] The range of attacks that could spark a conventional response short of war will likely be broader.

In short, the literature suggests that a conventional response to a cyberattack will only occur if the attribution challenge is resolved and if the cyberattack deals a strategic blow leading to severe military or economic damage or to civilian deaths (above a certain threshold, if Tikk is correct) – while casting some doubt that a nation would choose to escalate to that threshold.

ATTRIBUTION AND IMPACT

Attribution

Attribution techniques are becoming more accurate and rapid. Attribution occurs on multiple levels of granularity: assigning attacks to a group, country of origin, and identification of specific groups or people. The second level is the country of origin – the level required for state-level retaliation, and "the most common level of attribution"; about 85% of the 130 identified groups in public analysis reports are linked with a country.[43] Timo Steffens in "Attribution of Advanced Persistent Threats," breaks down the initial phases of the attribution processes: data collection and clustering, which both have seen technical improvements in recent years.[44] Resources like the Common Vulnerability Exposure dictionary and the YARA pattern-matching malware tool are widely used to create a common ground for compiling and sharing information on previous attacks.[45]

Artificial intelligence (AI) tools and machine learning are also advancing attribution. AI can analyze massive amounts of attack data to find patterns and similarities for actor identification.[46] The Department of Defense sponsored Rhamnousia, an algorithmic methodology that attempts to change manual attribution, which can takes weeks and months, into machine learning programs.[47] A cyber threat attribution framework can use a machine learning model, trained off publicly available cyber threat intelligence reports, to recognize attack patterns with about 50% higher precision than other publicly available profiles.[48] Another such model, developed on the Amazon Web Services Honeypot dataset, exceeded 95% accuracy.[49]

Public-private sector sharing and cooperation regarding information on vulnerabilities and actors has improved, both through formal and informal mechanisms. State-level attribution can be initiated by private security firms first identifying and investigating the issue, creating a collective knowledge base, and then building into a private-public effort for attribution.[50] The US introduced the Cyber Threat Framework to create a consistent common language for cyber threat activity sharing, across models and observations.[51] The Cybersecurity and Infrastructure Security Agency (CISA) also has networks for information sharing, and a recent bill, the Cyber Incident Reporting for Critical Infrastructure Act signed in March 2022, creates obligations for private sector reporting.[52]

Many cyberattacks in the three years ending in 2020 were publicly attributed, with improvements to digital forensics.[53] In an analysis of the Council on Foreign Relations (CFR) dataset of state-sponsored cyber incidents from 2014-2018, Mueller, et al., found that out of eighty-two incidents, 85% were publicly attributed to a government, private actor, or both.[54] CFR reported seventy-six operations in 2019 that were confirmed or suspected to have been state-sponsored, 77% of which were attributed to China, Russia, Iran, or North Korea,[55] and one hundred nineteen such incidents in 2020.[56] Some of the largest hacks that occurred within the last year: Solarwinds – malicious code that affected US government infrastructure,[57] Colonial Pipeline – a ransomware-triggered shutdown of a large oil pipeline,[58] JBS – ransomware attack against a global meat processing company,[59] and Kaseya – another ransomware attack that affected hundreds of supply chains,[60] were all state-sponsored or attributed by link within weeks or months of discovery. The US was also able to quickly attribute cyberattacks against Ukraine to Russia, showcasing an improved attribution arsenal.[61]

The Dyadic Cyber Incident and Campaign Database (DCID), which publishes known cyber incidents between rival dyads from 2000-2020, tracked 429 incidents that have steadily increased in severity of impact and volume annually, which suggests more attacks or improved attribution, or both, for cyber incidents.[62] The average severity has risen from most attacks being classified as a level three in impact, "stealing targeted critical information from one network" to level four, "widespread government, economic, military, or critical private-sector network intrusion, multiple networks."[63] In short, in the past few years, most of the large-scale cyberattacks that approach the conditions for triggering a conventional response have been

directly attributed to specific hacker groups and, in some instances, to states or state sponsors, which suggests some combination of better attribution methods and greater public-private cooperation for attack response and analysis, and faster attribution to adversarial cyber nation-states.

Impact

Civilian Deaths

In 2020, the first reported 'direct' cyberattack death occurred: misdirected ransomware targeting Heinrich Heine University hit a hospital in Düsseldorf, Germany instead, resulting in a patient dying before reaching an alternative hospital. The attacker withdrew its extortion demand and sent a decryption key upon discovering the error, to no avail.[64] This death was accidental, but confirms that cyberattacks can kill. More recently deaths have resulted from cyberattacks on power grids in Ukraine, and crippled hospital infrastructure in the United Kingdom (UK) and the US, but none of these events led to an escalatory response from the targeted countries.[65] So far at least, it appears a deadly cyberattack will not lead to a conventional response unless it was deliberately undertaken by a state or non-state violent actor and kills a certain threshold number.

The link between retaliation and deaths relates in part to public perception and political expectations. Sarah Kreps and Debak Das found in 2017 that US public support for a retaliatory air-strike increased by about 32% when a cyberattack causes casualties beyond economic injury.[66] A 2021 multi-country study by Ryan Schandler, Michael Gross, Sophia Backhaus, and Daphna Canetti likewise found that only lethal terrorist cyberattacks led to public expectations of military retaliation. By running randomized survey experiments with UK, US, and Israel civilians, Schandler, et al, identified a "lethality threshold for cyber terrorism effects, wherein the outcome of the attack must meet a minimum level of destruction in order to produce national responses equivalent to those for conventional terrorism."[67] The researchers found that, considering lethal and non-lethal conventional terrorist attacks and lethal and non-lethal cyberterrorist attacks, conventional attacks and cyberattacks with fatalities were more likely to engender demands for retaliation. Building on Kreps' and Schneiders' 2019 work, in which the researchers found that "individuals are far more reluctant to escalate in the cyber domain than for corresponding conventional or nuclear attacks," Shandler, et al, concluded from their own experiment that the public would expect retaliation for attacks causing at least seven deaths.[68]

Destruction of Military Capabilities

Cyberattacks can trigger kinetic effects that reduce the military's capabilities. In 2007, Idaho National Laboratory researchers found that from a remote location, with just thirty lines of code, they could blow a diesel generator attached to an electrical grid.[69] Damage in this instance was machine alone, but overpowering an electrical grid at a military base and causing permanent kinetic damage or even injury to soldiers can be viewed as acts of war.

As important as kinetic outcomes from cyberattacks, and more likely, are cyberattacks' destruction of elements of the military's technical ability. Non-kinetic attacks, such as disablement of weapon systems' command-and-control, drone hacking or corruption of targeting systems, or even damage to satellite and surveillance ability, can seriously undermine military operations. Even without any direct loss of life or kinetic damage, they can directly interfere with a nation's ability to defend itself or achieve military objectives.

A Microsoft report that tracked the first few weeks of the Russia-Ukraine war, from February 23 to April 8, observed "nearly 40 discrete destructive attacks that permanently destroyed files," with over 40% targeting "critical infrastructure sectors that could have negative second-order effects on the government, military, economy, and people."[70] A stand-out hack was the targeting of Viasat, a US satellite company, which wiped data and destroyed thousands of terminals, effectively crippling Ukraine's military communications, characterized as "the most concerted effort to disable Ukrainian military capabilities."[71]

Yet Russian cyber-attacks on military targets were limited to information compromise, such as Dev-0257 and STRONTIUM – phishing campaigns against government and military employees.[72] The Microsoft report found that there were "several attacks that appeared to show parallel cyber activity and ground activity."[73] For instance, Russia targeted government buildings in Dnipro with strikes on the same day an agency located there suffered a major malware attack.[74] This generally falls within the guidelines of current literature that suggests the destruction of military capabilities for now remains primarily within conventional weapon alternatives and cyberattacks will remain supportive.[75]

Despite the lack of current evidence of cyberattacks directed to disrupt or disable military capabilities, the technical vulnerability to and consequences of such attacks are concerning. The Department of Defense (DoD) "routinely found mission-critical cyber vulnerabilities" in developing systems.[76] Russia jammed GPS signals during the NATO exercise, Trident Juncture, in 2018. These attacks, while temporary, threatened loss of intelligence, surveillance, and reconnaissance functionality if ever later conducted on a larger scale.[77] An attack that interfered with military capabilities could lead to retaliation as a consequence of interference or out of the defending state's worry that it is a precursor for follow-on action, as seen in the Russian preemptive cyberattacks on Ukraine. Although strategic cyber operations cannot "hold ground... gain or reclaim it," when they threaten conventional capabilities to do so, they could spark conventional retaliation.[78]

Economic and Infrastructural Damage

President Biden in his June 16, 2021 meeting with President Putin listed sixteen critical infrastructure sectors that "should be off-limits to attack, period, by cyber or any other means."[79] A senior official noted that these sectors are those that fall under the auspices of CISA: chemical infrastructure, commercial facilities, communications infrastructure, critical manufacturing,

dams, the defense industrial base, emergency services, the energy industry, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors (including both materials, and waste), the transportation sector, and water and wastewater.[80] During the Russia-Ukraine conflict, Biden has stated that "If Russia pursues cyberattacks against our companies, our critical infrastructure, we are prepared to respond."[81] However, he has not stated the consequences of such attacks.

Direct damage that equates to an armed attack could result from cyberattacks on critical infrastructure. Hijacking and crashing vehicles, poisoning water supplies, flooding dams, or cutting off hospital functionality, for example, are acts that would be considered terrorism and hence qualify as acts of war. In 2017, the Department of Homeland Security ran an experiment where a team succeeded in remotely hacking into a Boeing 757.[82] While there have been no such large-scale attacks on critical infrastructure, a July 2021 attack by Russian-linked REvil, a ransomware-as-a-service criminal group, on Kaseya, a Dublin- and US-based company that develops computer software for business-networking, affected 800-1500 businesses' downstream supply chains.[83]

Although the US has not experienced a direct, crippling economic or critical infrastructure attack, the past two years have seen several large incidents globally; civilian infrastructure is not 'off-limits' for cyber conflict. Colonial Pipeline and JBS, while causing international concern, both resulted in a temporary halt in supply-chain operations due to ransomware disablement, rather than destruction.[84] It is unclear whether Colonial Pipeline was operationally affected, given that the company chose to internally shut down operations while investigating the attack, and the JBS shutdown resulted in less than a day's loss of output.[85]

However, other attacks have been more deliberately focused on damaging infrastructure, rather than monetary gain. On April 23, 2020, the Israeli National Cyber Directorate alerted energy and water companies that there were "intrusion attempts at wastewater treatment plants, water pumping stations, and sewers."[86] The attack was linked to the Jerusalem Electronic Army, an affiliate of the Gaza Cybergang, an Arab-speaking group believed to be working from Palestine. Western intelligence sources allege that hackers attempted to alter water chlorine levels, and nearly succeeded.[87] Yigal Unna, head of the National Cyber Directorate, noted that if the attack had not been detected in real time, the consequences could have been "harmful and disastrous" if chemicals were mixed into the water.[88] The hack also could have triggered a fail-safe and shut down water sources during an on-going heat wave.[89]

Iran's Shahid Rajaee port terminal was knocked out on May 9, 2021, causing long line-ups of vessels stuck in and outside the harbor. The computer system was off-line "briefly," but the lasting traffic build-up caused miles-long jams around the port that took days to clear. One official called the situation "total disarray," claiming that Iranian official media understated the damage.[90] Two months later, a cyberattack on Iran's railroad systems and Iran's transport and urbanization ministry website caused delays and cancellations of hundreds

of trains as false information was reported on display boards and the electronic train tracking system failed.[91] On July 22, 2021, Transnet SOC Ltd., a ports and freight-rail company responsible for over 60% of South Africa's shipments, experienced an "act of cyberattack, security intrusion, and sabotage" and declared a force majeure five days later with four harbors disrupted: Durban, Ngqura, Port Elizabeth, and Cape Town. The force majeure lasted for 11 days, with port operations systems, websites, and digital communication down, causing delays and bottlenecks.[92] Port issues ricocheted into importers and exporters of manufactured and agricultural goods, and experts predicted a high economic toll during an already unstable time for South Africa.[93] In April, Ukraine revealed that it had narrowly withstood a planned Russian attempt to shut down its power grid, with a potential blackout threatening two million citizens.[94]

Parallels in the US could have consequences reaching the threshold of cyber terrorism with secondary lethal effects. In a 2022 discussion on "Strengthening the Cybersecurity of American Water Utilities," Samantha Ravich, chair of the Center on Cyber and Technology Innovation, stated that "water may be the greatest vulnerability in our national infrastructure.... [E]ach of these [52,000 drinking water and 16,000 water waste] systems operates in a unique threat environment."[95] A mid-2021 publication confirmed three recent attempted US-based hacks of water facilities.[96] A large port shut-down in the vein of the Shahid Rajaee or Transnet SOC attacks would cost billions; a supply-chain congestion outside the Los Angeles and Long Beach ports left over twenty billion dollars' worth of goods stranded outside the docking area for days.[97] A hypothetical attack on the Northeast US power grid, affecting 15 states, would cost anywhere from 243 billion to a trillion dollars.[98] The Colonial Pipeline attack and the JBS attack cost about five and 11 million dollars, respectively, in ransom costs, with no publicly announced cost of the business disruption.[99] However, the scale of these attacks was limited to a short-term concern given the rapid recovery.

The Center for Strategic and International Studies, an American thinktank, compiles a worldwide rolling list of significant cyber incidents that focuses on "cyberattacks on government agencies, defense and high-tech companies, or economic crimes with losses of more than a million dollars."[100] They list 131 such incidents in 2020, thirteen of which had kinetic effects on critical infrastructure, over 100 in 2021, and 118 as of December 18, 2022.[101]

Without defining the threshold, the Biden administration has publicly floated the possibility of a US military response to cyberattacks, saying "we are not taking anything off the table as we think about possible repercussions, consequences, or retaliation."[102] Likewise, other countries are experiencing emerging thoughts regarding conventional responses to cyberattacks, and there is a growing global realization that cyber and/or political retaliation may not continue to suffice to counter severe cyber incidents.

CONCLUSION

Overall, the fast-evolving relationship between cyber conflict and the threshold for conventional warfare demands more attention. Libicki in 2020 correctly noted that there had not yet been a conventional response to a cyberattack, and that remains true today. But some states are realizing it is not too soon to develop norms, given the recent growth of serious incidents and the targeting of critical and civilian infrastructure. Cyberattacks increasingly are imposing significant costs on countries. Without effective deterrence mechanisms, the frequency and intensity of attacks will continue to grow. Public conservativism regarding responses cannot be expected to hold in the aftermath of a massive attack or significant loss of life. With military and infrastructure vulnerabilities, the boldness of state-sponsored cyberattacks, and more timely investigations, the US must prepare to respond to unprecedented cyber incidents or to aid allies in an invocation of Article 5.

While publicly stating thresholds of cyberattacks may be marginally useful, the NATO Secretary General has correctly observed that NATO never grants adversaries the privilege of knowing specifics on what will trigger Article 5. More consideration needs to be given regarding mutual, multi-lateral understanding of cyber conflict red lines.[103] This paper focuses on conditions that could justify conventional retaliation to cyberattacks, but future work is needed to address specifics regarding targets and responses. There may be different cost thresholds, for instance, for private sector attacks on civilian infrastructure than for state-sponsored infrastructure. A conventional retaliation can also take many forms depending on the target and impact; a retaliation for the degradation of missile launch capabilities may look different from that for civilian deaths from water shutdowns.

If cyberattacks meet the retaliation threshold - resulting in loss of life, degraded military ability, and/or strategic economic damage – and if sanctions and cyber counterattacks are deemed inadequate, a conventional retaliation may be reasonable and even necessary, especially if accurate attribution ceases to be a serious challenge.

NOTES

1. Nandita Bose, "Biden: If U.S. Has 'real Shooting War' It Could Be Result of Cyber Attacks," *Reuters*, July 28, 2021, sec. World, https://www.reuters.com/world/biden-warns-cyberattacks-could-lead-a-real-shooting-war-2021-07-27/.
2. Charles J. Dunlap, "Perspectives for Cyber Strategists on Law for Cyberwar," *Strategic Studies Quarterly* 5, no. 1 (2011): 85.
3. Dunlap, "Perspectives for Cyber Strategists on Law for Cyberwar"; see also David Graham, "Cyber Threats and the Law of War - Journal of National Security Law & Policy," *Journal of National Security Law* 4, no. 1 (2010): 91.
4. Michael Schmitt, ed., "The Use of Force," in *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Newport, Rhode Island: Cambridge University Press, 2017).
5. "International Strategy for Cyberspace" (The White House, May 2011).
6. Robert Work, "United States Cybersecurity Policy and Threats Hearing," https://www.govinfo.gov/content/pkg/CHRG-114shrg22270/html/CHRG-114shrg22270.htm.
7. "On the Application of International Law in Cyberspace" (The Federal Government of Germany, March 2021).
8. "On the Application of International Law in Cyberspace."
9. "On the Application of International Law in Cyberspace."
10. Przemyslaw Roguski, "France's Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations, Part II," *Opinio Juris* (blog), September 24, 2019, http://opiniojuris.org/2019/09/24/frances-declaration-on-international-law-in-cyberspace-the-law-of-peacetime-cyberoperations-part-ii/; "DROIT INTERNATIONAL APPLIQUÉAUX OPÉRATIONSDANS LE CYBERESPACE" (Ministère Des Armèes, September 2019).
11. Roguski, "France's Declaration on International Law in Cyberspace"; "DROIT INTERNATIONAL APPLIQUÉAUX OPÉRATIONSDANS LE CYBERESPACE."
12. Ministry of Foreign Affairs, "Letter to the Parliament on the International Legal Order in Cyberspace," July 5, 2019.
13. Ministry of Foreign Affairs.
14. Jens Stoltenberg, "Nato Will Defend Itself," Prospect Magazine, August 27, 2019, https://www.prospectmagazine.co.uk/world/nato-will-defend-itself-summit-jens-stoltenberg-cybersecurity.
15. Stoltenberg; Oscar Williams, "The WannaCry Ransomware Attack Left the NHS with a £73m IT Bill," *NS Tech* (blog), October 12, 2018, https://tech.newstatesman.com/security/cost-wannacry-ransomware-attack-nhs.
16. NATO, "Collective Defence - Article 5," NATO, accessed May 20, 2021, http://www.nato.int/cps/en/natohq/topics_110496.htm.
17. Red Tape, "Could Cyber Skirmish Lead U.S. to War?," NBC News, June 11, 2010, http://www.nbcnews.com/business/consumer/could-cyberskirmish-lead-u-s-war-flna6C10406234.
18. Tape.
19. Heads of State and Government participating in the meeting of the North Atlantic Council, "Brussels Summit Communiqué Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Brussels 14 June 2021" (North Atlantic Council, June 14, 2021), http://www.nato.int/cps/en/natohq/news_185000.htm; NATO, "Press Conference by NATO Secretary General Jens Stoltenberg Following the Extraordinary Virtual Summit of NATO Heads of State and Government," NATO, February 25, 2022, https://www.nato.int/cps/en/natohq/opinions_192455.htm.
20. Heads of State and Government participating in the meeting of the North Atlantic Council, "Brussels Summit Communiqué Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Brussels 14 June 2021."
21. John Stone, "Cyber War Will Take Place!," *Journal of Strategic Studies* 36, no. 1 (February 1, 2013): 101–8, https://doi.org/10.1080/01402390.2012.730485; Thomas Rid, "Cyber Will Not Take War Place," *Journal of Strategic Studies* 35, no. 1 (February 1, 2012): 5–32, https://doi.org/10.1080/01402390.2011.608939.
22. Rid, "Cyber War Will Not Take Place."
23. Ibid.
24. Stone, "Cyber War Will Take Place!"; Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, August 8, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world.
25. Martin C. Libicki, "Correlations Between Cyberspace Attacks and Kinetic Attacks" (12th International Conference on Cyber Conflict, 2020), 203–11.

NOTES

26. Libicki, 211.
27. Jacquelyn Schneider, "Cyber and Crisis Escalation: Insights from Wargaming" (USASOC Futures Forum, 2017).
28. Benjamin Jensen and Brandon Valeriano, "What Do We Know about Cyber Escalation? Observations from Simulations and Surveys" (Atlantic Council, November 22, 2019), https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/what-do-we-know-about-cyberescalation-observations-from-simulations-and-surveys/.
29. Jensen and Valeriano, 12.
30. Jensen and Valeriano, 6.
31. Aaron F. Brantly, "The Cyber Deterrence Problem," in *2018* 10th *International Conference on Cyber Conflict (CyCon)* (2018 10th International Conference on Cyber Conflict (CyCon), Tallinn: IEEE, 2018), 45, https://doi.org/10.23919/CYCON.2018.8405009.
32. Brantly, 45.
33. Charles Glaser, "Deterrence of Cyber attacks and US National Security" (Washington, D.C.: Cyber Security Policy and Research Institute, 2011).
34. Martin C. Libicki, "Crisis and Escalation in Cyberspace," January 3, 2013, https://www.rand.org/pubs/monographs/MG1215.html.
35. Ibid.
36. William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89, no. 5 (n.d.): 98.
37. Jonathan William Welburn, Justin Grana, and Karen Schwindt, "Cyber Deterrence or: How We Learned to Stop Worrying and Love the Signal," September 4, 2019, 3, https://www.rand.org/pubs/working_papers/WR1294.html.
38. Welburn, Grana, and Schwindt, 3.
39. Welburn, Grana, and Schwindt, 25.
40. Nadiya Kostyuk, Scott Powell, and Matt Skach, "Determinants of the Cyber Escalation Ladder," *The Cyber Defense Review* 3, no. 1 (2018): 128.
41. Kostyuk, Powell, and Skach, 129.
42. Susan G. Straus et al., "Collective Simulation-Based Training in the U.S. Army: User Interface Fidelity, Costs, and Training Effectiveness," Product Page (RAND Corporation, 2019), 34, https://www.rand.org/pubs/research_reports/RR2250.html.
43. Straus et al., 34.
44. Timo Steffens, *Attribution of Advanced Persistent Threats: How to Identify the Actors Behind Cyber-Espionage,* 1st ed. 2020 edition (Berlin Heidelberg: Springer Vieweg, 2020), 38.
45. John S. Davis et al., "Stateless Attribution: Toward International Accountability in Cyberspace" (RAND Corporation, June 2, 2017), 23, https://www.rand.org/pubs/research_reports/RR2081.html; "Welcome to YARA's Documentation! — Yara 4.2.1 Documentation," 2021, https://yara.readthedocs.io/en/latest/.
46. Eric Horvitz, "Applications for Artificial Intelligence in Department of Defense Cyber Missions," Microsoft On the Issues, May 3, 2022, https://blogs.microsoft.com/on-the-issues/2022/05/03/artificial-intelligence-department-of-defense-cyber-missions/.
47. Sally Cole, "Rhamnousia: Framework for Cyberattack Attribution - Military Embedded Systems," Military Embedded Systems, February 14, 2017, http://militaryembedded.com/cyber/cybersecurity/rhamnousia-framework-cyberattack-attribution.
48. Umara Noor et al., "A Machine Learning-Based FinTech Cyber Threat Attribution Framework Using High-Level Indicators of Compromise," *Future Generation Computer Systems* 96 (July 1, 2019): 227–42, https://doi.org/10.1016/j.future.2019.02.013.
49. Maimonah Alkaabi and Sunday O. Olatunji, "Modeling Cyber-Attribution Using Machine Learning Techniques," in *2020 30th International Conference on Computer Theory and Applications (ICCTA),* 2020, 10–15, https://doi.org/10.1109/ICCTA52020.2020.9477672.
50. Davis et al., "Stateless Attribution," 23.
51. Office of the Director of National Intelligence, "Cyber Threat Framework," accessed July 11, 2022, https://www.dni.gov/index.php/cyber-threat-framework.

NOTES

52. CISA, "Information Sharing and Awareness | CISA," February 16, 2022, https://www.cisa.gov/information-sharing-and-awareness; Richard Manfredi, "President Biden Signs into Law the Cyber Incident Reporting for Critical Infrastructure Act, Expanding Cyber Reporting Obligations for a Wide Range of Public and Private Entities," *Gibson Dunn* (blog), March 22, 2022, https://www.gibsondunn.com/president-biden-signs-into-law-the-cyber-incident-reporting-for-critical-infrastructure-act-expanding-cyber-reporting-obligations-for-a-wide-range-of-public-and-private-entities/.
53. Sanjay Goel, "How Improved Attribution in Cyber Warfare Can Help De-Escalate Cyber Arms Race," *Connections* 19, no. 1 (2020): 87–95.
54. Milton Mueller et al., "Cyber Attribution: Can a New Institution Achieve Transnational Credibility?," *The Cyber Defense Review* 4, no. 1 (2019): 107–22.
55. "Tracking State-Sponsored Cyberattacks Around the World," Council on Foreign Relations, 2020 2005, https://www.cfr.org/cyberoperations.
56. Ibid.
57. Christopher Bing, "Exclusive: Wide-Ranging SolarWinds Probe Sparks Fear in Corporate America | Reuters," *Reuters*, September 10, 2021, https://www.reuters.com/technology/exclusive-wide-ranging-solarwinds-probe-sparks-fear-corporate-america-2021-09-10/.
58. Scott Jasper, "Assessing Russia's Role and Responsibility in the Colonial Pipeline Attack," *Atlantic Council* (blog), June 1, 2021, https://www.atlanticcouncil.org/blogs/new-atlanticist/assessing-russias-role-and-responsibility-in-the-colonial-pipeline-attack/.
59. The Associated Press, "REvil, A Notorious Ransomware Gang, Was Behind JBS Cyberattack, The FBI Says," NPR, June 3, 2021, sec. Business, https://www.npr.org/2021/06/03/1002819883/revil-a-notorious-ransomware-gang-was-behind-jbs-cyberattack-the-fbi-says.
60. Charlie Osborne, "Updated Kaseya Ransomware Attack FAQ: What We Know Now," ZDNet, July 23, 2021, https://www.zdnet.com/article/updated-kaseya-ransomware-attack-faq-what-we-know-now/; Kari Paul, "Who's behind the Kaseya Ransomware Attack – and Why Is It so Dangerous?," *The Guardian*, July 7, 2021, https://www.theguardian.com/technology/2021/jul/06/kaseya-ransomware-attack-explained-russia-hackers.
61. Patrick O'Niell, "The US Is Unmasking Russian Hackers Faster than Ever," MIT Technology Review, February 21, 2022, https://www.technologyreview.com/2022/02/21/1046087/russian-hackers-ukraine/.
62. Ryan Maness, Brandon Valeriano, and Ben Jensen, "Codebook for the Dyadic Cyber Incidentand Campaign Dataset (DCID) Version 2.0," June 2022, https://drryanmaness.wixsite.com/cyberconflict/cyber-conflict-dataset.
63. Ibid.
64. Dan Goodin, "A Patient Dies After a Ransomware Attack Hits a Hospital," *Wired,* https://arstechnica.com/information-technology/2020/09/patient-dies-after-ransomware-attack-reroutes-her-to-remote-hospital/.
65. Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, March 3, 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/; Goodin, "A Patient Dies After a Ransomware Attack Hits a Hospital"; Williams, "The WannaCry Ransomware Attack Left the NHS with a £73m IT Bill."
66. Sarah Kreps and Debak Das, "Warring from the Virtual to the Real: Assessing the Public's Threshold for War over Cyber Security," *Research & Politics* 4, no. 2 (April 1, 2017): 2053168017715930, https://doi.org/10.1177/2053168017715930.
67. Ryan Shandler et al., "Cyber Terrorism and Public Support for Retaliation – A Multi-Country Survey Experiment," *British Journal of Political Science*, undefined/ed, 1–19, https://doi.org/10.1017/S0007123420000812.
68. Kreps and Das, "Warring from the Virtual to the Real"; Shandler et al., "Cyber Terrorism and Public Support for Retaliation – A Multi-Country Survey Experiment."
69. Andy Greenberg, "How 30 Lines of Code Blew Up a 27-Ton Generator," *Wired,* October 23, 2020, https://www.wired.com/story/how-30-lines-of-code-blew-up-27-ton-generator/.
70. Microsoft, "Special Report: Ukraine," Microsoft On the Issues, April 27, 2022, 3–4, https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/.
71. Patrick O'Niell, "Russia Hacked an American Satellite Company One Hour before the Ukraine Invasion," MIT Technology Review, May 10, 2022, https://www.technologyreview.com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine-invasion/.

NOTES

72. Microsoft, "Special Report: Ukraine"; Kate Conger and David E. Sanger, "Russia Uses Cyberattacks in Ukraine to Support Military Strikes, Report Finds," *The New York Times,* April 27, 2022, sec. U.S., https://www.nytimes.com/2022/04/27/us/politics/russia-cyberattacks-ukraine.html.
73. Microsoft, "Special Report: Ukraine"; Conger and Sanger, "Russia Uses Cyberattacks in Ukraine to Support Military Strikes, Report Finds."
74. Conger and Sanger, "Russia Uses Cyberattacks in Ukraine to Support Military Strikes, Report Finds."
75. Matthias Schulze, "Cyber in War: Assessing the Strategic, Tactical, and Operational Utility of Military Cyber Operations" (Berlin: 12th International Conference on Cyber Conflict, 2020), https://ccdcoe.org/uploads/2020/05/CyCon_2020_10_Schulze.pdf.
76. Government Accountability Office, "Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities | U.S. GAO" (U.S. Government Accountability Office, October 9, 2018), https://www.gao.gov/products/gao-19-128.
77. Ryan Browne, "Russia Jammed GPS during Major NATO Military Exercise with US Troops | CNN Politics," CNN, November 14, 2018, https://www.cnn.com/2018/11/14/politics/russia-nato-jamming/index.html.
78. Ciaran Martin, "Cyber Realism in a Time of War," Lawfare, March 2, 2022, https://www.lawfareblog.com/cyber-realism-time-war.
79. Sean Lyngaas, "Biden Says He Gave Putin List of 16 Sectors That Should Be Off-Limits to Hacking," *CyberScoop,* June 16, 2021, https://www.cyberscoop.com/biden-putin-summit-russia-geneva/.
80. CISA, "Commercial Facilities Sector | CISA," accessed September 1, 2021, https://www.cisa.gov/commercial-facilities-sector.
81. The White House, "Remarks by President Biden on Russia's Unprovoked and Unjustified Attack on Ukraine," The White House, February 24, 2022, https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/02/24/remarks-by-president-biden-on-russias-unprovoked-and-unjustified-attack-on-ukraine/.
82. Kate O'Flaherty, "How To Hack An Aircraft," Forbes, August 22, 2018, https://www.forbes.com/sites/kateoflahertyuk/2018/08/22/how-to-hack-an-aircraft/.
83. Osborne, "Updated Kaseya Ransomware Attack FAQ."
84. Ben Gilbert, "Colonial Pipeline Reportedly Paid Nearly $5 Million to the Hackers Who Shut off Service to the Largest Fuel Line in the US," *Business Insider,* May 13, 2021, https://www.businessinsider.com/hackers-get-5-million-after-causing-major-gas-shortage-2021-5; The Associated Press, "REvil, A Notorious Ransomware Gang, Was Behind JBS Cyberattack, The FBI Says."
85. Derek B. Johnson, "US Proposes $1 Million Fine for Colonial Pipeline Ransomware Attack," SC Media, May 9, 2022, https://www.scmagazine.com/analysis/critical-infrastructure/us-proposes-1-million-fine-for-colonial-pipeline-ransomware-attack; Joe Walsh, "Meat Producer JBS Says It's Fully Recovered From Cyberattack," Forbes, June 3, 2021, https://www.forbes.com/sites/joewalsh/2021/06/03/meat-producer-jbs-says-its-fully-recovered-from-cyberattack/.
86. Catalin Cimpanu, "Israel Government Tells Water Treatment Companies to Change Passwords," ZDNet, April 27, 2020, https://www.zdnet.com/article/israel-says-hackers-are-targeting-its-water-supply-and-treatment-utilities/.
87. Catalin Cimpanu, "Two More Cyberattacks Hit Israel's Water System," ZDNet, July 20, 2020, https://www.zdnet.com/article/two-more-cyberattacks-hit-israels-water-system/.
88. AP and TOI STAFF, "'Cyber Winter Is Coming,' Warns Israel Cyber Chief after Attack on Water Systems," May 28, 2020, https://www.timesofisrael.com/israeli-cyberchief-attack-on-water-systems-a-changing-point-in-cyberwarfare/.
89. TOI Staff, "Cyber Attacks Again Hit Israel's Water System, Shutting Agricultural Pumps," July 17, 2020, https://www.timesofisrael.com/cyberattacks-again-hit-israels-water-system-shutting-agricultural-pumps/.
90. Joby Warrick and Ellen Nakashima, "Officials: Israel Linked to a Disruptive Cyberattack on Iranian Port Facility," *Washington Post,* May 18, 2020, https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html.
91. AP Staff, "'Cyber Disruption' Stops Websites of Iranian Ministry," AP NEWS, July 10, 2021, https://apnews.com/article/middle-east-business-technology-iran-hacking-f03eb1887f2be46648886e1c80e50586.

NOTES

92. Suren Naidoo, "Transnet's Ports Force Majeure Is over, but Most Websites Are Still Offline," *Moneyweb,* August 2, 2021, sec. Industry, https://www.moneyweb.co.za/news/industry/transnets-ports-force-majeure-is-over-but-most-websites-are-still-offline/.
93. Felix Njini and Prinesha Naidoo, "South Africa Port Operator Declares Force Majeure Over Cyber Attack," *Bloomberg,* July 27, 2021, https://www.bloomberg.com/news/articles/2021-07-27/s-africa-port-operator-declares-force-majeure-over-cyber-attack-krln4ku6; Denys Reva, "Cyber Attacks Expose the Vulnerability of South Africa's Ports," *ISS Africa,* July 29, 2021, https://issafrica.org/iss-today/cyber-attacks-expose-the-vulnerability-of-south-africas-ports.
94. e Tidy, "Ukrainian Power Grid 'lucky' to Withstand Russian Cyber-Attack," *BBC News,* April 12, 2022, sec. Technology, https://www.bbc.com/news/technology-61085480.
95. Nate Nelson, "U.S. Water Utilities Prime Cyberattack Target, Experts," Threatpost, June 10, 2022, https://threatpost.com/water-cyberattack-target/179935/.
96. Kevin Collier, "A Hacker Tried to Poison a Calif. Water Supply. It Was as Easy as Entering a Password.," NBC News, June 17, 2021, https://www.nbcnews.com/tech/security/hacker-tried-poison-calif-water-supply-was-easy-entering-password-rcna1206.
97. Matt Egan, "$24 Billion in Goods Is Floating Outside California's Biggest Ports | CNN Business," CNN, October 25, 2021, https://www.cnn.com/2021/10/25/business/supply-chain-ports-inflation/index.html.
98. Will Daugherty, "Lloyd's Report Highlights Risk of Cyberattacks on National Power Grid," JD Supra, July 24, 2015, https://www.jdsupra.com/legalnews/lloyd-s-report-highlights-risk-of-83905/.
99. Vanessa Romo, "How A New Team Of Feds Hacked The Hackers And Got Colonial Pipeline's Ransom Back," NPR, June 8, 2021, https://www.npr.org/2021/06/08/1004223000/how-a-new-team-of-feds-hacked-the-hackers-and-got-colonial-pipelines-bitcoin-bac; Jacob Bunge, "JBS Paid $11 Million to Resolve Ransomware Attack," *Wall Street Journal,* June 10, 2021, sec. Business, https://www.wsj.com/articles/jbs-paid-11-million-to-resolve-ransomware-attack-11623280781.
100. CSIS, "Significant Cyber Incidents | Center for Strategic and International Studies," updated monthly, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.
101. CSIS, "Significant Cyber Incidents | Center for Strategic and International Studies," March 2022, https://www.csis.org/programs/strategic-technologies-program/significant-cyberincidents.
102. "US Mulling Military Response to Ransomware Attacks, Biden Officials Say," accessed June 26, 2021, https://www.theguardian.com/technology/2021/jun/06/us-military-response-ransomware-attacks-biden-russia-putin.
103. NATO, "Press Conference by NATO Secretary General Jens Stoltenberg Following the Extraordinary Virtual Summit of NATO Heads of State and Government."

Machine Learning Applications for Cybersecurity

M.A. Thomas

ABSTRACT

The trope of future cybersecurity as a battle between warring artificial intelligences awaits the development of artificial general intelligence. In the interim, however, machine learning is being applied to a number of cybersecurity problem sets. This article looks more closely at how machine learning is transforming cybersecurity, considering the examples of authentication and masquerade, spam filtering and spam, antimalware and malware, and intrusion detection and intrusion. Machine learning is adding new capabilities for cyber defense and in most cases is useful in conjunction with other approaches. At present, machine learning applications for cyber offense remain primarily proofs of concept.

A flurry of articles has warned that soon cybersecurity will be utterly transformed, becoming a battle between warring artificial intelligences that adapt to each other's moves at "machine speed." Like many claims in an era of artificial intelligence (AI) hype, the image is grounded in ideas of "artificial general intelligence," AI programs that can solve a wide range of problems at least as well as a human. But artificial general intelligence is likely decades away at best—and some say that it is an impossibility.

In the interim, "narrow" artificial intelligence is being used to develop applications for cybersecurity. The current dominant approach in artificial intelligence is machine learning (ML). ML programs use data to develop statistical or probabilistic models that can be used to classify, predict, or generate new examples.

M.A. Thomas is a professor at the College of Information and Cyberspace at National Defense University. She holds a BA in computer and information science from the University of California, Santa Cruz, a JD from the University of California, Berkeley, and a PhD in political economy and government from Harvard University. Her work has appeared in leading academic and policy outlets, including *Foreign Affairs, International Affairs, Defence Studies,* and *Strategic Studies Quarterly.*

This article examines how ML applications are shaping cybersecurity today. It discusses four examples in which machine learning tools are currently being applied: authentication and masquerade attacks; spam filtering and spam; antimalware and malware; and intrusion detection and intrusion. ML is adding new tools to the toolbox, primarily for cyber defenders, but the inherent limitations of machine learning often mean that it is most useful in combination with other approaches.

MACHINE LEARNING

There is no consensus definition of "artificial intelligence," a field of computer science that addresses problems previously thought to require human intelligence. Indeed, the definition is necessarily dynamic as innovation changes expectations of the kinds of problems computers can be used to solve.

Much of the hyperbole about AI is focused on "artificial general intelligence" (also called "general artificial intelligence"), programs that can solve a wide range of problems at least as well as humans can. However, artificial general intelligence does not exist and is not on the near horizon. Some believe it to be impossible.[1] Current AI is called "narrow AI," meaning that the programs are crafted to solve narrowly defined problems.

There are several families of approaches to artificial intelligence and approaches are often combined. For example, "first generation" artificial intelligence, or "expert systems," seek to distill human domain expertise into hard-coded rules that are applied by the program to make the same types of judgments using the same criteria. An example application is the diagnosis of medical conditions.[2] Another has attempted to mimic human reasoning by applying logical rules to data to reach conclusions, such as programs that verify models for quality control.[3] Game-theoretic approaches use game theory to map out possible responses to precisely

defined problems to determine which option is superior. This approach has been used to write programs that win at certain types of competitive games.[4]

However, the current dominant family of approaches in AI is machine learning, which involves building statistical and probabilistic models from data. The models are then applied to new data to make predictions, classify, or to generate new examples from a prompt. The field of ML has benefited from an explosion in the amount of data available for model generation ("training") due to internet and cell phone usage, improvements in data storage, and increased computational power that enables the analysis of that data.

ML models depend on human choices. Researchers select and analyze the input data and consider the desired outcome, deciding how the program will acquire data for model building, what variables ("features") and data should be used for model building, what type of model to build, what algorithm to use to build the model, what parameters should be used in the model building process, and how rare cases will be handled. They curate and provide the training data to build the model, a process called "supervised learning," or they may arrange for data to flow to the program without human curation (for example, from a sensor) in "unsupervised learning" or "reinforcement learning," or they may use a combination of these approaches. The algorithm generates the model from the data, a process called "training" a model. Because the models are probabilistic and statistical, some cases will not be handled correctly. Developers must decide whether some kinds of mistakes are more important than others and what kind of metrics will be used to evaluate model performance. They then test the model on new data and tweak the model or its parameters to optimize performance.[5]

Narrow AI programs are brittle. Novel cases are not handled well because they were not represented in the model's training data. In addition, if the relationship between model inputs and outputs changes, the model may no longer work as well or work at all, a phenomenon called "concept drift."[6] For example, a number of stock market models failed to correctly predict the behavior of the stock market during the COVID-19 pandemic.[7]

Finally, ML models can be defeated. A subfield of machine learning deals with the generation of adversarial examples deliberately designed to be misclassified by a given machine learning model. To generate such examples, researchers need some feedback about how new data are classified. Given that feedback, reverse engineering the model and generating adversarial examples is fairly straightforward.[8]

New tools for cybersecurity continue to be developed and deployed that use expert systems. But research and development of machine learning tools for cybersecurity have exploded in the last five years, in part because of the new availability of data for model training, such as the Github code repository and public malware repositories. Four cybersecurity problem sets highlight the contribution of ML tools: authentication and masquerade attacks, spam and spam filters, malware and antimalware, and intrusion detection.

AUTHENTICATION AND MASQUERADE

A key element of cybersecurity is user authentication, a process used to confirm that a user is who they claim to be before granting access to a system or resource. Authentication factors are *something you know*, *something you have*, or *something you are*. *Something you know* may be a user password; s*omething you have* may be a second device like a cell phone; *something you are* may be your face or fingerprint. ML has enabled wider use of biometric authentication (*something you are*). In a masquerade attack, an attacker seeks to defeat authentication by masquerading as a legitimate user. ML has been used to conduct masquerade attacks by defeating CAPTCHA tests designed to ensure that users are human.

Biometric Authentication

Advances in machine learning have led to increased use of biometrics as means of authentication for many functions.[9] Biometrics can be physiological, such as a person's face, fingerprint, or iris; or behavioral, such as distinct patterns in keystrokes or voice. The biometric information is gathered with appropriate sensors, e.g., a camera for visual information or a microphone for voice information. It is then preprocessed to extract features of interest. These are fed into a classifier model to identify the individual.

Both facial and fingerprint recognition are widely used for cybersecurity. An increasing number of smartphone manufacturers offer the ability to unlock a phone using facial or fingerprint recognition. Both Windows 10 and 11 offer the ability to unlock a laptop using facial recognition with the "Windows Hello" feature.[10] The Government Accountability Office reported in 2021 that sixteen federal agencies have used facial recognition technology for employees to unlock their government-issued smartphones, while two are experimenting with it to authenticate users of government websites.[11] Voice recognition is also used to access some websites.

Biometric authentication is an attractive problem set for machine learning applications because the key features of faces or fingerprints are relatively stable over the period of interest. However, as with all machine learning programs, authentication programs make mistakes. They can also be defeated, including by presenting falsified data to sensors, intercepting and then replaying the identifying data, or using constructed data.[12] Security researchers at Talos reported an 80% success rate in defeating fingerprint recognition, including on cell phones and laptops, using a fingerprint collected from a user and a 3D printer to create a replica.[13] One response has been to attempt to develop ML programs that seek to distinguish between "live" users and static replicas, either by collecting more data through hardware sensors (such as blood pressure) or by software.[14]

Defeating CAPTCHA

CAPTCHA ("Completely Automated Public Turing test to tell Computers and Humans Apart") systems are tests designed to determine whether an online user is human in the effort to prevent automated account creation and access to web resources such as webmail forms. They

were initially developed at Carnegie Mellon University in 2000.[15] An example task is to identify a visually distorted number. However, they can be challenging for the visually impaired. Accordingly, many also have an auditory form. Google originally acquired reCAPTCHA, one of the major CAPTCHA systems, as a way to leverage user image recognition to help with its book digitization project.[16]

Researchers have developed proof-of-concept machine learning attacks that bypassed CAPTCHA systems by using ML image recognition on visual CAPTCHAs and freely available machine learning speech recognition utilities on auditory versions.[17] Google released "Invisible reCAPTCHA" the same year. Invisible reCAPTCHA uses machine learning to analyze the user's browser behavior, such as mouse movements, to determine if the user is human.[18] However, this approach relies on cookies to store information about user behavior. If a user used a new device or cleared cookies, the system defaulted to the older reCAPTCHA system, and so was easily defeated. As one security researcher commented, "The fact that Invisible reCAPTCHA can be bypassed isn't because there was a fatal flaw in the design of the newer CAPTCHA. It's that any reverse Turing test is inherently beatable when the pass conditions are known."[19]

SPAM FILTERING AND SPAM

Cybersecurity company Proofpoint estimates from its customer data that less than one percent of cyberattacks depend on system vulnerabilities. The majority depend on social engineering—deceiving people into sharing sensitive information, giving access, or downloading malware.[20] A principal means of conducting such attacks is through "phishing" emails designed to trick users into sharing sensitive information. Verizon's analysis of a sample of convenience of more than 157,000 incidents confirms that phishing attacks and credential theft eclipse attacks that involve the installation of malware.[21]

Phishing emails may be sent in bulk as spam, or they may be specially targeted to a particular user or group of users. Some cyberattacks simply require that the user open the email ("fileless" attacks). Others require the user to open an attachment, which then installs malware. Still others require the user to click on a link that downloads malware or that leads to a website that deceives the user into entering credentials that are then stolen. Phishing emails are designed to persuade the user to take the necessary action to complete the compromise.

To reduce the incidence of this type of attack, as well as general nuisance emails, many email programs use email filters to classify incoming emails as spam or junk, which is then blocked or marked. The earliest spam filters relied on expert systems, hard-coded rules for classification based on an analysis of email traffic. Emails might be screened based on the addresses of senders, their headers, their content, or their language.[22] Spam senders responded by adopting tools that randomize parts of the email message so that they could not be excluded by a hard-coded rule.[23] Later filters used researcher-specified probabilistic or statistical models to evaluate whether an email is likely to be spam.

Machine learning approaches develop the models using data. They benefit from the public release of databases of emails to be used for model training.[24] Email service providers can also draw on the corpus of emails that are sent and received by their users and user classifications of emails. The literature on machine learning approaches to spam filtering is sufficiently voluminous to have given rise to multiple, recent literature reviews.[25]

These approaches are usually combined. Google, for example, uses both rules-based and machine learning approaches to combat spam on its Gmail email platform and claims to be able to detect and block 99.99% of spam, phishing, and malware emails.[26]

It does not appear that spam senders are using machine learning approaches. However, researchers have developed a proof-of-concept spam generator that uses machine learning to evade a spam filter by learning which phrases cause a filter to identify an email as spam.[27] As with all adversarial examples, this requires some feedback regarding how the email has been classified. In this case, the researchers had access to user inboxes and perfect information about how the email was classified.

ANTIMALWARE AND MALWARE

The Creeper was thought to be the first computer virus, designed in 1971 as a proof of concept, displaying the text, "I'm the creeper: catch me if you can!" It prompted the creation of the first antivirus program, The Reaper.[28] Today, malicious software is used to wipe hard drives, steal sensitive information, commandeer computers and equipment or physically destroy them, or to establish "backdoors" for later access.

The use of antimalware software to identify and quarantine malicious executable files on the end user's computer is considered the last line of cybersecurity defense. To operate, antimalware software must be able to classify executable files as malicious or benign. Security researchers would also like to know what the malware does and how it operates so they can check it more effectively. The classic approach to this problem is through signature-based malware detection. Machine learning approaches have been applied to different parts of the problem of signature development and malware detection. They have also been used to identify malware without relying on a fixed signature.

Signature-Based Malware Detection

In signature-based malware detection, security researchers who identify suspicious code study the sample. First, they examine the executable file at rest ("static analysis"). They may reverse engineer it, translating the binary executable code into a higher-level format that allows them to better understand the program logic and actions. They may then run the program to see what it does ("dynamic analysis"). Because of the possibly malicious nature of the code, suspected malware is run in a virtual "sandbox" environment where its behavior can be closely monitored and where it has limited ability to affect the computer.[29]

If the code is determined to be malicious, researchers attempt to identify a "signature," unique blocks or features of the code that can be used to identify it. This signature is added to the database of signatures. The antimalware program scans the files on the hard drive or processes in memory, flagging and quarantining malware with those signatures if it is detected.[30]

This signature-based detection method can only detect known malware for which signatures have been developed but it is still useful. Existing malware is often reused. There is no need for malware developers to develop something new if the old tools will meet their objectives.

However, malware developers do take steps to thwart the signature-development process and signature-based detection. Some malware is written to detect whether it is being run in a sandbox, and, if so, to terminate execution, preventing dynamic analysis. Developers may divide the malware into multiple files, encode or change strings, encrypt the files, or compress ("pack") them to make reverse engineering or detection more difficult.[31] A "stub" executable unpacks and runs the malicious payload. It is not uncommon for malware to have been subjected to multiple layers of encryption and packing. "Fileless" malware avoids writing files to the hard drive where they might be scanned, instead installing in firmware or remaining and running in memory and leveraging native operating system processes to further avoid detection.[32] Fileless attacks have been growing exponentially, bypassing many antimalware programs.

Machine learning approaches have been applied to different parts of this problem set. They include machine learning programs for reverse engineering and for identifying malware without using signatures. At the moment, malware that leverages machine learning remains proof of concept.

Reverse Engineering

One relevant application of machine learning is to facilitate reverse engineering. Computer programs are typically written in a high-level programming language in which a program is expressed as a set of tasks and then "compiled," translated into binary code representing instructions and data for a specific type of computer processor. Humans cannot read and follow binary executables of any length or complexity. Reverse engineering, or "reversing," translates binary code back into instructions that can be more easily understood by humans. Disassemblers translate binary into "assembly language," natural language representations of the instructions to the processor. Decompilers translate binary into a higher-level language program that carries out the same functions. In addition, there are programs that seek to capture and represent the program logic in forms other than a programming language, such as a control flow graph.

Reversing is complicated by the fact that there is not a unique one-to-one mapping between high-level source code and a binary executable. The mapping depends on the compiler, the computer architecture, and code optimization options used during compilation, information that is typically not available to a security researcher.[33] In addition, some information is lost

during the compilation process, such as natural language procedure and variable names that might explain what the purpose of a procedure is, the order in which procedures are called in execution, or information about where functions start and stop.[34]

In addition, developers may take steps to make reverse engineering of their code harder. Malware developers may wish to thwart security researchers. Developers of benign software may wish to protect their intellectual property or prevent tampering. Most commercial software licenses explicitly prohibit reversing for this reason. Examples of these kinds of measures are stripping strings and metadata that would provide clues to program functionality ("stripped" binary executables); using self-modifying code that overwrites its own instructions in memory; and using code that is encrypted at rest and only decrypted in execution.[35]

For these reasons, reversing has been a slow process conducted by a domain expert with software tools that are aids rather than solutions.[36] Disassemblers and decompilers have historically used expert-system, rule-based approaches.[37]

There have been several efforts to facilitate reversing using machine learning. For example, researchers proposed a proof-of-concept machine learning model to decompile small snippets of code from binary, following methods that had been used for text translation.[38] Others built on this approach, achieving greater accuracy by training a machine learning decompiler using code snippets compiled with a given compiler.[39] However, with this approach, each combination of architecture, programming language, and optimization settings would need to be modeled independently.

Other approaches have tackled subparts of the problem of reversing. For example, researchers have used machine learning to determine likely and descriptive names for functions in a stripped executable using control-flow graphs of application programming interface calls.[40] Others have used machine learning for detecting similar sections of binary code or determining where functions start and stop.[41]

Research in this area is still in proof-of-concept phase. It seems likely that machine learning will provide additional tools for reverse engineering but will still fall short of producing a fully automated solution because of obfuscation and information lost in the compilation process and the steps taken to thwart reverse engineering.

Malware Identification without Signatures

Another active area of research is the use of machine learning to classify malware without reliance on hard-coded, manually produced signatures. Researchers build machine learning models of various features of static code or of code in execution.[42] First generation efforts to use machine learning depended on researchers with expert domain knowledge to identify key features from static or dynamic analysis of malware to use as training data. Manually extracted static features include printable strings, application programming interface (API) function calls, function call graphs, control flow graphs, sequences of bytes and opcodes, or the

representation of the patterns of binary code as gray scale images, or a measure of entropy. Manually extracted dynamic features include memory and register usage, instruction traces, and network traffic and API call traces. The second generation uses deep learning to identify the important features from raw code or minimally processed data.[43] Another effort uses the text reports generated by running software in a sandbox.[44]

Machine learning models are more flexible than hard-coded rules and can more easily rely on a wider variety of features to flag suspected malware. However, they will fail to detect novel malware in general and can also be fooled by adversarial examples. Researchers at Skylight Cyber fooled Blackberry Cylance's PROTECT malware detection software simply by appending strings from a popular game to existing malware files.[45]

Environmentally Aware Malware

Although, as of this writing, it is unclear that any malware detected in the wild uses machine learning, researchers have suggested proofs of concept. One example is the use of machine learning for environmentally aware malware.

Environmentally aware malware classifies the environment and executes code based on this classification. This classification has historically been rules-based. For example, the malware may be designed to perform differently or not execute if it detects cues that it is in a sandbox or if it detects a process from a software analysis tool currently running, signals that it is under analysis by security researchers.[46] In 2018, a security researcher reported that 98% of malware that his team analyzed in a sandbox used at least one evasive tactic and 32% used six or more.[47]

Alternately, environmentally aware malware may be targeted, designed to execute its payload only when it is running on a machine with certain characteristics. A famous example of targeted malware, Stuxnet, executed its payload only if conditions were met that described the equipment used for uranium enrichment at Iran's Natanz facility.[48] It sped the centrifuges up periodically while disguising this activity from operators, causing centrifuges to break.

Classification problems are natural candidates for machine learning. Researchers have shown that it is possible to use machine learning, rather than expert systems, to classify the environment. For example, researchers at IBM developed DeepLocker, proof-of-concept malware that uses machine learning to determine whether it has reached the targeted machine and only then generates a decryption key used to unlock the payload, preventing reverse engineering.[49] In their demonstration, DeepLocker triggered only when it recognized the face of a specific user, using the infected computer's camera, another application of biometrics.

INTRUSION DETECTION AND INTRUSION

A final example of the use of machine learning for cybersecurity is in intrusion detection systems. Intrusion detection systems are used to detect unauthorized access to or use of computer systems and networks. They focus on patterns of network usage, system usage, or user behavior.

Intrusion detection systems are classified as signature based or anomaly based.[50] Signature-based intrusion detection is similar to signature-based malware detection. It uses logs of previous intrusions to identify unique patterns of network traffic, which are added to a database. The intrusion detection system then scans for a recurrence of these patterns. Like signature-based malware detection systems, signature-based intrusion detection systems can only detect attacks that have occurred previously and for which signatures have been obtained. Accordingly, they may give "false negatives," failing to detect attacks, even ones that are very similar to previous attacks.

Anomaly-based intrusion detection builds a model of normal system usage and flags deviations. In the 1970s and 1980s, system administrators attempted to detect anomalies by manually examining system audit logs.[51] Expert systems were introduced in the late 1970s. A 1980 report proposed collecting statistical data on system usage by individual users over a period of time, to be used as a baseline, and then using statistical analysis to detect deviations.[52] The first such system was created in the 1980s, using statistical profiles of the behavior of individual users on the system as well as a rules-based expert system.[53]

Although statistical techniques such as regression analysis are now considered to be in the family of machine learning approaches, modern machine-learning, anomaly-based intrusion detection systems rely on a wide variety of approaches, and may focus on different features such as packets, packets over time, packet sequences, logs, or client sessions.[54] Each of these has advantages and disadvantages in terms of the reliability of the outputs.

Unlike signature-based intrusion detection systems, anomaly-based systems can detect novel attacks when they cause a significant deviation from the model of "normal" behavior. At the same time, these systems also flag any other novel pattern, and there are many legitimate reasons why network, system, or user behavior can deviate from previous patterns. Concept drift is also a problem, requiring constant model retraining. Accordingly, these systems can have high false positive rates. One recommendation is to combine them with rules-based expert systems to get the benefits of both.[55] Some hybrid systems use the output of rules-based intrusion detection systems as an input to a machine learning model to attempt to prioritize alerts for human attention.[56]

Researchers are seeking to address challenges in using machine learning for anomaly-based intrusion detection systems, including a lack of data to train models and poor portability of the models to new environments once trained.[57] To be useful, the intrusion detection system must also run without consuming too many system resources so that it does not interfere with regular system use.

Again, given a signal of how an intrusion detection system classifies traffic, it is possible to learn how the intrusion detection system works and develop adversarial examples that evade it. Researchers have developed proof-of-concept intrusions that are successfully concealed in legitimate traffic.[58]

CONCLUSION

More Tools in the Toolbox

While a far cry from the hype of warring, adaptive artificial intelligences, these examples illustrate how machine learning approaches provide new capabilities for defenders in cybersecurity in authentication, spam filtering, and malware and intrusion detection. They are less brittle than rules-based expert systems, providing statistical or probabilistic classifications instead of an absolute classification that requires all conditions to be fully met. The model need not be fully specified by experts. Instead, algorithms can tease complex patterns from large quantities of data. In some cases, machine learning provides novel capabilities, such as biometric authentication.

As has been pointed out in other domains, machine learning is no panacea. Any classifier can be evaded if an attacker has access to enough information about how it classifies and can also shape the input data.[59] Machine learning models cannot reliably classify or predict examples that were not included in their training data, so they are most relevant for problems that do not change substantially over the period of interest. Training models require sufficient good quality data on relevant features of the problem. In the context of cybersecurity, machine learning models must also be nimble and light, providing quick answers without unduly consuming computational or network resources. For these reasons, machine learning tools complement, rather than replace, human experts and existing tools.

To date, most machine learning applications for cyber offense have been proof of concept. There is limited incentive for attackers to invest in machine learning attack tools when the current tools still serve their purposes well. However, as machine learning tools are adopted for antimalware and intrusion detection, it is possible to imagine attackers using machine learning to develop adversarial examples for evasion.

DISCLAIMER

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

NOTES

1. A 2018 survey of 352 AI researchers asked when "high-level machine intelligence" defined as "unaided machines that can accomplish every task better and more cheaply than human workers" will be achieved. Aggregating their forecasts, the survey found that the researcher estimated a fifty percent chance that this would occur within forty-five years and a ten percent chance that it would occur within nine years. Katja Grace et al., "Viewpoint: When Will AI Exceed Human Performance? Evidence from AI Experts," *Journal of Artificial Intelligence Research* 62 (July 31, 2018): 729–54, https://doi.org/10.1613/jair.1.11222. One point of discussion is the definition of, and the criteria for, "artificial general intelligence." IBM states that artificial general intelligence "only exists today as a theoretical concept versus a tangible reality" given that measures of success have not yet been developed. IBM, "What Is Strong AI? | IBM," accessed December 28, 2022, https://www.ibm.com/topics/strong-ai.
2. See, e.g., A. M. Mutawa and Mariam A. Alzuwawi, "Multilayered Rule-Based Expert System for Diagnosing Uveitis," *Artificial Intelligence in Medicine* 99 (August 1, 2019): 101691, https://doi.org/10.1016/j.artmed.2019.06.007.
3. Roberta Calegari et al., "Logic-Based Technologies for Intelligent Systems: State of the Art and Perspectives," *Information* 11, no. 3 (March 2020): 167, https://doi.org/10.3390/info11030167.
4. John T Hanley, "GAMES, Game Theory and Artificial Intelligence," *Journal of Defense Analytics and Logistics* 5, no. 2 (January 1, 2021): 114–30, https://doi.org/10.1108/JDAL-10-2021-0011.
5. See, e.g., Google Cloud, "Machine Learning Workflow | AI Platform," accessed December 29, 2022, https://cloud.google.com/ai-platform/docs/ml-solutions-overview.
6. Jie Lu et al., "Learning under Concept Drift: A Review," *IEEE Transactions on Knowledge and Data Engineering* 31, no. 12 (December 2019): 2346–63, https://doi.org/10.1109/TKDE.2018.2876857.
7. Will Knight, "Even the Best AI Models Are No Match for the Coronavirus," *Wired,* July 19, 2020, https://www.wired.com/story/best-ai-models-no-match-coronavirus/.
8. Joab Jackson, "Microsoft: Machine Learning Models Can Be Easily Reverse Engineered," *The New Stack* (blog), November 30, 2020, https://thenewstack.io/microsoft-machine-learning-models-can-be-easily-reverse-engineered/.
9. Shervin Minaee et al., "Biometrics Recognition Using Deep Learning: A Survey," *ArXiv:*1912.00271 [Cs], February 8, 2021, http://arxiv.org/abs/1912.00271 (under review).
10. Microsoft, "Windows Hello Face Authentication," July 15, 2021, https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/windows-hello-face-authentication.
11. Government Accountability Office, "Facial Recognition Technology: Current and Planned Uses by Federal Agencies," Report to Congressional Requesters (Washington, DC: Government Accountability Office, August 2021), https://www.gao.gov/assets/gao-21-526.pdf.
12. Battista Biggio et al., "Adversarial Biometric Recognition: A Review on Biometric System Security from the Adversarial Machine-Learning Perspective," *IEEE Signal Processing Magazine* 32, no. 5 (September 2015): 31–41, https://doi.org/10.1109/MSP.2015.2426728.
13. Paul Rascagneres and Vitor Ventura, "Fingerprint Cloning: Myth or Reality?," Talos, April 8, 2020, https://blog.talosintelligence.com/2020/04/fingerprint-research.html.
14. Syed Farooq Ali, Muhammad Aamir Khan, and Ahmed Sohail Aslam, "Fingerprint Matching, Spoof and Liveness Detection: Classification and Literature Review," *Frontiers of Computer Science* 15, no. 1 (2021): 1–18.
15. Stacey Burling, "Captcha: The Story Behind Those Squiggly Computer Letters," Phys.org, June 15, 2012, https://phys.org/news/2012-06-captcha-story-squiggly-letters.html.
16. Rhett Jones, "Google Has Finally Killed the CAPTCHA," Gizmodo, March 11, 2017, https://gizmodo.com/google-has-finally-killed-the-captcha-1793190374.
17. Elie Bursztein et al., "The End Is Nigh: Generic Solving of Text-Based {CAPTCHAs}" (8th USENIX Workshop on Offensive Technologies (WOOT 14), USENIX, 2014), https://www.usenix.org/conference/woot14/workshop-program/presentation/bursztein; Kevin Bock et al., "UnCaptcha: A Low-Resource Defeat of ReCaptcha's Audio Challenge" (11th USENIX Workshop on Offensive Technologies (WOOT '17), Vancouver, BC, Canada, 2017).
18. Rob Verger, "Google Just Made the Internet a Tiny Bit Less Annoying," P*opular Science* (blog), March 18, 2019, https://www.popsci.com/google-invisible-recaptcha/.
19. Nick Flont, "How Cybercriminals Bypass CAPTCHA," Shape Security Blog, July 12, 2017, https://blog.shapesecurity.com/2017/07/12/how-cybercriminals-bypass-captcha/.
20. Proofpoint, "Human Factor Report 2019" (Sunnyvale, CA: Proofpoint, 2019).

NOTES

21. Verizon, "2020 Data Breach Investigations Report," 2020, https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf.
22. Fortinet, "Email Spam Filtering: Different Methods & How They Work," Fortinet, accessed December 16, 2021, https://www.fortinet.com/resources/cyberglossary/spam-filters.
23. See, e.g., Fahim Abbasi, "Tracking the Chameleon Spam Campaign," Trustwave, September 25, 2019, https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/tracking-the-chameleon-spam-campaign/.
24. Emmanuel Gbenga Dada et al., "Machine Learning for Email Spam Filtering: Review, Approaches and Open Research Problems," *Heliyon* 5, no. 6 (June 1, 2019): 8, https://doi.org/10.1016/j.heliyon.2019.e01802.
25. See, e.g., Dada et al., "Machine Learning for Email Spam Filtering"; S. Abiramasundari, V. Ramaswamy, and J. Sangeetha, "Spam Filtering Using Semantic and Rule Based Model via Supervised Learning," *Annals of the Romanian Society for Cell Biology*, 2021, 3975–92; Aliaksandr Barushka, "Machine Learning Techniques in Spam Filtering," 2020; Alexy Bhowmick and Shyamanta M. Hazarika, "E-Mail Spam Filtering: A Review of Techniques and Trends," *Advances in Electronics, Communication and Computing*, 2018, 583–90; Hanif Bhuiyan et al., "A Survey of Existing E-Mail Spam Filtering Methods Considering Machine Learning Techniques," *Global Journal of Computer Science and Technology*, 2018; Pooja Revar et al., "A Review on Different Types of Spam Filtering Techniques.," *International Journal of Advanced Research in Computer Science* 8, no. 5 (2017).
26. Neil Kumaran, "Spam Does Not Bring Us Joy—Ridding Gmail of 100 Million More Spam Messages with Tensorflow," *Google Cloud Blog*, February 6, 2019, https://cloud.google.com/blog/products/g-suite/ridding-gmail-of-100-million-more-spam-messages-with-tensorflow/.
27. Sean Palka and Damon McCoy, "Fuzzing E-Mail Filters with Generative Grammars and N-Gram Analysis" (Woot '15, 9th USENIX Workshop on Offensive Technologies, Washington, DC, August 10, 2015), https://www.usenix.org/conference/woot15/workshop-program/presentation/palka.
28. Tom Meltzer and Sarah Phillips, "From the First Email to the First Youtube Video: A Definitive Internet History," *The Guardian*, October 23, 2009, sec. Technology, https://www.theguardian.com/technology/2009/oct/23/internet-history.
29. See, e.g., Kurt Beker, "Malware Analysis Explained | Steps & Examples | CrowdStrike," Crowdstrike.com, January 4, 2022, https://www.crowdstrike.com/cybersecurity-101/malware/malware-analysis/.
30. Mohammed Al-Asli and Taher Ahmed Ghaleb, "Review of Signature-Based Techniques in Antivirus Products," in *2019 International Conference on Computer and Information Sciences (ICCIS)* (Piscataway, NJ: IEEE, 2019), 1–6, https://doi.org/10.1109/ICCISci.2019.8716381.
31. Trivikram Muralidharan et al., "File Packing from the Malware Perspective: Techniques, Analysis Approaches, and Directions for Enhancements," *ACM Computing Surveys* 55, no. 5 (December 3, 2022): 108:1-108:45, https://doi.org/10.1145/3530810.
32. Sudhakar and Sushil Kumar, "An Emerging Threat Fileless Malware: A Survey and Research Challenges," Cybersecurity 3, no. 1 (December 2020): 1–12, https://doi.org/10.1186/s42400-019-0043-x.
33. H. Xue et al., "Machine Learning-Based Analysis of Program Binaries: A Comprehensive Study," *IEEE Access* 7 (2019): 65889–912, https://doi.org/10.1109/ACCESS.2019.2917668.
34. Yaniv David, Uri Alon, and Eran Yahav, "Neural Reverse Engineering of Stripped Binaries Using Augmented Control Flow Graphs," *Proceedings of the ACM on Programming Languages* 4, no. OOPSLA (November 13, 2020): 1–28, https://doi.org/10.1145/3428293.
35. Shoreh Hosseinzadeh et al., "Diversification and Obfuscation Techniques for Software Security: A Systematic Literature Review," *Information and Software Technology* 104 (December 1, 2018): 72–93, https://doi.org/10.1016/j.infsof.2018.07.007.
36. Daniel Votipka et al., "An Observational Investigation of Reverse Engineers' Processes," 2020, 1875–92, https://www.usenix.org/conference/usenixsecurity20/presentation/votipka-observational.
37. See, e.g., Jakub Křoustek and Peter Matula, "RetDec: An Open-Source Machine-Code Decompiler."
38. Deborah S. Katz, Jason Ruchti, and Eric Schulte, "Using Recurrent Neural Networks for Decompilation," in *2018 IEEE 25th International Conference on Software Analysis, Evolution and Reengineering (SANER)* (2018 IEEE 25th International Conference on Software Analysis, Evolution and Reengineering (SANER), Campobasso: IEEE, 2018), 346–56, https://doi.org/10.1109/SANER.2018.8330222.
39. Omer Katz et al., "Towards Neural Decompilation," *ArXiv:1905.08325 [Cs]*, May 20, 2019, http://arxiv.org/abs/1905.08325.

NOTES

40. David, Alon, and Yahav, "Neural Reverse Engineering of Stripped Binaries Using Augmented Control Flow Graphs."
41. Xue et al., "Machine Learning-Based Analysis of Program Binaries."
42. Daniel Gibert, Carles Mateu, and Jordi Planes, "The Rise of Machine Learning for Detection and Classification of Malware: Research Developments, Trends and Challenges," *Journal of Network and Computer Applications* 153 (March 1, 2020): 102526, https://doi.org/10.1016/j.jnca.2019.102526.
43. Gibert, Mateu, and Planes.
44. Chani Jindal et al., "Neurlux: Dynamic Malware Analysis without Feature Engineering," *in Proceedings of the 35th Annual Computer Security Applications Conference*, ACSAC '19 (New York, NY, USA: Association for Computing Machinery, 2019), 444–55, https://doi.org/10.1145/3359789.3359835.
45. Kim Zetter, "Researchers Easily Trick Cylance's AI-Based Antivirus into Thinking Malware Is 'Goodware,'" Vice, Motherboard Tech by Vice, July 18, 2019, https://www.vice.com/en/article/9kxp83/researchers-easily-trick-cylances-ai-based-antivirus-into-thinking-malware-is-goodware.
46. Francis Guibernau and Ayelen Torello, *USENIX Enigma 2020 - Catch Me If You Can!—Detecting Sandbox Evasion Techniques* (USENIX Enigma Conference, 2020), https://www.youtube.com/watch?v=_Oes22LvgtI.
47. Siggi Stefnission, "Evasive Malware Now a Commodity," SecurityWeek, May 4, 2018, https://www.securityweek.com/evasive-malware-now-commodity.
48. Marco De Falco, "Stuxnet Facts Report: A Technical and Strategic Analysis" (Talinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2012), https://ccdcoe.org/uploads/2018/10/Falco2012_StuxnetFactsReport.pdf.
49. *DeepLocker - Concealing Targeted Attacks with AI Locksmithing.* Black Hat, 2020. https://www.youtube.com/watch?v=9g-PllDrJfSU.
50. Ansam Khraisat et al., "Survey of Intrusion Detection Systems: Techniques, Datasets and Challenges," Cybersecurity 2, no. 1 (December 2019): 1–22, https://doi.org/10.1186/s42400-019-0038-7.
51. Jeffrey R. Yost, "The March of IDES: Early History of Intrusion-Detection Expert Systems," *IEEE Annals of the History of Computing* 38, no. 4 (October 2016): 42–54, https://doi.org/10.1109/MAHC.2015.41.
52. James P Anderson, "Computer Security Threat Monitoring and Surveillance" (Fort Washington, PA: James P. Anderson Co., April 15, 1980), https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/ande80.pdf.
53. Yost, "The March of IDES."
54. Hongyu Liu and Bo Lang, "Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey," *Applied Sciences* 9, no. 20 (2019): 4396.
55. Ibid.
56. Ibid.
57. Ibid.
58. Zilong Lin, Yong Shi, and Zhi Xue, "IDSGAN: Generative Adversarial Networks for Attack Generation against Intrusion Detection," *ArXiv:1809.02077 [Cs]*, April 23, 2021, http://arxiv.org/abs/1809.02077.
59. Jackson, "Microsoft."

What Types of Tactical Vulnerabilities Do Future Officers Most Anticipate: *Are Cyber as well as Non-Cyber Threats on their Radar?*

Aryn Pyke, Ph.D.
James Ness, Ph.D.
Major Dave Feltner

ABSTRACT

Modern multi-domain battle involves not only physical threats like IEDs, but also, increasingly, cyber threats. The enemy may jam or intercept communication signals, or hack electronics including navigation systems and drones. Thus, all military leaders - not just signal/cyber specialists - now require some awareness of tactical cyber resources and vulnerabilities. Physical threats come more readily to mind due to their frequency, and because their effects are so salient to the senses. Cyber threats have less historical precedence and are less 'visible' ("out of sight, out of mind"). We developed a task (Problem Anticipation Task: PAT) to gauge the degree to which future Army officers automatically anticipate cyber as well as non-cyber tactical threats. They read a hypothetical mission description and tried to anticipate up to 25 problems that could arise. The mission description explicitly mentioned several cyber-vulnerable components (e.g., radios, navigation systems, drones, biosensors). Yet 39% of these "digital native" participants failed to list a single cyber issue, and only 8% of anticipated issues were cyber-related. The PAT allowed us to assess a baseline regarding our readiness to anticipate cyber vulnerabilities, and can be used in future to assess the effectiveness of training interventions to raise cyber situational understanding.

Keywords: *anticipating tactical cyber threats, cyber situational understanding, cyber readiness, cyber warfare, multi-domain operations*

Aryn Pyke, Ph.D., is a Cognitive Cyber Research Scientist with the Army Cyber Institute and an Associate Professor in the Engineering Psychology Program at West Point. Her doctorate in Cognitive Science provided an interdisciplinary background for the study of cognition (artificial intelligence and modelling, psychology, linguistics, neuroscience). She also obtained BASc and MASc degrees in Electrical and Computer Engineering. Dr. Pyke's research interests include human-computer interaction and teaming, and STEM (Science, Technology, Engineering and Math) education innovations and interventions, especially those involving visuospatial representations. In the cyber domain, Dr. Pyke's focus is on the human in the loop: cyber situational understanding, the impact of affective responses, usable cyber security, and cyber talent management (assessment, training, and retention). To gain insight on human information processing in cyber and educational contexts, she combines behavioral tasks and measures with one or more of neuroimaging, psychophysiological measures (e.g., heart rate, galvanic skin response), eye-tracking and computational modelling and simulation.

Cyber is a Key Domain in Multi-domain Warfare

In the current era of multi-domain warfare, cyber is one of the five key domains (together with air, land, sea, and space). Of the five domains, we view cyber as the one that will most consistently play a role across engagements. Since engagements will not be siloed within a single domain, and will usually incorporate cyber effects,[1] cyber knowledge and situational understanding should not be siloed within particular units or branches (e.g., cyber, signal, and military intelligence). Rather, for the US to be militarily effective, especially against near peer competitors, it has been suggested that every Soldier should be a Cyber Warrior to some extent.[2] The need for such awareness among all military personnel was highlighted when it was discovered that military base locations were being revealed due to the upload of Soldiers' jogging routes recorded by their personal fitness-tracking devices.[3]

Thus, the demands of multi-domain battle raise two related questions: i) how can we assess our Soldiers' level of awareness of cyber vulnerabilities; and ii) how might we further improve it? A main focus of the present research was to develop a method to assess the ability to anticipate potential cyber vulnerabilities in tactical contexts. Without first establishing such a method, it will not be possible to reliably evaluate any training interventions to improve such cyber awareness. The other key objective of the current study was to determine a current baseline level of cyber awareness in a sample of future Army Officers, who will join a variety of different Army Branches. Such a baseline is necessary to gauge our readiness to anticipate possible cyber vulnerabilities in a multi-domain context, and such baseline information is necessary to evaluate the need (if any) for further education and training initiatives to raise cyber awareness among Soldiers in general.

James Ness, Ph.D., is a human factors engineer at the William J. Hughes Technical Center of the Federal Aviation Administration working in modeling and simulations, recently retired from the U.S. Army in the rank of Colonel assigned as Academy Professor, U.S. Military Academy, West Point. He earned the academic rank of full professor in 2016 and upon retirement, he was awarded professor emeritus of the U.S. Military Academy. Before West Point, he served as Command Inspector General, NATO Training Mission/ Combined Security Training Command - Afghanistan. He earned a Bronze Star for his efforts in reforming the Afghan National Military Hospital and establishing an internal assessment program within the Ministry of Interior. Throughout his military career, COL(R) Ness has had varied assignments in human systems integration. Of particular note is his work which led to changes to safety standards by the American National Standards Institute (ANSI) and the International Commission on Non-Ionizing Radiation Protection (ICNIRP) for long-term viewing of near IR laser sources.

Threat-scape Awareness: A Precursor to Situational Awareness

In the heat of the moment, situational awareness,[4,5] involves perceiving those cues in the environment (Observe), that signal potential threats, comprehending their meaning, predicting what may happen next (Orient), deciding what to do (Decide), and then doing it (Act). Due to this Observe-Orient-Decide-Act iterative sequence, the situational awareness process, initially described by John Boyd, is also known as the OODA loop.[6]

A precursor or pre-requisite for situational awareness, however, is typically an advance awareness of the taxonomy of potential threats that might be encountered – what we are calling the threat-scape. To paraphrase Louis Pasteur – "situational awareness favors the prepared mind." Before even entering the tactical context, one should be armed with rudimentary knowledge of the range of potential threats that might occur – including, importantly, cyber threats. This advance awareness of the threat-scape invariably will facilitate a more thorough and nuanced understanding of environmental cues. For example, someone discovering a seemingly inoperable radio (the cue) who did not first anticipate a threat-scape that includes cyber and electronic warfare (EW) might conclude that the device is malfunctioning. Advance awareness allows for another interpretation — that the signal is being jammed. These different interpretations are associated with different implications and courses of action. Presumably, part of the understanding (Orient) phase may involve proactively seeking additional cues to discriminate among multiple possible interpretations of an initial cue.

Readiness and situational awareness for today's and tomorrow's multi-domain battles mandate a threat-scape mindset in military personnel that includes both cyber and non-cyber threats. The current research sought to gauge the degree to which a sampling of future Army officers was armed with this mindset.

Major Dave Feltner, currently a Battalion Executive Officer at 1-508th Parachute Infantry Regiment (Fury From the Sky!) at Fort Bragg, NC. He recently served as Assistant Professor in the Engineering Psychology Program at West Point. His broad research interests include human-computer interaction, cognitive workload, anthropometrics, and biomechanics. He is passionate about arming Soldiers with the right equipment to fight, win, and survive in combat, and has brought experience as an Infantry Officer to bear in research and to help the Army develop, assess, and field optimal equipment.

Why Cyber Vulnerabilities are Not Always Salient in the Threat-scape

As "digital natives," the incoming generation of Army Officers might be keenly attuned to cyber infrastructure issues and vulnerabilities. However, there are several reasons to expect that cyber vulnerabilities may not readily come to mind. First, frequent use of technologies (e.g., computers, cell phones, GPS systems, and the internet of things) does not always equate to familiarity with the inner workings and vulnerabilities of these technologies and their communication signals. Certainly, those who routinely drive cars are seldom familiar with the underlying technology and the diversity of possible ways a car might fail. Second, the wireless communications signals that support modern warfare and travel to and from radios, satellites, drones, cell towers, Wi-Fi hubs, biosensors, et cetera, are invisible. In comparison to visible/tangible targets (e.g., Soldiers, convoys, and bases), which are vulnerable to kinetic attacks, the invisible communication signal vectors for cyber-attacks are, quite literally, out of sight, and often, therefore, out of mind.

Additionally, as the expansion of cyber's importance as a warfare domain is relatively new, cyber-related threats often do not feature in the war stories and scenarios shared by military instructors and mentors. Cyber threats often are omitted in the scenarios encountered in virtual training simulations like Virtual Battle Space (VBS). That said, Service Academies provide academic courses and majors in areas such as computer science, electrical engineering, and cybersecurity that could shed light on vulnerabilities related to the inner workings and wireless signaling of computing and telecommunications equipment, and thereby contribute to cadets' cyber awareness. There may be some limitations to the impact of such academic instruction, however. First, not all students choose to major in such areas (from 2017 to 2021, only about 7% of graduating West Point cadets had majors within computer science

or electrical engineering). Furthermore, although some coverage of information technology is included in the core curriculum taken by all cadets, these academic courses may seldom highlight the use and vulnerabilities of such technology in tactical contexts.

The Present Research

In the current research, we developed and applied a Problem Anticipation Task (PAT) to gauge the degree to which future officers automatically anticipate cyber along with non-cyber threats in tactical contexts. To gauge the diversity and frequency of the types of tactical issues anticipated, our sample of cadets — all "digital natives" — read a description of a hypothetical tactical mission and were asked to anticipate up to 25 possible problems that could arise. Due to the salience challenges discussed above, we expected that participants would anticipate far fewer (if any) cyber issues than non-cyber issues.

For each issue they anticipated, they were asked whether they just thought of it themselves or if they had heard about a similar issue during class, in the news/social media, or via word of mouth. Our hope was to get some insight into the sources of cadets' awareness of tactical cyber versus physical threats. In this vein, we also sought to test whether juniors/seniors were likely to list more cyber issues than freshman/sophomores, given their greater exposure to course work and military training and mentorship. We also sought to investigate whether Science, Technology, Engineering, and Math (STEM) majors were more likely to list cyber issues than non-STEM majors.

To increase the chances that participants would anticipate cyber issues, mission descriptions explicitly mentioned cyber-vulnerable components (radios, navigation systems, biosensors, satellites, drones, cell phones). Our coding scheme categorized responses into three main types of issues: i) non-cyber issues (e.g., equipment malfunction, physical attacks by enemy); ii) cyber issues (e.g., hacking or signal jamming by enemy) and iii) non-cyber information technology/telecommunications (ITT) issues. Non-cyber-ITT issues are those that involved a possible cyber vector like a radio or drone, but the anticipated problem was not due to a cyberattack but rather from other factors such as weather or terrain-caused signal transmission issues. Segregating non-cyber-ITT from cyber and non-cyber issues helped us get a sense of the participant's awareness of unit reliance on equipment that typically is vulnerable to cyberattacks (e.g., cell phones, radios, GPS systems, drones etc.). If some participants list non-cyber-ITT issues but no cyber issues, this will suggest that they are mindful of some intrinsic imperfections and malfunctions associated with communications and digital equipment, but not as mindful of the possibility of deliberate cyberattacks.

METHOD

Participants

West Point Cadets (N = 79; 34% female; mean age: 19.7 years, SD = 1.9 years) received course

credit for participating. These individuals are slated to become U.S. Army officers. Two were seniors, 20 were juniors, one a sophomore, and 56 were freshmen who had almost completed their second semester. In all, 51% were Social Science/Humanities majors and 49% were STEM majors. Sample demographics should reflect the population demographics at the Academy (69% White, 14% African American, 9% Hispanic, 8% Asian, and less than 1% American Indian/Alaska native or other).

Materials

Participants read one of two brief hypothetical mission scenarios, Mission X (311 words) or Mission Y (313 words), (see Appendix 1). Mission X entailed travel to meet with a leader of a local friendly faction and Mission Y was setting up an observation post. Mission descriptions included a sequence of events, modes of transportation, equipment, references to the enemy, supplies, Soldier health, weather and terrain. Such elements in missions can serve as vectors which are subject to attack or other vulnerabilities. The equipment included information transmission, reception and/or storage: radios, cell phones, biosensors, drones, satellites, databases, and GPS devices (e.g., Blue Force Trackers). Such equipment (and/or associated wireless signals) are all vulnerable to cyberattack.

Procedure

The procedure was implemented on-line via the Qualtrics platform. Stimuli and questions were presented on the screen as black text on a white background. A random number generator was used to assign participants to read either Mission X (N = 44) or Mission Y (N = 35). Prior to the display of the mission description subjects were instructed: *"As a military leader it is important to be able to anticipate (and ultimately plan for) possible things that could go wrong on a mission. Next, you'll read a paragraph describing a hypothetical tactical mission. As you read it, try to consider various possible kinds of problems that might arise."* The mission description was then presented on the screen for the participant to read (self-paced), with reminders at the bottom of the description to consider the full range of different problems that might occur, and that even low-probability possibilities were welcome. We refer to our task as the Problem Anticipation Task (PAT). Participants were asked to foresee at least 12 possible problems that might arise, but they had the opportunity to enter as many as 25.

For each possible problem the participant identified, they were asked to describe both the problem and its underlying cause. Requiring the underlying cause ensured that the participant provided sufficient detail to categorize/code the issue. For example, if a possible problem was that the informant could not be contacted – this issue would be coded differently if the cause was: i) a broken cell phone (equipment malfunction); versus ii) the cell signal being deliberately jammed by the enemy (cyber enemy action); versus iii) the informant being killed by the enemy (kinetic enemy action). Participants were also asked to state whether they had heard of their listed issue from the following possible sources: i) in class; ii) news/social media; iii) word of mouth; or iv) just thought of by themself. The procedure took approximately 30 minutes.

Data Coding Procedure

The issues participants listed were each coded according to a two-level scheme involving a type and a subtype. The three main types of issues were: cyber (e.g., radio signal being jammed by enemy); non-cyber-ITT (e.g., radio malfunctioning); and (other) non-cyber (e.g., vehicle breakdown). Cyber problems are those deliberately caused by the enemy (offensive cyber/EW operations), and typically affect equipment vulnerable to cyber threats, including radios, GPS/BFTs, cell phones, drones, biosensors, etc. The non-cyber-ITT category sought to capture cyber-vulnerable equipment problems not caused by enemy cyber operations. Within the cyber type, subtypes of issues included jamming, tapping/tracking of signals, altering information in signals/databases, destruction, or incapacitation of cyber or communications infrastructure, cyber-induced kinetic effects and other. Subtypes for the non-cyber and non-cyber-ITT issues included, among others: equipment malfunction/damage/loss; supply issues; enemy actions (other than cyber/EW); health issues; and issues with weather and terrain. The full coding scheme is summarized in Table 1. Each participant response (anticipated issue) was coded by two independent coders (one military, one civilian) and all discrepancies were resolved in discussion.

Table 1: Coding scheme to categorize anticipated issues by type and subtype

Type	Subtype	Description
Cyber	Jam	Enemy jams signal (e.g., radio, gps)
	Tap/Track Signal	Enemy detects your signal (location) &/or intercepts information
	Alter Information	Enemy alters your communication signals/databases (e.g., to insert false information/ messages/commands)
	Destroy/Hamper Infrastructure	Enemy destroys/hampers cyber/communications infrastructure (e.g., radio/cell towers, satellites)
	Kinetic Effects	Enemy hacking produces kinetic effects (e.g., allows them to overheat or control physical actions of equipment like drones & autonomous systems in vehicles)
	Other	This other category was not actually needed/used
Non-cyber-ITT	(subtypes overlap with non-cyber subtypes below)	Issues with cyber-vulnerable equipment (e.g,. radios, GPS, cell phones, drones) that aren't caused by enemy cyber/EW operations
Non-Cyber	Enemy-Induced	Enemy spots or attacks you (or allies/informants) or moves to a location you were going to use/traverse (e.g., ambush, IED, any injury/fatality/equipment damage caused by enemy)
	Malfunction/Loss of Equipment	Equipment malfunction/breakdown/damage/loss (not caused by enemy)
	Plan	Problems with initial plan or a change of plan
	Supply Issues	Run out of something (gas, bullets, water etc.)
	Health Issues	Health issues not caused by enemy (e.g., fatigue, illness, injury, overheating)
	Personnel/Training Issues	Inadequate training/human error, poor communication, cultural faux pas, infighting, insubordination, disobedience, toxic leadership, AWOL, traitors...
	Intelligence	Incorrect/incomplete intelligence about enemy, or enemy has intelligence on you (without specifying a cyber means of obtaining such intelligence).
	Weather/Terrain/Transmission	Weather or natural terrain affects cover or visibility or signal transmission, or affects travel (e.g., rain washes out a bridge)
	Locals	Local civilians or informants/alleged allies acting against you or compromised or endangered

Participants sometimes listed more than one type and/or subtype of problem in a single entry, e.g.,

Issue: Can't use cell; Cause: No service due to terrain or enemy is jamming it.

Such entries were split into two:

Issue 1: Can't use cell; Cause1: No service due to terrain.

Issue 2: Can't use cell; Cause2: Enemy is jamming it.

For Issue 1, the type is non-cyber-ITT (involving a cyber-vulnerable vector, a cell phone) and the subtype is weather/terrain. For Issue 2, the type is cyber, and the subtype is jamming. When instances were split as exemplified above, both issues inherited the source(s) identified in the original entry. In a few cases (4 cases = 0.4% of trials), a subject listed the same issue twice or listed an issue so broad/vague it could not be specifically coded. In such cases we excluded the issue from our analyses.

RESULTS

Number of Issues Anticipated by Type

Participants averaged 14.4 issues each for a total of 1140 issues generated (not all distinct). Notably, 39% listed no cyber issues whatever. Of the issues identified, 91.8% were non-cyber issues (to include 27.2% non-cyber-ITT), and cyber issues totaled only 8.2%. Figure 1 displays the percent breakdown of issue types and, within each type, the breakdown by subtype.

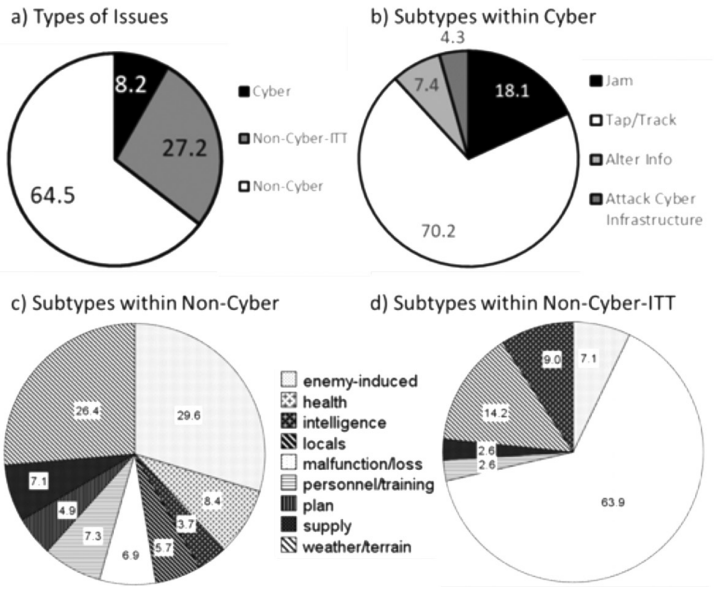


Figure 1. Breakdown of anticipated issues: a) by type; b) by subtypes within cyber; c) by subtypes within the non-cyber-ITT; and d) by sub-type within the non-cyber-other type.

The sample of Computer Science/Electrical Engineering majors was insufficient to allow meaningful comparison with that subgroup specifically, but we did examine whether STEM majors were more likely to list cyber issues than non-STEM majors, and whether juniors/seniors were more likely to list cyber issues than freshmen/sophomores, given their greater exposure to course work and military training and mentorship. For each type of issue (cyber, non-cyber-ITT, non-cyber), we performed a 2 (college level: freshmen/sophomores vs. juniors/seniors) X 2 (type of major: STEM vs. non-STEM) analysis of variance (ANOVA) on the number of potential issues raised by each participant. As summarized in Table 2, the analysis revealed no significant differences by college level nor by major (STEM vs. non-STEM), nor any significant interactions between the two variables. Thus, in this sample at least, there is no significant evidence of significantly increased ability to anticipate more cyber threats (nor more physical threats) among older cadets nor among STEM majors.

Table 2: Mean number of issues listed (per participant) for each type by college level and major.

Issues	Cyber		Non-cyber-ITT		Non-cyber-ITT		Cyber Infrastructure	
College Level	Non-STEM	STEM	Non-STEM	STEM	Non-STEM	STEM	Non-STEM	STEM
Freshman/	1.2	1.2	4.1	4.0	9.2	10.1	14.4	15.2
Sophomores	1.3	1.3	3.5	3.9	8.9	7.7	13.5	12.9
Statistics	**Note: All statistical comparisons failed to reach significance**							
Main effect: College Level	$F(3,75)=0.04$, $p=.845$		$F(3,75)=0.43$, $p=.512$		$F(3,75)=2.39$, $p=.126$		$F(3,75)=3.15$, $p=.080$*	
Main effect: Major	$F(3,75)=0.02$, $p=.893$		$F(3,75)=0.10$, $p=.749$		$F(3,75)=0.04$, $p=.845$		$F(3,75)=0.01$, $p=.937$	
Interaction	$F(3,75)=0.16$, $p=.689$		$F(3,75)=0.21$, $p=.649$		$F(3,75)=1.55$, $p=.217$		$F(3,75)=0.65$, $p=.423$	

** Significant p-values are those <.05, Freshman/Sophomores listed marginally (p<.1) more issues overall (but not in cyber) than Juniors/Seniors.*

Cyber Threats Anticipated: Subtypes and Vectors

Figure 1 illustrates that the most common subtype of cyber issue anticipated was that the enemy would tap or track a signal (70.2% of cyber issues raised), which corresponds to compromising the *confidentiality* aspect of cybersecurity. The next most anticipated issue was an enemy jamming a signal (18.1%), compromising *availability*. The third most anticipated issue was the enemy-alteration of a signal or stored/displayed information (7.4%), which corresponds to the information *integrity* aspect of cyber security. Fourth was an enemy physically destroying cyber infrastructure (4.3%), which, like signal jamming, also relates to information *availability* (for a total of 22.4% availability issues). Our pre-experimental coding scheme also included a code for a cyberattack with kinetic effects (e.g., enemy hacking a drone and directing it to fly into a friendly Soldier or vehicle), but our participants did not list any such examples. In terms of which vectors (e.g., pieces of equipment, signals) were most anticipated as cyberattack targets, the most frequently mentioned was a cell phone, followed in order by the GPS, the radio/comms, and the drones and biosensors.

Table 3 associates different vectors (e.g., pieces of equipment) with the distribution of subtypes of issues that cadets anticipated might arise for that vector. Note, the unbracketed percentages are percentages just within the subset of issues associated with a particular vector (column). For example, issues with drones (N=58) amounted to 5% of the total cyber and non-cyber-ITT issues. Only 15% of the 58 issues associated with drones were cyber issues, and the rest were non-cyber-ITT issues (e.g., equipment malfunction).

Table 3: Percent of anticipated cyber (grey background) and non-cyber-ITT (white background) problems associated with different pieces of cyber-vulnerable equipment.

Issues	Drone	Navigation System	Bio-sensor	Radio/Comms	Cell Phone	Cyber Infrastructure
Number Issues	N=58	N=99	N=64	N=78	N=86	
Cyber						
Jam	None	3% (18%)	5% (18%)	8% (35%)	6% (29%)	n/a
Tap/Track	5% (5%)	16% (24%)	9% (9%)	13% (15%)	36% (47%)	n/a
Alter Info	5% (43%)	4% (57%)	none	none	None	n/a
Kinetic Effects	none	none	none	none	None	n/a
Attack Cyber Infrastructure	5% (75%)	n/a	n/a	n/a	n/a	1% (25%)
Total Cyber	15%	23%	14%	21%	42%	1%
Non-Cyber-ITT						
Enemy (spots/damages)	22%	1%	2%	none	1%	(coded as cyber)
Malfunction	17%	62%	77%	58%	34%	n/a
Supply/Batteries	none	1%	none	8%	1%	n/a
Weather/Terrain	9%	9%	3%	10%	21%	n/a
Personnel/Training	none	2%	5%	1%	none	n/a

Note: Un-bracketed percentages reflect responses of that subtype within that column (equipment type), and percentages in round brackets are the percentages of that subtype within that row.

Non-Cyber Threats Anticipated: Subtypes and Vectors

Part (c) of Figure 1 above breaks down the subtypes of non-cyber issues listed by participants, to show the percentage of issues in terms of the most common attack surfaces and/or aspects implicated: route/visibility (31.0%), Soldiers (21.9%), local informant/ally (12%), plan/preparation/support (9.8%), vehicles (8.6%), weapons/ammunition (4.1%), and other equipment (1.6%).

Sources of Participants' Ideas about Possible Issues: Were any mentioned in class?

For each issue flagged, cadets were asked to identify whether they had previously heard of this possible issue by checking all that applied from the following possible sources: i) classroom; ii) news/social media; iii) word of mouth; or iv) thought of by the cadet without outside prompting. The data were coded so that unprompted issues were those where only that source was checked and no other. It is hard to claim that you just thought of something yourself if you also stated that you had heard it mentioned in class, and/or in the news or social media, and/or

via word of mouth. Figure 2 shows the proportion of participants who cited each possible source for the issues they listed by type (cyber, non-cyber-ITT and non-cyber). Since only 61% of participants listed a cyber issue, values in the cyber category can't exceed that percentage.

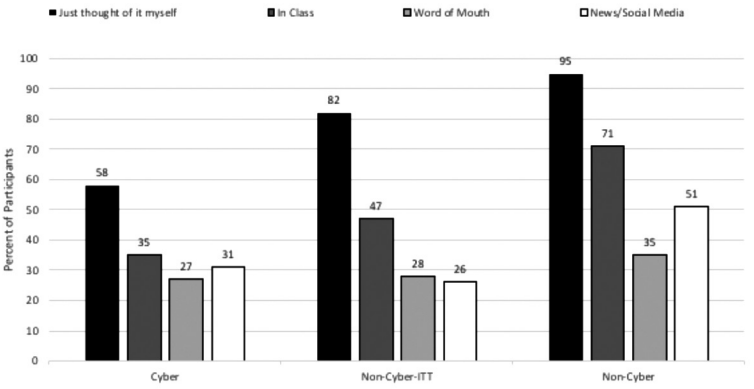


Figure 2: Percent of participants citing various (non-exclusive) sources for anticipated issues, separated by issue type.

For several reasons we predicted that cadets might anticipate fewer cyber issues. First, they have less historical precedent than non-cyber issues, and may be less likely to be mentioned in class or via word of mouth by military mentors. In contrast to the 71% of participants who attributed anticipating one or more non-cyber issues to in-class exposure, only 35% of participants attributed anticipating a cyber issue to in-class exposure. Word-of-mouth attributions were also lower for cyber than non-cyber issues. Second, not all students are familiar with the workings of cyber technology, which renders 'invisible' cyber threats more abstract and hence more difficult to picture than, say, an explosion. This view is consistent with our finding that, compared to the 95% who came up with non-cyber issues themselves (without exposure to any external source), only 58% reported coming up with a cyber issue themselves.

DISCUSSION AND CONCLUSION

In this research we developed a methodology to assess a type of cyber awareness relevant to multi-domain battle - i.e., the ability to anticipate both cyber and physical vulnerabilities in a tactical context, because situational awareness on today's battlefield demands both. It is necessary to be aware, in advance, of the types of problems that could occur (Threat-scape Awareness), as preparation to be aware of cues in the heat of the moment that a particular problem might be occurring right now (Situational Awareness).

Overall, only 8% of anticipated problems were cyber related, and 39% of participants anticipated no cyber issues at all. Thus, despite our subjects being "digital natives," potential cyber issues were not even on the radar for many of these future Army officers. That said, being digital natives likely did facilitate cadets' ability to anticipate non-cyber-ITT issues like malfunction,

human error, and battery supply associated with equipment like radios, drones, cell phones etc. Our results are compatible with research on mobile device use in civilian contexts, which suggests that many digital natives lack high cyber security awareness,[7] and they need education and/or training to inculcate cyber security awareness.

In terms of education and training, a surprising finding – and concern - is that, in this sample at least, neither older cadets nor STEM majors evidenced an increased ability to anticipate more tactical cyber threats. West Point is increasing opportunities for both curricular and extra-curricular exposure to cyber-related content. In terms of the curriculum, all cadets, regardless of major, must take two core internet technology courses, and a 3-course engineering sequence, and one of the six options is Cyber Engineering. The Department of Computer Science and Electrical Engineering offers three majors for interested cadets: Computer Science, Electrical Engineering, and a recently added Cyber Science Major. A Cyber Engineering Minor is also offered. Several other departments have also offered cyber-related elective courses (e.g., Cyber Policy, Cyber Law, Cyber History), which are often developed and/or taught by faculty from the Army Cyber Institute. In addition, extra-curricular opportunities include a cyber leader development program where cadets may earn a cyber skill identifier, as well as several cyber-related clubs and teams, e.g., the Cadet Competitive Cyber Team (C3T), Cyber Policy Team, Esports Team, Electrical Engineering Systers Club, Amateur Radio Club, Electronic Experimenters' Group, Association for Computing Machinery Student Chapter (ACM-SIGSAC), and more.

We expect that West Point is not unique among the service academies in offering such opportunities, yet it would not surprise us to learn that our counterparts also may come up short in ready awareness of potential tactical cyber threats and vulnerabilities. Again, we envision two plausible reasons for this. First, beyond core required internet/cyber courses, not all students will engage with the available opportunities. Second, academic courses on cyber-related content may not touch on tactical cyber threats and vulnerabilities. An example of an exception at West Point was an engineering psychology colloquium on Human-Computer-Interaction, developed and taught by the second author, which involved brainstorming and story-boarding ways to include cyber threats into scenarios in a video-game-like military training simulation platform called Virtual Battle Space (VBS). Due to faculty turnover and availability, however, specialty and elective courses may not always be systematically available.

Beyond the academic curriculum, tactical cyber issues could be more directly addressed in the military instruction and training components of the cadet experience. We acknowledge that only two cadets in our sample were seniors, and further, that their post-graduation level of awareness of cyber and EW threat vectors could be enhanced by branch Basic Officer Leader Course (BOLC) training. That said, we suspect that many BOLC courses for non-cyber officers may include minimal cyber content, and so it is an open question whether a Problem Anticipation Task (PAT) administered post-BOLC would yield results much different from those reported here.

Recommendations and Future Work

An obvious extension of the current work would be to apply our PAT methodology to gauge tactical cyber awareness in other services and stages of training or career development. In the Army, this could include, for example, before and after each institutional professional education course (e.g., BOLC and ILE: Intermediate Level Education). Beyond assessing current awareness, the PAT can also be used as a pre-/post-test to assess the effectiveness of inserting additional cyber content into professional military education courses.

More narrowly, within the West Point context, a core required cyber course or military instruction course could be modified to include a section on tactical implications of cyber threats and vulnerabilities, to ensure exposure for every student. One could take a training approach and explicitly spell out several specific examples (i.e., give someone a fish). Or, taking a more educational approach, we could provide students an example and encourage them to apply and generalize their (non-tactical) cyber knowledge to generate other potential cyber issues (i.e., teaching them to fish). This could be done in the context of the task used in this study (PAT). Research indicates that students better retain/recall content they helped to generate versus content that was presented to them.[8,9] Participants engaged in this generation process in the current study when they reported the source of their issue idea as "just thought of it myself." Beyond the benefits of better retention/recall (of known threats), this generation process is crucial to enabling anticipation of potential novel/future threats that could emerge in the evolving, multi-domain context of modern warfare.

The "invisible," and hence more abstract nature of cyber threats will always be a challenge. To ameliorate this, the military is actively researching and developing interfaces to better support cyber understanding for leaders. Such interfaces might visually represent not only the physical assets and aspects of an area but also, potentially, cyber resources, signals and interconnectivity. Visual representations might also support better understanding for students in the classroom. This is an area for continued, on-going research.

APPENDIX 1: PARAGRAPH DESCRIPTIONS OF HYPOTHETICAL MISSIONS

Mission X: The goal of your Platoon (PLT) is to meet with a leader of a US-friendly faction in the region. You'll start at a Forward Operating Base (FOB). After a quick medical check, you will travel 65 miles via Stryker ground vehicles to the meeting point. The current forecast predicts good weather. Your planned route will take advantage of the local roads and bridges, but to avoid engagement, your route will detour around regions that seem to be occupied by hostile forces - based on reconnaissance images transmitted wirelessly by Drones. Thus, you will detour across a river to travel 25 miles on the far side and then cross back again. In addition to rations, each Soldier in your unit will still carry an M4 with a full ammo load, and the Strykers will be equipped with machine guns and a 60mm Mortar system. Each Stryker is also equipped

with a Situational Awareness Navigation system (Blue Force Tracker: BFT), which has GPS and satellite communication capabilities and displays a route map with information on your position, destination, the positions of other vehicles in your unit, and expected positions of the enemy forces based on the most recent intel. There are actually two possible meet locations (A and B). When your unit is about 20 minutes out from the meet, you (the PL) will contact the local faction leader via cell phone to determine which meeting site to use. You will then communicate this information by radio to members of your PLT in the other Strykers and to company HQ. When you arrive at the final meet site, you and the Platoon Sergeant (PSG) will dismount the Stryker to walk across the clearing to meet the local leader. Your PLT and company HQ can still monitor your well-being remotely because all Soldiers will be equipped with biomedical sensors that track their vitals and position.

Mission Y: The goal of your Platoon (PLT) is to set up an observation post to detect enemy movements along a particular route. You will start from a forward operating base (FOB). After a quick medical check, and after packing rations, observation equipment, M4s and a full ammo load, your unit will be flown at night by C-130 aircraft to parachute into an area several miles from your destination. This should minimize the likelihood that hostile forces will detect your movements. You will then navigate on foot using satellite-enabled GPS to a site on a ridge overlooking the route to be observed. The GPS will provide a route map with information on your position, destination, and the positions of other members in your unit. Your ruck to the ridge will involve crossing a riverbed that should be dry at this time of year. Your observation site on the ridge was selected based on images transmitted wirelessly by Drones that indicate that it is not occupied by enemy forces and will provide you with ample cover due to rock formations and vegetation. It should also provide an excellent line of sight to the target route if the good weather/visibility holds. If enemy movement is detected along the target route, you'll immediately communicate this information via radio to company HQ at the FOB. You also have a cell phone which can allow you to receive intel from a local informant who can give you advance warning if your position has been compromised or if the enemy is making unexpected movements in the region. Besides keeping watch from the observation post, you will also periodically send a squad out to do a foot patrol of the area. The PLT and company HQ can monitor the well-being of Soldiers on patrol because all Soldiers will be equipped with biomedical sensors that track their vitals and position.

DISCLAIMER

The views expressed here are exclusively those of the authors and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, or the Department of Defense. Correspondence concerning this article should be addressed to Aryn A. Pyke, Army Cyber Institute, 2101 New South Post Rd, U.S. Military Academy, West Point, NY 10996. Email: aryn.pyke@westpoint.edu.

NOTES

1. Bruce Schneier and Tarah Wheeler, “Hacked drones and busted logistics and the cyber future of warfare”. TechStream, June 4, 2021, https://www.brookings.edu/techstream/hacked-drones-and-busted-logistics-are-the-cyber-future-of-warfare/.
2. Christopher J. Heatherly and Ian Melendez. "Every soldier a cyber warrior." *The Cyber Defense Review* 4, no. 1 (2019): 63-74.
3. Jeremy Hsu, “The Strava Heat Map and the End of Secrets.” *Wired*, January 9. 2018, https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/.
4. Mica R. Endsley, "Measurement of situation awareness in dynamic systems." *Human factors* 37, no. 1 (1995): 65-84.
5. Mica R. Endsley, "Design and evaluation for situation awareness enhancement." In *Proceedings of the Human Factors Society annual meeting*, vol. 32, no. 2, 97-101, Los Angeles, CA: Sage Publications, 1988.
6. Chet Richards, “Boyd’s OODA Loop” *NECESSE* (Royal Norwegian Naval Academy Monographic Series), February 11, 2020, https://fhs.brage.unit.no/fhs-xmlui/bitstream/handle/11250/2683228/Boyds%20OODA%20Loop%20Necesse%20vol%205%20nr%201.pdf?sequence=1&isAllowed=y.
7. Vasileios Gkioulos, Gaute Wangen, Sokratis K. Katsikas, George Kavallieratos, and Panayiotis Kotzanikolaou, "Security awareness of the digital natives." *Information* 8, no. 2 (2017): 42.
8. Norman J. Slamecka and Peter Graf, "The generation effect: Delineation of a phenomenon," *Journal of Experimental Psychology: Human Learning and Memory* 4, no. 6 (1978): 592.
9. Aryn A. Pyke and Jo-Anne LeFevre, "Calculator use need not undermine direct-access ability: The roles of retrieval, calculation, and calculator use in the acquisition of arithmetic facts," *Journal of Educational Psychology* 103, no. 3 (2011): 607.

Rethinking US Concepts and Actions in Cyberspace:

Building a Better Foundation for Deterring China's Aggression

Major Travis "TJ" Siemion

ABSTRACT

China's use of cyberspace is a significant threat to US relative power in an inherently dangerous and anarchic international system. Despite the clear threat, the US limits its own deterrent potential by maintaining a narrow view of cyberspace, applying a restrictive understanding of cyber attribution, and conceding to the influences of its own strategic culture. By prioritizing deterrence over other competing interests, while also adopting a broader view of the domain and a more stratified view of cyber attribution, the US can improve its ability to take the type of consistent, credible, and decisive action needed to deter China's aggression in cyberspace.

When Thucydides wrote of envisioned dialogue between the Athenians and the Melians, in 400 B.C, one cannot help but wonder whether he knew his words would influence thinking on power and conflict for centuries. A single quote from this Athenian general can be claimed the very progenitor of international relations theory: "The strong do what they can, and the weak suffer what they must."[1] This anarchic nature of the international political system creates an inherent danger and drives states to concern themselves primarily with power and security.[2] While the realities of the 21st century have not changed this natural tension between states, they have changed the tactics and strategies states employ. Between great powers, nuclear weapons offer no realistic positive political objective, and the utility of traditional military force has been reduced due to the perceived risk of escalation

MAJ Travis "TJ" Siemion is a recent distinguished graduate of the Air Command and Staff College, receiving a master's degree in Military Operational Art and Science. After enlisting in the U.S. Army in 2001, he deployed to Iraq in 2003 as a paralegal specialist focused on operational law and criminal justice. He graduated as Dean's Distinguished Graduate and Distinguished Military Graduate from the University of Texas at Austin, commissioning as a Military Intelligence officer. After commanding a counterintelligence detachment, he deployed with Special Operations Joint Task Force-Afghanistan in 2014. Joining Cyber Branch shortly after, he served on a National Mission Team and commanded a cyber company in the 780th MI Brigade, followed by Aide-de-camp to the Commanding General of the Cyber Center of Excellence, and Capability Developer for the Persistent Cyber Training Environment. He is currently the Chief of Cyber/EW Modernization in the Department of the Army Management Office for Strategic Operations.

to nuclear war.[3] This has resulted in an expansion of competition below the level of armed conflict. Cyberspace has catalyzed and accelerated this type of competition. China has adapted to this reality faster than the United States (US), stealing trillions of dollars in intellectual property (IP) from America's commercial industries and research and development (R&D) from its defense industrial base.[4] Despite this demonstrated and significant threat to its relative power, the US limits its own deterrent potential by maintaining a narrow view of the cyberspace domain, applying a restrictive understanding of cyber attribution, and ceding to the influences of its own strategic culture. By prioritizing deterrence over competing interests, while also adopting a broader view of the domain and a more stratified view of cyber attribution, the US can improve its ability to take the type of consistent, credible, and decisive action needed to deter Chinese aggression in cyberspace.

THE CHINA THREAT

Before discussing the nuances of deterrence, cyberspace, or deterrence in cyberspace, it is prudent to clearly articulate the behavior to be deterred. Certainly, any deterrence strategy should account for the unique motives, costs, and risks of specific undesirable adversary behavior. For example, Russian state-led efforts to destabilize US institutions and manipulate the electorate involve benefits, costs, and risks that are distinct in scope, scale, and influence when compared to a non-state actor's relatively simplistic employment of ransomware to obtain economic resources. To influence an adversary's decision calculus and deter undesirable behavior, deterrence strategies should be deliberately catered to these unique considerations. The question is, then: Of the myriad ways China uses cyberspace in the pursuit of its national interests, what specific behavior should the US seek to deter?

China's laws, policies, and actions indicate three overarching priorities in cyberspace: domestic control and regime stability, espionage, and access to technology.[5] The worldwide expansion of the Internet toward the end of the 20th century was largely shaped by the West. The thinking amongst the technological elite was that expanded connectivity, access to information, and unrestricted digital speech would have a liberalizing influence on the world, tempering and marginalizing authoritarian rule. Unfortunately, China quickly recognized the Internet's potential for unregulated free speech and uncontrolled proliferation of information, which the Chinese Communist Party (CCP) viewed as existential threats to party security, control, and legitimacy.[6] In response, by implementing measures such as the "Great Firewall," as well as state-leveraged intermediary liability and a state-controlled information technology industry, the CCP has managed to turn the Internet into a massive tool of domestic surveillance and censorship.[7] While this state behavior is at odds with the values of American democratic society, it should not be the primary focus of deterrence.

China's second priority in cyberspace, espionage, is complicated by matters of moral authority and legitimacy. The US, having significantly shaped and influenced the current rules-based international order, is committed to the norms and laws of the system and seeks to maintain international support through action that is consistent with its principles. James Clapper, then Director of National Intelligence, stated in 2015 that in cyberspace "there is a difference between an act of espionage, which we conduct as well, and other nations do, versus an attack."[8] This recognition that the US conducts cyber espionage tacitly acknowledges the legitimacy of espionage in cyberspace. It also tangentially supports both the idea that espionage is a sovereign right and the belief that espionage has a fundamentally stabilizing influence in the international system, as improved awareness of adversary capabilities can temper expectations of benefit from the use of force. While the US should expect states to continue cyber espionage, a policy of deterrence would be manifest hypocrisy.

We then consider China's third priority in cyberspace—access to technology. China has demonstrated an extensive willingness and ability to exploit and access public and private networks worldwide in the pursuit of information and IP, particularly defense-related or technologically innovative R&D.[9] China's IP theft should not be dismissed as merely a private sector or economic concern. The U.S. National Counterintelligence and Security Center emphasizes this in its 2018 annual report, depicting foreign economic and industrial espionage as a significant threat to US prosperity, security, and competitive advantage.[10] China's ability to reap the benefit of massive American investments in military and commercial R&D diffuses US relative power within the international system. It also allows China to negate one of the most consequential competitive advantages of America's democratic, capitalist system over China's authoritarian, state-planned economy—the innovative forces of economic incentive in an open-market system.[11]

The US has been slow to realize, and slower still to respond to, the gravity of the threat posed by China's theft of IP. The speed and operational tradecraft, as well as the breadth and diversity of targets involved, strain Washington's ability to appreciate the scope and scale of the collective impact to US national interests. For the sake of comparison, the military is quite proficient at contextualizing the direct, tangible threat that adversary military forces pose to national security. Weapon system ranges, hypersonic weapon speeds, operational reach, and force projection are all relatively easily understood and measured concepts that translate well to traditional conceptualizations of threats to national security. What is more difficult to measure, and thereby contextualize in degree and severity of vulnerability and effect, is the cumulative impact of comparatively abstract grey zone threats and attacks that target the intersection of security and other national interests.

For example, Russian social media disinformation and misinformation efforts target a state's national psyche, polarizing the electorate and undermining a democratic state's ability to achieve political and social consensus by exploiting the seams among freedom of speech, freedom of the press, and national security. Chinese IP theft exploits a different vulnerability: the seams among national security, commercial enterprise, and economic prosperity. When adversaries target these seams, they create not only uncertainty about the extent of what is happening but also an inability or unwillingness to coordinate and execute the type of assertive, credible, associative, and timely national response needed to achieve deterrence. Yet, purely with respect to economic prosperity and relative power, the collective costs of cyberattacks may very well compete with or outweigh the net costs of any war in US history.

CYBERSPACE: UNDERSTANDING THE PHENOMENON

To improve the conceptual foundations needed to deliver policies and strategies that could realistically create the conditions needed for deterrence, the US must first expand how it views the phenomenon of cyberspace. Throughout much of the 21st century, the government and military communities debated the question of whether or not cyberspace is a domain of warfare, equal in status and warfighting significance to the maritime, land, air, and space domains.[12] This particular question appears to be at least partially resolved, with the military's position apparent in its definition of "cyberspace" in Joint Publication 3-12: "the *domain* [emphasis added] within the information environment that consists of the interdependent network of information technology (IT) infrastructures and resident data."[13]

A myopic focus on the military aspects of cyberspace is insufficient for the US to pursue and defend its national interests. While cyberspace certainly creates opportunities and vulnerabilities during war, it also offers US enemies a low-cost opportunity to pursue their strategic interests during peace, entirely negating the coercive and deterrent influences of US economic and military might. This ability of a state or an individual actor to pursue their interests through cyberspace, unthreatened and unimpeded by any relative power asymmetries that

exist, suggests that the environment should not be thought of as the "fourth military offset," but as an international relations *offset*.[14] The figure below depicts cyberspace not merely as a military domain, but a broad spectrum, while also highlighting the relatively small portion of cyberspace where the military primarily operates.

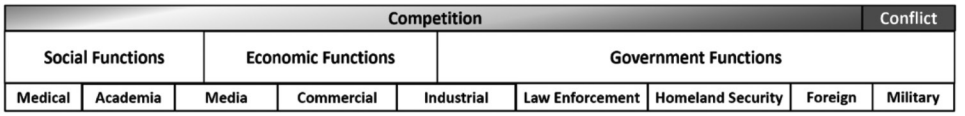


Figure 1: Cyberspace as a spectrum of geopolitical competition and conflict.

Cyberspace is not a domain where national business is conducted, and national interests are pursued in isolated silos. Instead, the US must view cyberspace as a broad and interconnected spectrum that supports and enables the sources and instruments of national power across the entire continuum of competition to conflict on a geopolitical—***not*** just a military—battlefield.

Yet, the continued evolution of war, and therefore the military instrument of national power, has resulted in a US military that performs functions and duties that go well beyond traditional armed conflict. From nation-building, including the construction of schools and hospitals or training of judges and politicians in Afghanistan, to humanitarian assistance, disaster recovery, and agricultural development in Africa, the military is no longer a simple hammer, but has become a geopolitical multi-purpose tool.[15] However, while the modern US military is capable of far more than applying conventional force in the pursuit of political objectives, this does not change the fact that it is still built primarily for war. This belligerent purpose not only influences military culture, recruitment efforts, virtues, and norms, but drives how the military trains and disciplines itself, educates its leaders, and is entirely deterministic in how it identifies, prioritizes, develops, and acquires its capabilities. War is not merely what the military plans for but shapes the very process that the military uses *to plan*.

Within game theory, a finite game is one in which either the rules of the game or the incentives of the players serve to ensure that the game ends with clear winners and losers. Since nations in an armed conflict seek or are generally incentivized to end the conflict, a declared period of war is a finite game. Geopolitical competition between the US and China, however, is an infinite game, since it is reasonable to assert that neither party is sufficiently incentivized realistically to seek a permanent and definitive culmination of the competition.[16] Instead, both parties seek to establish and exploit their own competitive advantages while avoiding or negating their opponent's comparative strengths. Understanding the temporal character of both competition and conflict should inform, if not determine, the dominant strategies of the game, influencing how players think about time, resources, maneuver, and objectives. The macro trends of twenty-first century competition and conflict thus far indicate that while the nature of cyberspace provides actors with ample opportunity for influence, espionage, exploitation, and subversion, the environment is significantly less conducive to coercion than other domains.

An important implication here may be that cyberspace is better suited for the pursuit of broad objectives in an infinite game, as opposed to the narrowly defined and time-constrained objectives of a finite game.

For instance, Moscow's failure to meaningfully disrupt Ukraine's ability to coordinate its national defense through employment of cyber capabilities prior to or during Russia's invasion supports the idea that cyberspace is better postured for broad geopolitical competition objectives than discrete, narrowly tailored war objectives. Despite a decade of politicians, military leaders, academics, and pundits alike predicting a future conflict largely decided by cyber means, it does not appear that Russia mounted a consequential cyber offensive as part of its invasion. This has caused some to doubt the current or future strategic utility of cyberspace.[17] However, prudence demands caution before making definitive statements or attempting conclusions regarding Russia's failure, as both time and declassification are equally likely to disprove many seemingly factual observations. If Russia has employed cyberspace capabilities as part of its invasion of Ukraine, very few observers have the means to observe and assess their impact sufficiently, or understand the degree that commercial, state, or non-state entities aided in the defense of Ukrainian cyberspace.

Whether Russia failed to develop, integrate, and deliver strategically consequential cyber effects, or the Microsoft, Anonymous, and NATO-supported community-based cyberspace defense efforts succeeded in neutralizing those effects, both potentialities provide logical support to the argument that cyberspace is better suited to geopolitical conflict than war. Russia has demonstrated the ability, when unconstrained by time and comparatively broad in its desired targets or effects, to shut down national electric grids as part of a broader geopolitical effort to destabilize its opponents or competitors.[18] In contrast, it appears that Russia has learned that during war—or a finite game—it needed to count on the effectiveness of specific capabilities and effects against a narrowly defined set of targets on a specific timeline. While military capabilities like tanks, bombers and aircraft carriers offer military planners the ability to predict or make realistic assumptions about the types of effects the military can deliver on a particular timeline, capabilities and vulnerabilities in cyberspace are often ephemeral, offering much less predictability or reliability over time.

By comparison, objectives during geopolitical competition are not as often constrained by time, do not always include narrowly defined targets, or demand discrete or tailored effects. Russia's ability to influence the 2016 US election was not only the result of years of effort, but the nature of the political objective meant that Russian actors in cyberspace had nearly unlimited targets and potential effects they could reasonably claim to be influencing the election. Additionally, as is often the case with well-conceived information operations, the uncertainty surrounding the degree to which Russia compromised the election created additional division and distrust within the electorate. Russia also had the benefit of rehearsals for its techniques, having targeted several elections in Belarus, Ukraine, and, of course, its own internal elections since 2007.[19]

Chinese IP theft via cyberspace is similarly a matter of geopolitical competition in which China, seeking to out-compete the US over time, pursues broad objectives against a diverse set of targets and effects. Washington should carefully reconsider the wisdom of leaning too heavily on its finite-game player (the military) to counter China's infinite-game strategy, while ensuring a comprehensive understanding of whether the US seeks to win, or out-compete, before establishing policies or strategies that direct how it uses national resources to play the game.

Regardless, if deterrence—or the ability to dissuade Beijing from certain behavior because the perceived benefits do not justify the perceived costs and risks—is the objective of US policy regarding Chinese IP theft, this will require the ability to influence CCP perceptions and intention.[20] Targeting and influencing perception requires both capability and credibility. However, before discussing strategies for using capability and credibility to influence perception and intention, it must be understood that existing deterrence theory was developed largely to deter *aggression*.[21]

Within the context of international relations, as well as deterrence theory, aggression is most often a matter of the coercive threat or use of force between states. Yet, it is exceedingly counterproductive to limit the conversation of cyberattacks to this narrow context, not only because most attacks in cyberspace offer poor analogical parallel to the concept of force in the physical world, but also because *force* is not defined in the United Nations (UN) Charter. To date neither the US nor China—despite overwhelming evidence of cyberattacks that undermine their national interests and threaten the security of their critical infrastructure—has invoked the protection of Article 2(4) of the UN Charter prohibiting the use of force. That neither state has claimed this protection supports the assertion that most cyberattacks should not be considered within the context of military force employment.

NO LAWS OF UNARMED CONFLICT: REVISITING OUR THEORIES, LAWS, AND CONCEPTS

Without international consensus characterizing the preponderance of state behavior in cyberspace as "force," logic should then demand skepticism among cyber policymakers regarding the wholesale applicability, and advisability of deference to, existing theories, laws, and norms surrounding the conventional use of force to competition or conflict in cyberspace. The Law of Armed Conflict (LOAC), for instance, is a body of international law intended to limit humanitarian impacts caused during the use of force between states. If there is no existing law or normative international agreement characterizing state cyberattacks against other states as force, what is the virtue or value of allowing restraining concepts like proportionality, distinction, or military necessity to interfere with the defense—or pursuit, for that matter—of national interests in cyberspace? Why would the US elect to conduct the cognitive gymnastics necessary to frame cyberattacks within the context of LOAC? To avoid the ire of operational law attorneys, this article will sidestep the nuances and technicalities of the legal debate by

simply asserting that LOAC is an analogically poor framework for regulating state behavior in cyberspace. While there remains insufficient international consensus to establish the type of norms needed to constrain state behavior, insistence upon applying the constraints of LOAC is diffusing US relative power and restraining US ability to deter aggression in cyberspace.

Extant deterrence theory and policies should be viewed with similar skepticism. Classical deterrence theory, devised to disincentivize the aggressive use of force between states, may prove insufficient in deterring the unique forms of aggressive state behavior seen in cyberspace. In their book *Cross-Domain Deterrence,* Jon R. Lindsey and Erik Gartzke note that classic deterrence theory is itself a historical product of a particular technological innovation—nuclear weapons—and cast doubt on the theory's application to the emergence of new technologies.[22]

The unique nature of cyberspace, and the fledgling historical record of competition and conflict therein, also gives reason to question strategic assumptions regarding the propensity for escalation, both within cyberspace as well as the cross-domain variety. In *The Perfect Weapon*, David Sanger notes that one reason the US cannot figure out how to counter cyberattacks is its belief that response incurs a great risk of escalation.[23] However, hesitation by the US to respond to attacks in cyberspace over concerns of escalation is poorly founded, based more on sentiment and abstraction than historical or empirical evidence. To the contrary, two decades of state competition and conflict in cyberspace suggest that a rational actor in the current international system will not use traditional military force as a response to cyberattacks that deliver only economic or information effects. To attribute the observed lack of proliferation in kinetic effects delivered through cyberspace to some inherently deterrent influence of cyberpower itself is logically lacking, as the cyber domain in that situation becomes merely a medium for cross-domain kinetic effect.

It is also logically consistent that the effects of conventional deterrence would have cross-domain influence, deterring escalation from cyber effect to kinetic action both internally and externally to the cyber domain. It stands to reason that any cyberattack that delivers armed attack equivalent effects will be treated by a state no differently than conventional force employment. In such a case, the medium of delivery is logically relevant, but should be inconsequential, as there would be little rational reason for a state to treat such an attack any differently than the use of land, maritime, or air power to deliver conventional force.

It can also be counterproductive to constrain thinking on national cybersecurity to extant military theory or doctrine. For instance, the wisdom of Clausewitz contributes to the theoretical foundations of belligerency the assertion that between two parties with equal means, defense is not only easier than attack but is the stronger and more superior form of fighting.[24] Here it should be noted that Clausewitz differentiates between "pure defense," or the act of waiting for a blow that permanently leaves the initiative with the enemy, and "relative defense," which encompasses both defensive and offensive maneuver for the purpose of either attriting the enemy or deliberately manipulating time and/or space in order to negate an enemy's temporal

advantage or influence the enemy's decision calculus.[25] Clausewitz casts pure defense aside as contrary to the very idea of war. In cyberspace pure defense—static defense measures such as firewalls, antivirus scanners, personal security products, and other automated security tools employed and monitored by system administrators and network defenders—certainly has an important place in geopolitical competition, conflict, and war.

Clausewitz's characterization of the asymmetries of interest and the nature of interplay between the offense and defense, as well as other supporting arguments for the general superiority of the defense, also apply inconsistently to conflict in cyberspace. The unique aspects of cyberspace, including the inherent obfuscation of identity, the relative ease of concealing digital presence and activities, the lack of geographic buffers, and the compression of both time and distance, combine to provide distinct advantages to the attacker over the defender.[26] In an infinite game, the advantages of maneuver, objective, initiative, economy of force, unity of command, simplicity, speed, and surprise all belong to the offense.

While the debate over the comparative advantages of offense or defense in cyberspace is unlikely to culminate in foreseeable future, the 21st century experience suggests that while the best defense in cyberspace might require some offensive action, deterrence in cyberspace will undoubtedly require both. Deterrence by denial—or lowering an adversary's expectation of success—is supported through improved cybersecurity and defensive measures intended to frustrate, mitigate, or prevent cyberattacks. Yet, there are dual asymmetries to resolve in deterring IP theft through cyberspace. First, the fundamental and inherent asymmetry between the significant potential benefits and comparatively low costs and barriers to entry makes it difficult to deter IP theft exclusively through defense. This, combined with an asymmetry of vulnerability created by US commitment to open societies, capitalist market-based economies, and global interdependency, makes it unlikely that defense alone can achieve deterrence.

The fact that China's IP theft occurs within an infinite game only compounds this reality. In an infinite game, the low cost of offense and significant financial and manpower costs of defense make it is unrealistic to expect defense alone to reduce state perceptions of benefit sufficiently to a level that achieves deterrence over time. While the continued maturation of security-focused network architectures such as zero-trust, as well as increased integration of automation or even artificial intelligence, may with time improve the effectiveness of defense and cybersecurity, there is little reason to doubt that offensive techniques and attack capabilities will be similarly improved in the time needed to implement these defensive measures. Yet, when reduced perception or likelihood of benefit is combined with increased perception of costs and risks, achieved through consistent and credible punishment, deterrence might be possible.

On top of the need to critically evaluate the applicability of existing theory, laws, and norms to cyberspace, it is prudent to reflect on US cyber policy, as the credibility of US national response to Chinese IP theft has been constrained by a variety of policy and bureaucratic

limitations across presidential administrations.[27] One such constraining influence is America's strategic culture, which is the idea that deeply rooted cultural preferences exert influence on strategic choices, and that a nation's security history imposes a certain inertia on the decisions of the state in a way that can make strategy less responsive to modern evolutions in the character of competition and conflict.[28] In cyberspace, an artifact of the multi-decade Cold War is that the US maintains a significant strategic preference for intelligence over effects. Since 2011, options for decisive offensive cyber operations in response to cyberattacks have been presented regularly to national leadership. A common objection to offensive operations, often coming from the U.S. Intelligence Community, is that offensive action poses risk to intelligence collection capabilities while delivering only a limited or short-lived benefit.[29] However, consistent deference to this view has destroyed Washington's ability to establish the credibility needed to deter cyber aggression. The predictability of the US strategic preference for economic stability, diplomatic influence, and intelligence collection over deterrence in cyberspace inexorably undermines its own credibility.

While strategic culture is certainly an obstacle, the challenge of attribution also constrains US thinking and consistency of action in cyberspace.[30] Cyber attribution, the process of identifying and laying blame on the actor of a cyberattack, is strained by many unique aspects of cyberspace itself. The logical rules that govern how networked devices communicate serve to obfuscate identity in a way that is understandably confusing to a lawyer or a politician, but much less so to a trained cyber professional. The challenge of convincing non-technical policy and decision-makers of the significance and accuracy of cyber forensics evidence has certainly contributed to a decade of failure deterring aggression in cyberspace. The US must mature not only its understanding of attribution, but its willingness to act in situations of attributional uncertainty, if the nation is to achieve the consistency of action needed for deterrence.

There are five "elements" of attributing action in cyberspace, including persona, geopolitical, geographic, logical, and physical layers. Each element can be independently and definitively determined through advanced cyber forensics. An in-depth articulation of the nuances of each element is not needed to understand the greater point: the US should reject the thinking that all five elements of attribution must be satisfied to justify action in response to cyberattacks. Currently, US decision-makers are holding attribution for actions in cyberspace to an unnecessarily high standard when each singular element of attribution offers a unique objective justification for a wide variety of potential national response actions. In other domains, decisions regarding US military action are often made based on comprehensive, multi-factor intelligence assessments. The same type of assessment is possible in cyberspace.

ADDRESSING THE CONSTRAINTS OF ATTRIBUTION

A multi-factor cyberspace attribution assessment would combine cyber forensics evidence with an analysis of the historical records of cyberattacks, economic and geopolitical

motivations, as well as signals and human intelligence, to enable analysts to provide decision-makers with a comprehensive, contextually informed confidence assessment. This framework would deliberately allow for some subjectivity, including an assessment of whether a cyberattack is consistent with enemy state interests, previously attributed cyberattacks, or known state cyber capabilities and signatures. Combining objective forensics evidence with subjective intelligence analysis should serve to improve the comfort level of decision-makers in approving and directing timely and decisive action in response to cyberattacks.

The US cyber response playbook should include the widest possible variety of punitive and responsive legal, diplomatic, informational, economic, and military actions. Such actions should include international or domestic indictment, as well as the colloquial "name and shame" brand of embarrassing public statements and condemnation. In 2015, President Obama demonstrated that the evidence of cyberattacks can be used quite effectively as leverage during diplomatic or trade negotiations.[31] The US should also expand its use of economic punishment measures to target the material interests of not only national governments, but also private commercial entities that enable enemy cyberattacks. In addition, of course, the US can use overt, covert, or clandestine offensive cyberspace operations for a wide variety of deliberate effects. Each of these potential responses receives a unique degree of logical support from the individual elements of attribution.

For example, consider a cyberattack in which the US can definitively identify the physical devices used during an attack, as well as the geographic location—in, such as China—of the equipment during the attack. Without the ability to attribute the persona element or geopolitical association (individual hacktivist versus government-sanctioned operative) of the attacker, it is perfectly reasonable to take certain playbook options, like indictment, off the table. However, given the location of the attack origin, this partial attribution offers at least some value as leverage in diplomatic negotiations, while actions targeting the device(s) or the material interests of any identified enablers would also be justified. For the sake of contrast, in the less common scenario in which the identity and geopolitical association of an attacker can be attributed, the entire playbook should be viewed as available, with or without definitive attribution of the physical or logical layers of the equipment used during the attack.

Yet, obfuscation of identity is only one way that the challenge of attribution strains a state's ability to deter aggression in cyberspace. Not only is it possible for a skilled cyber actor to obfuscate or destroy digital evidence of their presence and actions, but attributional efforts are further frustrated by the pace of technological change, the inherent and real-time customizability of cyberspace capabilities, and the omnipresent need for secrecy to protect both capabilities and a state's awareness of adversary vulnerabilities. The consequence here is that attributing action in cyberspace will, for the foreseeable future, undermine the type of timely, transactional, and associative punitive response needed to sufficiently signal to adversaries a correlation between cause and effect.

This inescapable delay between cyberattack and punishment poses a serious problem within the cognitive confines of classical deterrence theory, as a state that intends to signal or deliver punishment for undesirable behavior needs to do so in a timely and associative manner. With the nature of cyberspace naturally complicating timely response, perhaps deterrence in cyberspace demands that states evolve thinking beyond transactional tit-for-tat responses to seemingly isolated incidents of cyberattacks, and instead respond comprehensively to the collective and cumulative impacts of an adversary's actions to the state's national interests.

Lucas Kello, the director of the Centre for Technology and Global Affairs, expands upon this idea in his 2021 article in the Journal of Cybersecurity: "*Cyber Legalism: why it fails and what to do about it.*" In the article, Kello articulates four principles that should inform better doctrine for cyber conflict. His first principle, the "accretional principle," suggests that states should treat attacks as strategic campaigns, not individual actions.[32] If cyberattacks were punished cumulatively, it would allow a state to target the psychological component of adversarial decision making without the constraints of time, possibly even reducing the burden of attribution through aggregation. Similar to the Clausewitzian notion of relative defense, a strategy that observes the accretional principle would allow the victim of cyberattacks to maintain initiative by delivering penalties in a concentrated fashion and controlling key conditions of the interaction—namely time and location. This effectively enables the defender to determine, and when desirable obfuscate, the threshold of aggregate harm that triggers punishment. The "many possible permutations of punishable actions and their attendant penalties give the defender a wide scope of maneuver," introducing the type of uncertainty that should complicate an adversary's risk-benefit analysis. Well-executed, the ability to deliberately create uncertainty could reasonably cause an adversary to guess conservatively about the location of the line of response, delivering a deterrent effect on the utilization of cyberattack.[33]

OBSTACLES AND IMPEDIMENTS: COMPETING INTERESTS AND POOR NATIONAL UNITY OF EFFORT

If deterrence demands both capability and credibility, then why has deterrence failed in cyberspace? While the US is the "world's stealthiest, most skilled cyber power,"[34] since 2006, it has also been the target of more significant cyberattacks than the next seven countries combined.[35] Despite possessing tremendous cyber capabilities and capacity—military and commercial alike—the US is not feared in cyberspace.[36] While this observation demands a theory-based articulation of whether the nature of cyberspace complicates or precludes coercion, such an endeavor is beyond the scope of this article. Instead, it is enough to simply observe that while China is undoubtedly aware of US cyber capabilities, it is increasingly convinced of Washington's lack of resolve to use those capabilities to punish its behavior.[37] However, even if the US can broaden its view of cyberspace, resolve the limitations of its strategic culture, expand its view of attribution, and deliver a strategy that increases its willingness to act, certain obstacles and impediments still weaken the foundations of US deterrent potential in cyberspace.

One such impediment is the lack of trust, communication, collaboration, and cooperation between the government and the private sector. When Google executives were notified in 2009 that the Chinese had compromised their systems, they waited nearly a year to acknowledge the attack publicly. Moreover, Google did not reveal the full extent of the exposure; a server used to store court orders from the U.S. Foreign Intelligence Surveillance Court had also been compromised. Google's response was not unusual—when targeted by a cyberattack, most American corporations turn to private cybersecurity firms, and are hesitant to work with the US government due to concerns over what federal investigators might find in their computer systems.[38] This hesitation to cooperate is based on a lack of trust, which is a natural consequence of competing interests. The private sector fears that the government will pursue its other interests, namely law enforcement, while casting aside corporate concerns over publicity or economic ramifications whenever such interests impede investigation.

While progress on this front may already be underway, there is still much work to be done. In 2018, the US created the Cybersecurity and Infrastructure Security Agency (CISA), a subordinate agency within the Department of Homeland Security (DHS). The Agency seeks to work across public and private sectors, challenging traditional ways of doing business by engaging with government, industry, academic, and international partners.[39] This type of work should posture CISA to pursue the kind of "civilian military government (CMG) integration" needed to incentivize collaboration and cooperation between the public and private sectors. What is missing is transparency and clarity regarding the nature of CISA's relationship with the Intelligence Community (IC), the Department of Defense (DoD), and the Department of Justice (DOJ).

To partially mitigate the concerns of the private sector, the US government must pass legislation prohibiting CISA from collecting or storing privately owned data found during its cybersecurity response, operations, or forensics investigation activities, while also requiring corporate anonymization in threat reporting to protect corporate interests. Legislation must also clarify that CISA has no investigatory authorities with respect to domestic laws and prohibit any cooperation or communication with the FBI that does not directly advance collective national cybersecurity. Such measures would improve the private sector's perception of this new organization by demonstrating that CISA is capable of, and committed to, pursuing cybersecurity separate from other government functions, helping to establish trust and encourage national collaboration and cooperation unfettered by competing interests.

Achieving CMG integration would significantly improve two additional challenges that the nation faces in the pursuit of national cybersecurity: a lack of shared understanding of cyber threats and poor unity of effort toward the common interests of cybersecurity. Currently, if thought of as a collective entity, the national "cyber talent pool" is highly fractured and disconnected. Large telecommunications giants such as AT&T and Comcast have very talented infrastructure managers. Silicon Valley attracts software engineering experts. Norton and FireEye target cyber forensics and reverse engineering specialists. There is a large community

of independent penetration testers and certified ethical hackers throughout the country. The National Security Agency offers its civil servants the opportunity to specialize in cryptography, code breaking, or intelligence work, and those drawn to the uniform can pursue each of these specialties, and more, by service in one of the uniformed services, and through them the U.S. Cyber Command (USCYBERCOM). However, the tremendous economic incentives of the US private sector make it difficult, if not entirely unrealistic, for the government to recruit and retain the nation's top cyberspace talent. CMG integration may offer an opportunity to partially address this challenge.

For well over a decade, there has been an ongoing debate in the US regarding the ethical and security ramifications of allowing the victims of cyberattacks to "hack-back." The idea is poorly received by many, often citing concerns over escalation to war. However, it is nothing short of injustice for the government to acknowledge that it does not have the authorities or capacity to defend private commercial interests, while also constraining the response options of commercial victims of cyberattacks.[40] The fundamental implication of the "defend forward" element of the 2018 Department of Defense Cyber Strategy is that defending US government networks, critical infrastructure, and key resources requires a willingness and ability to regularly operate beyond US networks in order to disrupt, degrade, or deny adversary offensive capabilities before they reach America's digital shores. It is a phenomenal policy that has clearly improved USCYBERCOM's ability to identify, neutralize, or exploit threats to US government networks. However, the strategy also exposes an injustice, as US law and policy preclude Silicon Valley from taking similar measures, when necessary, to defend its own networks or commercial interests. China does not observe the US delineation between private or public, only national interests. While the US government's position is that the private sector should invest appropriately to defend its networks, defense is clearly not enough.

Setting aside abstract principled objections, or even existing US or international law, the reality is that restricting the private sector's immense cyber talent from taking the necessary actions to defend US economic interests in cyberspace undermines both collective cybersecurity and deterrence. To marginalize the technical talent of the private sector operationally is akin to a football team that keeps its star players on the bench. If the US thought of cyberspace as a spectrum of geopolitical competition, and not merely a domain of military or government conflict, it would not hesitate to fully leverage the best talent available to win the game. Since such a fundamental change to how the US thinks and operates in cyberspace seems unlikely in the near term, improving CMG integration might offer a meaningful compromise.

Once CISA establishes a collaborative cybersecurity community that improves the national sight picture of cyber threats, it could assume an additional role by giving the private sector a central point of contact for requesting offensive action in response to foreign cyber aggression against its corporate or economic interests. CISA would then coordinate with the appropriate agency to seek approval of the operation, affording the aggrieved company the opportunity

to provide relevant information, and possibly even offer materiel or technical support, toward achieving responsive remedial—and ideally deterrent—action. Imagine, for a moment, Silicon Valley engineers collaborating with the offensive teams of USCYBERCOM to execute timely action in response to China's cyber aggression. This future operation would have better access to both threat intelligence and cyber talent than the current siloed model, with improved capability and credibility—and *trust*—setting a more solid foundation for deterrence.

CONCLUSION

China is very effectively using cyberspace to marginalize whatever relative power advantage the US might possess, and this has Beijing on a strategic azimuth to surpass Washington in terms of relative power. Despite possessing more capacity and capability than any nation in the world, the US has been unable to leverage its national abilities to deter undesirable Chinese behavior in cyberspace.[41] This inability to achieve consensus reflects the fact that the US attempts to understand cyberspace largely through analogical reasoning, seeking conceptual understanding through the lens of existing phenomena like war or domestic and international law. This is a fundamentally flawed and limited approach that will continue to contribute to constrained thinking and national policy. Thucydides never would have imagined a world where *the strong suffer what they must, while the weak do what they can*. By broadening its view of cyberspace, resolving the constraints of its own theories, policies and thinking, and improving private and public sector cooperation, the US can build a better foundation from which to take the type of consistent and credible action needed to deter China's aggression in cyberspace.[42]

DISCLAIMER

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

NOTES

1. Robert B. Strassler and Victor Davis Hanson, *The Landmark Thucydides: A Comprehensive Guide to the Peloponnesian War.* Riverside: Free Press, 1998, 352.
2. John J. Mearsheimer, *The Tragedy of Great Power Politics. Updated edition. The Norton Series in World Politics.* New York: W.W. Norton & Company, 2014, 19.
3. Mark Clodfelter, "The Limits of Airpower or the Limits of Strategy: The Air Wars in Vietnam and Their Legacies," *Joint Forces Quarterly,* no. 78 (3rd Quarter, 2015): 112
4. Sue Gordon and Eric Rosenbach, "America's Cyber-Reckoning," *Foreign Affairs* (January-February 2022), 14.
5. Adam Segal, *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*, second edition, PublicAffairs, 2017.
6. David E. Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age,* first paperback edition (New York: Broadway Books, 2019), 104-15.
7. The Great Firewall of China: How to Build and Control an Alternative Version of the Internet," *China Review International* 25.3-4 (2018).
8. Jan Wolfe and Brandon Pierson, "Explainer-U.S. Government Hack: Espionage or Act of War?" December 19, 2020, https://www.reuters.com/article/global-cyber-legal/explainer-u-s-government-hack-espionage-or-act-of-war-idUSKB-N28T0HH.
9. Ben Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*, Harvard University Press, 2020, 86-89.
10. National Counterintelligence and Security Center, *Foreign Economic Espionage in Cyberspace* (Washington, D.C.: Office of the Director of National Intelligence), 2018, 4.
11. Matthew Kroenig, *The Return of Great Power Rivalry: Democracy versus Autocracy from the Ancient World to the U.S. and China,* Oxford University Press, 2020, 20.
12. Dorothy Denning, "Rethinking the Cyber Domain and Deterrence," *Joint Force Quarterly* 77 (April 2015).
13. JP 3-12, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf, I-1.
14. Jared King, "The Cyber (Electromagnetic Spectrum) Offset," April 30, 2018, https://othjournal.com/2018/04/30/the-cyber-ems-offset.
15. Rosa Brooks, *How Everything Became War and the Military Became Everything: Tales from the Pentagon,* First Simon & Schuster, 2016, 13-14.
16. Simon Sinek, *The Infinite Game,* 1st edition, Portfolio/Penguin, 2019.
17. Farhad Manjoo, "The Ukrainian Cyberwar that Wasn't" March 11, 2022, https://www.nytimes.com/2022/03/11/opinion/russia-ukraine-cyberattacks.html.
18. "Cyber-attacks on Ukraine are conspicuous in their absence," *The Economist,* March 1, 2022, https://www.economist.com/europe/2022/03/01/cyber-attacks-on-ukraine-are-conspicuous-by-their-absence.
19. Andy Greenburg, Everything We Know About Russia's Election-Hacking Playbook, June 9, 2017, https://www.wired.com/story/russia-election-hacking-playbook/.
20. Thomas C. Schelling and Anne-Marie Slaughter, *Arms and Influence,* Veritas, Yale University Press, 2020, 35.
21. Jon R. Lindsay and Erik Gartzke, editors, *Cross-Domain Deterrence: Strategy in an Era* of C*omplexity,* Oxford University Press, 2019, 15.
22. Ibid., 16.
23. Sanger, *Perfect Weapon*, xii.
24. Carl von Clausewitz On War, Edited and translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1976, 84.
25. Ibid., 357.
26. Lindsay and Gartzke, Cross-Domain Deterrence, 96.
27. Sanger, Perfect Weapon, 103.
28. Alastair Iain Johnston, *Cultural Realism, Strategic Culture and Grand Strategy in Chinese History* (Princeton, NJ: Princeton University Press, 1995), 2.
29. Sanger, *Perfect Weapon,* ix.

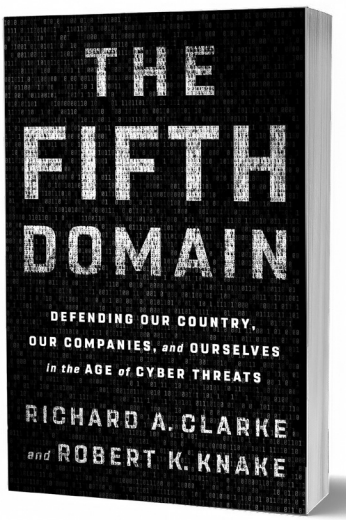
NOTES

30. Ibid., 3.
31. Ibid., 121-123.
32. Lucas Kello, "Cyber Legalism: Why it Fails and What to do About it," *Journal of Cybersecurity* (2021).
33. Ibid., 11.
34. Sanger, *Perfect Weapon,* VIII.
35. Carmen Ang, "The Most Significant Cyber Attacks from 2006-2020, by Country" May 10, 2021, https://www.visualcapitalist.com/cyber-attacks-worldwide-2006-2020.
36. Steve Turnham, "NSA Nominee Says Russian Adversaries 'do not fear us'" March 1, 2018, https://abcnews.go.com/Politics/nsa-nominee-russian-adversaries-fear-us/story?id=53441167
37. NCSC, *Economic Espionage,* 1-7.
38. Sanger, *Perfect Weapon,* 106-110.
39. "About CISA," accessed March 3, 2022, https://www.cisa.gov/about-cisa.
40. Sanger, *Perfect Weapon,* 148.
41. Ibid., xi.
42. I would like to thank Maj Jason "Brick" Sewell, the quintessential "steel man," for the many discussions and debates that helped me refine my arguments.

The Cyber Defense Review

BOOK REVIEW

The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats



By Richard A. Clarke and Robert K. Knake

Reviewed by
Cadet Dylan Green

EXECUTIVE SUMMARY

Richard A. Clarke and Robert K. Knake's book *The Fifth Domain: Defending our Country, our Companies, and Ourselves in the Age of Cyber Threats* (2019) explains "why raising the alarm on cyber threats is warranted, and... lays out a plan for how the worst outcomes can be avoided."[1] Both Clarke and Knake provide unique perspectives on potential cyber threats as both have served as members of multiple presidential administrations' Department of Defense and Homeland Security staffs. Richard Clarke, in particular, "drafted the first national strategy on cybersecurity that any nation ever published."[2] With a foundational understanding of cyber policy implementation, both Clarke and Knake capitalize on their experience to create a superbly-crafted plan to reinforce corporations' cyber readiness, increase governmental focus and impact on cyber security, develop lasting and successful cyber policies, increase personal cyber security, and share their perspectives on critically important issues likely to surface in the near future. This review highlights Clarke and Knake's key assertions about establishing lasting cyber peace, and their views on implementing the proposed segmented plan.

1 Richard A. Clarke and Robert K. Knake, "The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats," Amazon (Penguin Press, 2020), https://www.amazon.com/Fifth-Domain-Defending-Companies-Ourselves/dp/052556196X, 15.

2 Ibid., 6.

CDT Dylan Green, is a Computer Science major at the United States Military Academy. He graduated from Northwood High School in Irvine, California, in 2020, and is currently performing undergraduate research in the Department of Electrical Engineering and Computer Science (EECS) and is a member of the Army West Point e-Sports team. He hopes to earn a master's degree in Computer Science through either the Lincoln Labs Fellowship Program or the National Science Foundation Graduate Research Fellowship Program before commissioning as a Cyber Officer in the U.S. Army.

It is worth noting that Knake and Clarke regularly refer back to their 2010 work, "*Cyber War: The Next Threat to National Security and What to do About It,*" and summarize some of the key ideas of that book, which, if read first, helps readers better conceptualize what is presented in *The Fifth Domain*. For those familiar with the US military, there also are references to military acronyms (e.g., the "OODA Loop" and "TTXs)," and institutions (e.g., West Point and Army Cyber Command). Clarke and Knake provide an invaluable overview of the greatest looming cyber threats and how best to implement cyber policy. In short, for cyberspace experts and novices alike, "The Fifth Domain'' provides a clear, in-depth, big-picture foundation to see our nation's path forward in this frontier.

Review

The Fifth Domain's readability distinguishes this book from most other titles in the genre. Despite hitting the market some three and a half years ago, the accuracy with which Clarke and Knake predict many issues that have become prevalent in recent times demonstrates the persisting value that this book has to offer. Additionally, the issues which have yet to come to fruition only further cements the necessity of continuing to reflect on this work. Clarke and Knake bring decades of experience at the highest levels of government to provide invaluable hypothetical and real-life examples on technical and policy issues for both novice and highly cyber-sophisticated readers. The book is broken into distinct sections, allowing for a clear understanding of their overarching cyber defense plan.

The first section, "**THE TWENTY-YEAR WAR**," lays out an excellent backdrop for this fifth (and only manufactured) domain, i.e., the "cyber domain," in which nations are rapidly competing for superiority. Clarke and Knake argue the US approach to the cyber domain is historically and fundamentally flawed due

to the overemphasis on developing offensive cyber capabilities. Rather than cyber offense, they advocate for cyber resiliency—the ability to side-step, blunt, and otherwise survive cyber-attacks with minimal damage. This would also make attacks on the US more costly, less effective, and potentially pivotal in achieving peace in the cyber domain. The authors acknowledge some irony in proclaiming their path to cyber peace, given their earlier book "Cyber War" (2010). Yet, they assure the reader that such a goal is entirely possible. They make specific recommendations for what actions corporations, the government, and individuals must take to achieve this goal.

Part two, "T**HE CORPORATE FRONTLINE,**" outlines what the authors view as the most important repository of responsibility for protecting our nation's cyberspace — corporations and the private sector. They underscore the responsibilities and behaviors businesses must be called upon to develop their cybersecurity and resilience capabilities. They discuss the uneven outcomes certain businesses can suffer with the same attacks, and one business can remain relatively unscathed while the other suffers major losses. The stark disparity in the quality of cyber security among companies critically undermines its value to the private sector. To remedy this systemic vulnerability, many basic changes must be internalized within corporate cyber security. To ensure overall security, the authors encourage the use of multidimensional and all-encompassing tools. They also urge universal standards for security tools and minimum standards to which all companies must adhere, along with the periodic public testing of tools, after and on top of internal lab testing—trust but verify. They view the implementation of cyber security minimums and opening businesses to public testing as attainable but observe that incentivizing cyber security companies to condense their software will be highly challenging, given the competing lucrative incentive to market multiple separate (and often redundant) products.

Part three, "**THE GOVERNMENT'S SUPPORTING ROLE**," discusses how the government can support the private sector through funding, basic laws, and the interplay between cyber security and the military. Clarke and Knake articulate clear and feasible methods for the government to support and improve cyber resilience. They argue that the most effective way for the government to increase general cyber security is through "nudges and shoves," by financially incentivizing companies that adopt certain cyber policies while withholding funds from those who do not implement these policies. The authors underscore the widespread distrust of government as to why the private sector should be the first and foremost responsible for cyber security, as it would be far more effective than trying to implement cyber security through government-run institutions. They argue that the government can and should support industry from behind the scenes. They additionally dedicate an entire chapter in this section to the US power grid, which remains vulnerable to cyber-attacks. They outline a five-step plan to secure the power grid, which requires direct cyber policy beyond mere governmental "nudges and shoves" and justifies this heavy-handed approach given the

dire consequences when a power grid is attacked. They urge the creation of a federal oversight agency to bolster the security of our power grids. They also flag the need to identify the existing back doors in the grids, add state-of-the-art cyber security, and create backup power grids for worst-case events. Their ultimate goal is to render US power grid security so airtight that potential aggressors question their ability to successfully launch an attack. In their detailed recommendations, the authors demonstrate a deep understanding of how the government and the general public process new policies and the politics of delivering an achievable, well-thought-out plan with minimal resistance from stakeholder parties.

Part four, "**WARRIOR DIPLOMATS AND CANDIDATES**," highlights the global interplay between government and the internet. They note that the many weapons in our cyber arsenal, with the lack of universally accepted rules on usage in this domain, render offensive deployment challenging and precedent-setting. They also note the absence of information flow between the US and its allies and how that impedes our collective ability to stop cyber threats from actors operating from other countries. To remedy this, they urge something akin to the EU's "Schengen Accord" to govern the internet, which allows freedom of movement through many European nations' borders. Rather than allowing countries to continue having their laws regarding cybercriminals, those participating nations would adhere to the same rules that govern individual conduct and law enforcement, such as access to shared databases. The authors acknowledge the political difficulties of such a regimen but conclude that to protect the very essence of democracy, the US must find a way to combat non-state actors who pose serious threats to democratic elections, which could be significantly facilitated by codifying a shared set of rules.

Sections five and six, "**THE (NEAR) FUTURE IN CYBERSPACE**" and "**YOU AND THE WAY AHEAD**," close out the book by describing the future of cyber warfare and laying out actions that we as individuals must take to exercise prudent individual cyber security. They include discussing some of the new and fast-evolving frontiers of cyber combat, i.e., artificial intelligence (AI), Quantum Computing, and 5G. These technologies are revolutionizing cyberspace. The authors conclude their book with takeaway lessons for all, i.e., the individual cyber security practices everyone should actively focus on daily. They reiterate that a lack of personal security has more far-reaching impacts than just the individual, and why effective resilience mandates the periodic backing up of key information and vigilantly ensuring that apps are not unwittingly allowed unnecessary access, and other basic cyber hygiene that lends itself to prudent defense and resilience in cyberspace.

Ultimately, *The Fifth Domain* outlines a coherent, cohesive, and executable plan to strengthen our country's cyber resilience. Some of their proposed corporate cyber policies may be challenging, as they may require businesses to forgo altruistically short-term profits and produce fewer but more comprehensive products. If these corporate changes were implemented, they would measurably improve national cyber security and lead to multiple long-term

benefits (and perhaps even include profits). And, unlike many alarmist books without foundation, these two authors cover an amazing array of issues, including glaring vulnerabilities, while providing an equally sound range of solutions. Clarke and Knake's depth of knowledge and ability to translate complex concepts in simple ways make "*The Fifth Domain"* an essential book that continues to be important not only for individuals not schooled in the intricacies of the cyber battlespace but for seasoned cyber warriors as well.

Title: ***The Fifth Domain: Defending our Country, our Companies, and Ourselves in the Age of Cyber Threats***

Authors: By Richard A. Clarke and Robert K. Knake

Publisher: Penguin Books (July 16, 2019)

eBook: 351 pages Language: English

ISBN: 052556196X

Price: $12.99 (eBook)

THE CYBER DEFENSE REVIEW

CONTINUE THE CONVERSATION ONLINE

CyberDefenseReview.Army.mil

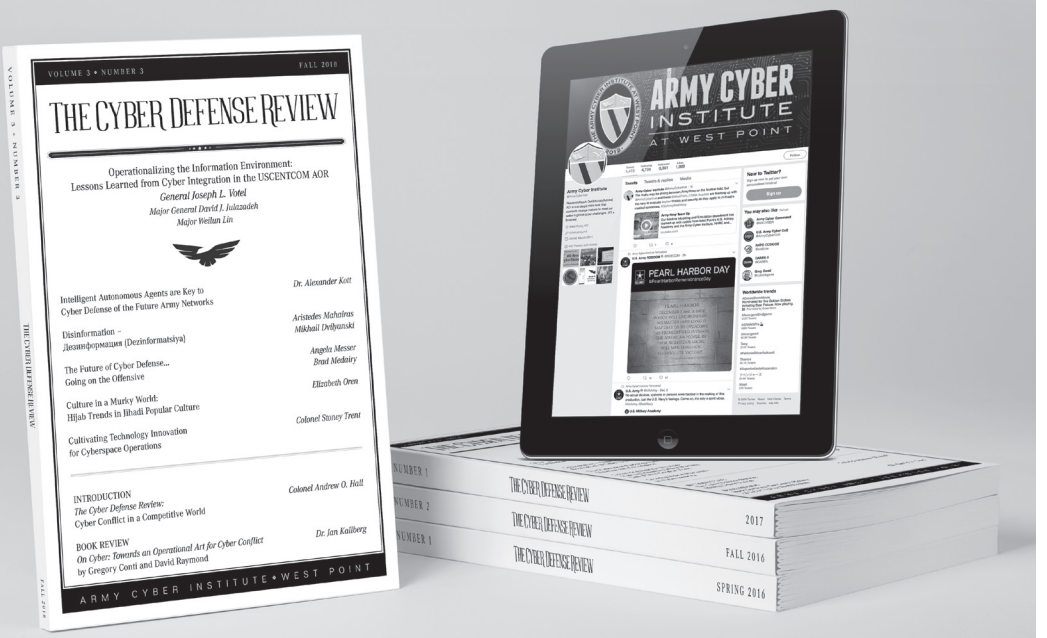
westpointpress.com

AND THROUGH SOCIAL MEDIA

Instagram @WestPointPress

LinkedIn @West-point-press
@LinkedInGroup

Twitter @WestPointPress
@CyberDefReview



ARMY CYBER INSTITUTE ◆ WEST POINT PRESS

WEST POINT
PRESS

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