VOLUME 9 ◆ NUMBER 1 SPRING 2024

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
TheCyberDefenseReview@westpoint.edu

WEBSITE
cyberdefensereview.army.mil

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

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.

FROM THE EDITOR

INTRODUCTION

SENIOR LEADER PERSPECTIVE

PROFESSIONAL COMMENTARY

RESEARCH ARTICLES

RESEARCH ARTICLES

DEAR COLLEAGUES,

I am honored and humbled to be selected as the editor-in-chief of *The Cyber Defense Review* (CDR). I follow in the footsteps of the ever positive and tireless Dr. Corvin Connolly who established and built the CDR as the foundation of intellectual discussion and scholarly works for the cyberspace domain. Thank you, Corvin. I am grateful for your efforts, the team you built, and this thriving and respected publication.

It is a difficult task to improve the performance and quality of the CDR and indeed my first goal is to work with the wonderful team of Area Editors, Reviewers, West Point Class of 1970 Assistant Editors, Designers, and the Printer to ensure a smooth handover and maintain our current level of excellence. I am grateful for the opportunity to be a part of our nation's preeminent leader development institution where we can leverage the talent at the Army Cyber Institute, Innovation Hub, the Long Gray Line, and the West Point staff and faculty to help our Army and Joint Forces fight and win on the battlefield, and ultimately compete and win as a nation.

My second goal is to ensure the CDR is on a sustainable long-term path by attracting the readers who will lead our cyber forces, the Army and our nation into the future. While *The Cyber Defense Review* is the place for the most scholarly of works, I see the need for a more interactive dialog for all members of the profession. With that in mind, I will seek to expand the CDR's online and social media presence to engage our junior leaders where they are and help them solve today's tactical and operational problems. These young people will build the new capabilities, the new organizations, and the doctrine that will define our profession and become the means by which our nation will create positions of advantage in competition and in war.

My third goal is to ensure we widen the aperture of the research we publish. As our Joint Force is called on to use military capabilities to influence strategic competition, our cyber forces will be at the forefront. Therefore, widening the aperture is twofold. First, I want to reach further into the future to where today's disruptive technologies and innovation converge to arm all our readers with a body of knowledge that will enable them to understand the operational environment, think critically, adapt to changes, rapidly resource, and creatively apply military power to win. Secondly, we will reach out to other academic institutions, think tanks, policy makers, members of industry, allies, other federal agencies, and members of our operational forces to share their discoveries with us and be a part of the debate on the employment of cyber forces across the continuum of military operations. I ask you to help us, as a journal and a professional community, solve the problems of today as we adapt to long-term, global competition and build the campaigns that will have lasting impacts ten years out and beyond.

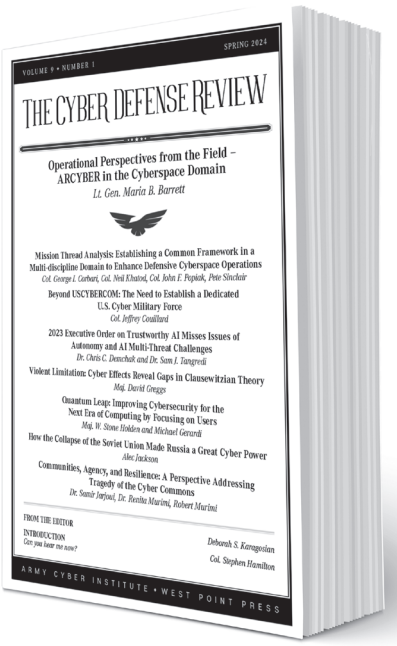
I believe the CDR and the combined efforts of this community will push the envelope on the concepts that will keep the competitive balance tilted in our favor. Having an interactive dialog with readers from across the community and broadening our aperture will have a great and long-lasting effect on our profession. —DSK

The Cyber Defense Review

Introduction

Can you hear me now?

Colonel Stephen Hamilton, Ph.D.



While serving at USCYBERCOM, shortly after it was created, I began to make my way around various parts of the agency and one day, I had an interesting conversation with a senior civilian. He asked me a rhetorical question I had to think hard about: "What matters more: the message or the ability to send that message?" I pondered it momentarily, trying to decide on what message was critically important—was it a 911 call? A call for fire at a critical point in battle? These are critically important. However, the message is meaningless if you do not have a way to send it. It suddenly became clear to me where he was going: it is the ability to send a message that is important. The ability to communicate is paramount to just about everything we do, and cyber turns that ability on or off. After more than a year as the Director of the Army Cyber Institute, I'm not so sure anymore.

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

Communication is always challenging, especially in the highly technical cyber domain. To pull this thread a little more, consider the following example. If the message is important, then it must make it to the destination intact, and the sender needs confirmation it was received (i.e., syn-ack in TCP). This is generally good enough for short concise communication; however, what if the message is not clear? What is the syn-ack equivalent of understanding the *meaning* of the message? In computer terms, this is typically solved with a hash function. However, there is no equivalent for humans other than possibly having the receiving person explain back to the sender what they understood about the communication. If what I just wrote went over your head, is that my fault as the message sender or your fault as the receiver? Did just reading that – the ability to send the message – accomplish what either of us hoped for?

However, with some thought and work, it is possible to communicate technical topics succinctly. During the beginning of the COVID lockdown, I was teaching a web application course, and since we went completely remote, the cadets used our private VPN to connect to the department's hypervisor server to build web applications on virtual machines. This allowed me to see each of their screens in a browser tab, giving me direct feedback on what the cadets were doing while I instructed them how to set up the web framework. I quickly realized that as I spoke, they often interpreted my words to result in different outcomes than expected. Since I could see this in real-time, I could correct what I was saying to explain further how to perform a task. This made me think about how we may believe in our head that we have communicated something perfectly; however, all too often, we do not realize that the person listening may not receive the message that we intended to communicate.

A quote widely attributed to Mark Twain says, "I didn't have time to write a short letter, so I wrote a long one instead." While most topics are complicated and experts tend to push back against writing short summaries of their work, as the director of ACI, I am constantly looking for ways to take difficult-to-understand topics and break them down so we can successfully communicate them in no more than one page. These one-page documents are essential for senior leadership, as there is not enough time in the day to go down the rabbit hole on all the topics within cyber. The problem is that it takes more time to boil down certain topics into their essence and communicate them clearly – but it is also a mark of an expert to be able to explain something simply. Several of our academic programs at USMA require cadets to write shorter papers, and while they initially think these will be easier, they quickly learn the errors in their assumptions.

Cyber experts have not always excelled in clearly communicating issues around their field to non-experts. The depth of technical expertise required to understand cyber operations and actions is critical to our mission, and so is communicating clearly to non-experts. Therefore, it is vital to communicate as thoroughly as possible to ensure we create a shared understanding of our cyber world – the ability to send the message is equally essential to ensuring the content of the message is received as intended. It is common to use a baseline of what someone knows to explain something new. However, the delta between what is known, and unknown can easily lead to misunderstanding. In "Mission Thread Analysis: Establishing a Common Framework in a Multi-Discipline Domain to Enhance Defensive Cyber Operations," COL Corbari et al. directly state, "Miscommunication results in a different understanding of mission requirements and similarly the expectations between those requesting support and those providing support." They propose a method of tackling this problem by proposing a Mission Thread Analysis (MTA) concept to help close this communications gap.

Other articles in this edition focus on combining traditional warfighting knowledge with cyber expertise to help bridge the gap between cyber and other warfighting functions. The range of articles in this edition goes from examining Clausewitzian Theory on war (Violent Limitations: Cyber Effects Reveal Gaps in Clausewitzian Theory) to the future of cybersecurity in a post-quantum world (Quantum Leap: Improving Cybersecurity for the Next Era of Computing). Finally, LTG Barrett's article discusses ARCYBER's enterprise capabilities. She first discusses NETCOM, which operates the world's largest network of its kind. This network provides the Army with the ability to communicate worldwide. All of these articles display that even in this one cyber journal, we look to the history of what we know to help describe the future of cyber, yet there are gaps, and it is difficult.

I hope you enjoy this edition of the CDR, and I challenge you to not only read these articles but also think about how you can better communicate about cyber in your work!

The Cyber Defense Review

Senior Leader Perspective

Operational Perspectives from the Field – ARCYBER in the Cyberspace Domain

Lieutenant General Maria B. Barrett

The spring of 2024 brings to the Army Cyber Command (ARCYBER) a renewed sense of optimism, and an opportunity to assess our mission set and reflect on the changes we have experienced across the Army and our organization. As I look back on 2023, increased tension and conflict around the world highlight the importance of our capabilities and the need for continued efforts to deter aggression and remain fully prepared to prevail in conflict when necessary. Every Soldier and civilian of ARCYBER is keenly aware of these conflicts, and more pointedly, conflict in cyberspace is now an integral element of enduring strategic competition amongst nations. Conflicts in both Ukraine and Gaza have revealed that all belligerents are operating in the cyber domain to support their tactical and strategic objectives. The persistent nature of around-the-clock cyber competition, and continuous preparations for crisis and conflict, requires constant adaptation to optimally employ our limited resources. Often, I am asked, "How exactly does ARCYBER contribute to or support the Army, U.S. Cyber Command (USCYBERCOM), and our overall National Defense?" This simple, straightforward question has a five-part answer.

First, ARCYBER consists of an enterprise of capabilities required to support and execute operations through cyberspace. We refer to the activities conducted by the ARCYBER Enterprise as "ODAII" (pronounced "O-Day"). First and foremost, the Network Enterprise Technology Command (NETCOM) **OPERATES** the Army's portion of the Department of Defense Information Network (DoDIN-A)—the world's largest network of its kind in terms of scope and endpoints. NETCOM comprises the majority of the ARCYBER workforce, employing over 16,000 people globally.

Lt. Gen. Maria B. Barrett assumed command of U.S. Army Cyber Command (ARCYBER) on May 3, 2022. A Massachusetts native, Barrett was commissioned as an Army second lieutenant via the Reserve Officers Training Corps program in 1988 after graduating from Tufts University with a B.A. in International Relations. Prior assignments include tours as Deputy Director of Current Operations, J-3, U.S. Cyber Command (USCYBERCOM); Deputy Commanding General, Joint Force Headquarters—Cyber, ARCYBER; and Deputy Commander (Operations), Cyber National Mission Force, USCYBERCOM. She has commanded units at the company, battalion, brigade, and command level, including service as Commander, 160th Signal Brigade, Third U.S. Army, and Commander, U.S. Army Network Enterprise Technology Command, her position prior to commanding ARCYBER. Barrett has also earned master's degrees in National Resource Strategy from the Industrial College of the Armed Forces (Eisenhower School) and in Telecommunications Management from Webster University.

Operating this vast network introduces multiple opportunities for complex problem-solving. The DoDIN-A is not only the conduit for simple communication via email, chat, Voice over Internet Protocol, or video conferencing, but it is also the lifeline of the Army's ability to conduct data-centric operations. Collectively, these requirements drive our obligation to provide the Army and supported Joint Forces with communications that ensure the integrity, confidentiality, and availability of information, which are imperatives to the military element of power in the 21st century. Safe, reliable, and accessible data and information collected from multiple sensors on the battlefield, combined with combat platforms, offer unprecedented lethality and rapid decision-making by the Joint Force Commander.

For NETCOM, the responsibility to Operate the DoDIN-A extends to various instantiations of cloud infrastructure, administrative controls, approval to connect devices and software, compliance, and basic cybersecurity. Ultimately, unifying the DoDIN-A through network convergence will elevate the complexity of information systems and communication terminal management to higher echelons. A converged network will better support division-level units of action during unified land operations. Disparate and expeditionary access to data circuits and cloud-based platforms will offer Army forces more mobile command posts and reduce risks of emissions and electronic signatures standing out to enemy forces. Converging tactical and installation-based networks into the unified network will enhance this heartbeat of data-centric operations, provide a resilient and secure base for sensor-to-shooter linkages, and accelerate vital decision-making. Personnel *operating* our networks also serve as our first line of defense against adversaries seeking to compromise our networks and disrupt operations.

The second part of the answer is that the ARCYBER Enterprise **DEFENDS** the DoDIN-A and, as an extension,

the weapons and systems connected to it. Whereas network operators focus on the functionality and protection of their systems and networks, the Cyber Protection Brigade (CPB) team conduct deep, targeted analysis of adversary activities through cyberspace. Often NETCOM Regional Cyber Centers enable the CPB to accomplish broader assessments across the entire DoDIN-A, such as aiding in the historical examination of anomalies. The teams and professionals within the CPB conduct "hunt" operations in search of adversary activities based on specific intelligence and other analytical assessments supported by an integrated data architecture.

Based on the realized benefits of network unification and zero trust, ARCYBER, like many organizations, is working to safely incorporate Artificial Intelligence capabilities in a practical, assistive manner. As sensors and associated data inundate modern formations and combatants, we know that human-AI pairing will provide decisive advantages in modern conflict. Network unification and investments in integrated data architecture are already collecting data to inform our decision-making related to cyberspace operations. Through the work of our Technical Warfare Center, ARCYBER G36, and NETCOM, "Hunters" from CPB are employing enterprise-wide analytics on clean and plentiful data that fuel their maneuvers like never before.

Our Cyber Protection Teams (CPT) serve a mixture of roles, executing general support requirements to the Army and direct support to specified Geographic Combatant Commanders (GCC) via USCYBERCOM. These capabilities are in high demand, never idle, and require continual training on the various systems we require them to learn about and then defend. Understanding the critical nature of data and information technology systems underpinning Army organizations depend on the operational staff and commander's understanding of their *mission threads*. I'm excited to introduce an article later in this edition of *The Cyber Defense Review* (CDR) authored by ARCYBER staff members. The authors have been closely involved in Mission Thread Analysis / Defense and Department of the Army prioritization efforts related to Defensive Cyber Operations (DCO) for the past five years. While ARCYBER provides DCO expertise to supported commands, we remain dependent on experts within each warfighting function to understand better their data, their decisions, and system dependencies enabling their unit's mission.

Mission Thread Analysis and follow-on resourcing to ensure proper defense and resiliency will help commanders appreciate how true data-centric operations enhance information advantage. This work is challenging, complex, and resource intensive, but critical to understanding how data and networks support the edge our Army deserves. A priority for the Cyber Center of Excellence (CCOE) is preparing today's signal and cyber workforces to improve support to commanders. By continuously adapting pilot courseware across the Signal and Cyber Schools at Fort Eisenhower, the CCOE delivers modern and practical data literacy education to our signal functional areas, warrant officers, and noncommissioned

officers throughout the Signal and Cyber Corps. Once introduced to their unit's mission, these technical experts will help commanders understand where data or the missions are at risk and where data can be better leveraged to support information advantage.

Third, the ARCYBER Enterprise mans, trains, and equips the National Mission Teams, Cyber Mission Teams, National Support Teams, and Cyber Support Teams that **ATTACK** by conducting Offensive Cyberspace Operations (OCO) on behalf of the Commander, USCYBERCOM and supported GCC or Functional Combatant Commanders (FCC). The part of the ARCYBER Enterprise that oversees and coordinates both OCO and DCO is Joint Forces Headquarters-Cyber (Army). As the dual-hatted Commander of JFHQ-C (A), I also rely upon the Cyber Operations – Integrated Planning Elements (CO-IPE) aligned to JFHQ-C (A) supported CCMDs. The robust CO-IPE support coordination and planning between JFHQ-C(A) and the CCMD to enhance the delivery of desired effects through OCO, DCO, and foreign partner engagements, from Security Cooperation to integrated operations.

Fourth, elements across the ARCYBER Enterprise contribute to and often execute activities to **INFLUENCE** foreign adversary military audiences. Strategic competition in cyberspace continues to prompt discussions about how the nation and the Department of Defense (DoD) can best counter mis- and dis- information. Our ongoing efforts to illuminate and attribute nefarious activity are continuously met by adversaries seeking to perpetuate malicious narratives.

The Army's *Information Advantage* initiative addresses such concerns and drives multiple changes to the formations associated with these operations from their force structure to their geo-location. Traditionally, the 1st Information Operations Brigade supported and conducted these operations. The Army's transformation included the establishment of a trans-regional Theater Information Advantage Detachment (TIAD) within the ARCYBER Enterprise, which will experiment with data sets, analytics, and various capabilities and expedite other formations to achieve similar effects in the information environment. Partnering with and supporting the TIADs in both U.S. Army Pacific Command (USARPAC) and U.S. Army Europe - Africa (USAREUR-AF), the ARCYBER TIAD is driving policy change and piloting force structure as the vanguard of Army information advantage forces and supporting reconnaissance of the information dimension for Army commanders.

ARCYBER's TIAD views reconnaissance as a key first step in gaining a regional understanding of the information environment for the commander and thereby inputting courses of action that offer U.S. Forces an information advantage. As the Army develops and matures new conceptual models to employ these capabilities, ARCYBER remains best postured to support and execute Influence operations given the array of capabilities, tools, and skills that readily exist within the Enterprise. Cyberspace requires continuous leverage adaptation to maintain and strengthen U.S. advantages in the information dimension while the terrain, circumstances, and sources of conflict shift and evolve around us.

Finally, ARCYBER **INFORMS** Army leaders and supported commanders on myriad cyberspace and information dimension threats and activities of adversaries. Through Operating and Defending the network and exploiting opportunities resulting from OCO, ARCYBER must continuously *inform* commanders, thereby enhancing decision-making and reducing or mitigating potential and actual operational threats. Though still maturing, the relatively new Cyber Military Intelligence Group has developed robust partnerships with Intelligence Community (IC) resources and private and academic partnerships through ARCYBER and USCYBERCOM authorities to provide specialized reporting and insights related to cyberspace and information dimension activities.

The players, methods, and circumstances that define intelligence collection and dissemination are changing rapidly and continuously. Once highly classified satellite capabilities providing imagery and tracking of enemy forces, only possible with nation-state resources and expert analysts, today are readily available open-source information to hobbyists, citizens, and adversaries alike. With unprecedented capabilities, these groups increasingly play a role in intelligence operations across the information dimension of warfare. Smartphones, global networks, and modern, data-literate populous increase battlefield transparency beyond that of even the height of U.S. intelligence, surveillance, and reconnaissance dominance during the Iraq and Afghanistan wars, which, in turn, has prompted changes in the Army's Intel strategy to incorporate and otherwise exploit open-source intelligence practices and policies. Beyond our own intelligence needs, increased battlefield transparency will require shifts in our training and materiel to ensure that our maneuver forces remain concealed and distributed.

As you see from what I've reported above, the Army must always embrace continuous transformation as an imperative. Amidst this continuous change, ARCYBER remains riveted on preparing for modern and emerging threats, and our obligation to ensure that our forces maintain a competitive edge in any armed conflict. At its core, the ARCYBER is and will always remain a learning organization. As we mature and modernize our execution of cyberspace operations, we must continue to demonstrate our adaptability as we face new challenges. Following the tragedy of October 7, ARCYBER demonstrated its flexibility, gained through years of persistent cyber operations in support of U.S. Central Command (USCENTCOM). Our long-standing regional expertise and experience enabled our teams to pivot quickly in response to the USCENTCOM Commander's requirements. We have demonstrated the value of cyber operations delivering effects against enemy targets. These recent cyber operations also provided opportunities for Joint Force Commanders to message and influence within the information dimension. These operations have imposed cost on the adversary, enabled simultaneity of operations by supported forces, and, most importantly, have broadened the array of options available to supported commanders.

"How exactly does ARCYBER contribute to or support the Army, U.S. Cyber Command, and our overall national defense?" Through an *enterprise-wide* approach of integrating disparate capabilities to supported commanders. Our capabilities are significant, but our value begins with and is measured by the quality of our world-class workforce. We are proud to lead multiple efforts that enhance the effectiveness of Army formations, directly contributing to the defense of our Nation. Our talented, diverse, and cohesive workforce remains steadfastly committed to delivering comparative advantages to commanders who increasingly rely on data-centric enhancing capabilities. I am optimistic about our future and fully committed to acquiring, employing, developing, and retaining the very best talent we need to increase and maintain our comparative advantages.

The Cyber Defense Review

Professional Commentary

2023 Executive Order on Trustworthy AI Misses Issues of Autonomy and AI Multi-Threat Challenges

Chris C. Demchak, Ph.D.
Sam J. Tangredi, Ph.D.

On October 30, 2023, the Administration released Executive Order (EO) 14110 on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (AI). For several reasons this EO lays a light hand on the Department of Defense (DoD).

First, the DoD had and was already implementing "responsible AI" safeguards for defense programs.[1]

Second, as the federal agency most likely interested in "killer robots," the DoD for years has firmly embedded an ironclad policy to ensure that "[t]here is always a human always responsible for the use of force" – the so-called "human-in-the-loop (HITL)."[2]

Third, peer adversaries to the U.S. have yet to openly demonstrate autonomous capabilities that could force the military to publicly reconsider its ethical principles, even though we do not naively expect adversaries to observe ethical constraints in combat.

Fourth, non-DoD U.S. government agencies are a step behind the military in setting, much less enforcing, policies on responsible AI.[3]

Fifth, a public debate over AI for some time has been in progress among political and IT capital goods elites over a rising concern that uncontrolled commercial and government use of AI is spreading too rapidly into all private and consequential aspects of citizens' lives – areas in which DoD generally plays a limited role.

With engineering, economics, and comparative complex organization theory/political science degrees, **Dr. Chris C. Demchak** is the RDML Grace M. Hopper Chair of Cyber Security and the Senior Cyber Scholar, Cyber and Innovation Policy Institute, U.S. Naval War College. Her research and many publications cyberspace as a globally shared insecure complex 'substrate' take a systemic approach to emergent structures, comparative institutional evolution, adversaries' use of systemic cybered tools, virtual worlds/gaming for operationalized organizational learning, and designing systemic resilience through collective cyber defense against imposed surprise.

Sixth, while the President cannot enforce these principles on the nation's commercial vendors, he can dictate policy and procedure to federal agencies as to how they pursue their AI, and through their purchases, perhaps indirectly influence the wider national AI market.

While these are all solid justifications for the EO's limited attention to the DoD, it is worth exploring how consideration of two related and forthcoming realities might have made a difference if included – autonomy and dual uses of AI.

Contents of the EO

The Executive Order weighs in at 36 pages. Its stated purpose is to reduce the potential for "irresponsible use" of AI which it defines as "exacerbate[ing] societal harms such as fraud, discrimination, bias, and disinformation; displac[ing] and disempower[ing] workers; stifl[ing] competition; and pos[ing] risks to national security."[4] As can be detected right away, its examination is more on "societal harms," than extensive risks to national security. However, it does make substantial reference to "dual-use" technology and necessary cooperation between other departments and DoD to establish further policies on related risks.

The EO gives directives to government departments and agencies in a seemingly firm and decisive manner. As an example: "The Secretary of Labor shall, within 180 days of the date of this order and in consultation with other agencies and with outside entities, including labor unions and workers, as the Secretary of Labor deems appropriate, develop and publish principles and best practices for employers that could be used to mitigate AI's potential harms to employees' well-being and maximize its potential benefits."[5]

However, this apparent decisiveness is mitigated by the fact that the EO applies *only* to government agencies. It has no authority over commercial or non-government organizations. Thus, to use the Labor Department

Dr. Sam J. Tangredi is the Leidos Chair of Future Warfare Studies and professor of national, naval and maritime strategy at the U.S. Naval War College. A retired Navy captain and surface warfare officer and strategic planner, he has published seven books, over 200 journal articles and book chapters, and numerous reports for government and academic organizations. His latest book (co-authored with George Galdorisi) is *Algorithms of Armageddon: The Impact of Artificial Intelligence on Future Wars* (Annapolis, MD: Naval Institute Press, 2024). He held command at sea and directed strategic planning organizations.

example, there is nothing to compel "outside entities" to cooperate with directive activities if they chose not to cooperate. What if labor unions and worker have no desire to be in "consultation" with the government? Can the practical objectives of the EO—as opposed to the churning out of published "best practices" and other white papers—be fulfilled if the non-government sector ignores it? This is particularly acute concerning corporations developing AI which have every desire to take every legal action they can to turn a profit, oppose government regulation, and keep control over their intellectual property.

AI development is dominated by commercial firms for commercial purposes to which the EO does not apply. In a sense, the EO can only posture the U.S. government to set a good example.

Ironically, it is DoD that has the greatest measure of influence and control over its particular commercial sector—the Defense Industrial Base. This is one of the reasons that the practices and policies of DoD can more easily exceed the requirements of the EO, and probably the one major reason why the EO exhibits such a light hand on the department.

Autonomous Systems and Human-in-the-Loop

The autonomy of AI-driven machines has long been a political concern, usually captured emotion-laden public debates on "killer robots" able to cause disaster without human controls.[6] The White House's EO reflects the wider public debate on the topic which today is more likely to address police use of robots than the military use.[7] Furthermore, the DoD's often repeated policy of limiting autonomy by keeping a "human-in-the-loop" should in principle serve to discourage military robotic adventurism. Less mentioned, however, are more specific alternatives such as human-on-the-loop (HOTL) supervision, human-adjacent-to-the-loop (HATL) refining, or even human-out-of-the-loop

(HOOL) automaticity, which pose increasingly more distant human direct control of what the AI-trained and controlled machines ultimately do.[8]

It is a sensible assessment of possible future combat to attempt to envision the conditions under which human-in-the-loop intentionally, or not, becomes human-on-the-loop only.[9] That is, when having a human deeply embedded in assessing a situation and then choosing and initiating the next steps becomes a too slow, inaccurate, or risky process. Human-on-the-loop then becomes a human initiating and then monitoring a process by which the AI-controlled machine then assesses, chooses, and then autonomously executes the sequence of steps towards an objective. What then is acceptable when, due to the exigencies of super rapid combat with AI-enabled adversaries, even human-on-the-loop becomes too slow or risky? The next iteration is the human-adjacent-to- or human-near-the-loop (HNTL) where the human is removed from real-time monitoring to episodic monitoring conditions by which interactive machines collectively share information, assess, choose, and initiate steps in operational processes. Finally, a devolution to human-out-of-the-loop or, at least, humans-on/offing-the-automatically-triggerable-autonomous-otherwise-sealed-loop could easily become the only militarily sensible choice against adversaries doing the same.[10] It is not a slippery slope, but possibly an evolution in practice from the machines needing human interaction to their not needing humans or not having many entry points by which humans could interfere. Having the slow and nonexpendable humans interfering in rapid-fire, drone swarm, battle decisions might not be sensible in high-end, high-stakes warfighting in a highly contested electromagnetic warfare-rich environment, other than to centrally shut systems down.

Deputy Secretary of Defense Kathleen Hicks underscores the importance of ensuring that the "appropriate level of human judgment" be "flexible."[11] DoD policy on Lethal Autonomous Weapons Systems (LAWS) does not expressly bar development or use of these capabilities. The key distinctions lie in the definition summarized by the Congressional Research Service; LAWS "are a special class of weapon systems that use sensor suites and computer algorithms to independently identify a target and employ an onboard weapon system to engage and destroy the target without manual human control of the system."[12] To "independently identify" targets and act to harm "without manual human control" defines the LAWS, and therein also lies some of the flexibility in defining "in-the-loop" noted by Dr. Hicks. The human remains "in-the-loop" if the targets cannot be selected without human input, or if control is delegated under human supervision with the option to cancel the mission at key points in its execution.

For example, for the recently announced "Replicator" program, which is designed to produce thousands of surveillance, disrupting, or lethal drones, the human 'in-the-loop' would control overarching instructions to the drone swarm, yet it is unclear what else the human controls in these drone operations.[13] The human-loop evolution is still evolving within DoD along with everyone else; however, the Administration's new EO makes no mention of this challenging spectrum of human involvement in targeting.

Russia, The People's Republic of China, and Military AI

Adversaries and vendors also get a vote in the future of trust with AI and DoD. Their choices could increase environmental pressures on the U.S. military to move faster, to more precisely define what falls within (and without) the outer bounds of acceptable and unacceptable flexibility in what human-in-the-loop means, and to unwittingly expand the operational choices of automation, despite the best of ethical intentions of DoD leaders. There is no reason to assume that aggressive autocratic nations like Russia or China have any incentive to maintain the human-in-the-loop 'principle' concerning the use of deadly force in autonomous systems. Russia's Vladimir Putin has urged international controls on other states while asserting the need for Russia to ensure America has no monopoly on AI.[14] Rapidly adapting commercial AI for use in battle is hard and time-consuming. Commercial developers, absent regulations or other oversight, do not spend the time for careful consideration of the longer-term systemic ethical consequences in democracies, let alone in today's war-driven Russia.[15] And Putin is incentivized to move quickly given his stated position that the nation who "rules AI" will "rule the world."[16]

China's Xi Jinping repeatedly has expressed strong ambition for China to lead the world in artificial intelligence and other technologies perceived as critical to the national socio-technical-economic systems of democratic systems. The Chinese 2017 'New Generation AI Development Plan' projected that China would be the 'major AI innovation hub of the world' by 2030.[17] At the same time, China has a robust history of technological theft through cyber attacks, hostile buys, and bullying economic or political coercion.[18] One after another major cyber attack has been attributed publicly to Chinese state-sponsored hackers across major underlying operating systems.[19] There is no reason to presume any change in China's extraction operations as part of China's relentless centrally fueled AI development program.[20] Nor is there any evidence that the Chinese approach to gaining dominance in or employing artificial intelligence – whether in espionage, economic theft, or combat – will be any different than its admittedly creative cyber extractive pursuit of other technology targets.[21] The one silver lining is the natural conservative bent of the Chinese military to want to be sure a new technology works as planned before it is used extensively.[22] Beyond that functional certainty, however, China's embrace of AI reveals no more ethical constraints than China has shown with cyber in general when opportunities emerge to disrupt democratic targets in or outside of combat.

Industrial Base and Dual-Use

Vendors also get a vote. The principles of the White House AI EO, as the DoD's AI Ethics are voluntary for any commercial entity unless one is already a contractual partner to the DoD in the Defense Industrial Base (DIB).[23] The non-DIB commercial AI industry conducts the vast majority of AI development and production, especially the massive foundation models and their products, but these firms are not obligated to ensure ethical standards through their development or deployment process. Given what is likely to be available within DoD's accelerated time limits, ethically integrating AI effectively inevitably will force choices between

ensuring ethical standards or missing deadlines. Rigorous observance of ethical standards throughout the AI development cycle will be more difficult than assuring the cyber security of the software development process, and the latter is largely not yet anything close to a success.[24] DIB contractors must adhere to DoD ethical principles in order to obtain and retain DoD contracts, but they are by and large not the major developers or vendors of cutting edge AI despite their glossy advertisements making timelines, ethics, and bleeding edge quality of DoD's AI purchases open to question and possible distrust, despite assurances today.[25]

Impacted by the dominance of commercial actors are challenges presented by the dual-use of AI potentially facilitating Chemical, Biological, Radiological & Nuclear (CBRN) development by terrorists or non-experts, regardless of whether humans are in, on, nearby, or out of the loop. Again, although the EO's dual-use provisions will affect private commerce relating to defense, most of the directives only affect other government agencies. DoD and the intelligence community are already deeply invested in following well-known and cyber-enabled CBRN connections, but public sources do not reveal whether this issue will have sufficient AI expertise or dedicated focus.

Demands on DoD to Lead AI Policy

The EO provides little guidance as to these serious external pressures on DoD, rather it has only several demands on the department. The Secretary of Defense is directed to "capitalize on AI's potential to improve United States cyber defenses" (for national security systems) and (along with Department of Homeland Security) "develop plans for...an operational pilot project to identify, test, evaluate, and deploy AI capabilities, such as large language models, to aid in the discovery and remediation of vulnerabilities in critical United States Government software, systems, and networks." The Secretary is also to contract, in consultation with the National Security Advisor and the Office of Science and Technology Policy, with the National Academies of Science, Engineering and Medicine on a study to assess ways in which AI can increase or reduce biosecurity risks. Finally, the Defense Secretary and Chairman, Joint Chiefs of Staff are also members (along with other Cabinet Departments and numerous Presidential advisors) of a White House Artificial Intelligence Council to formulate and implement AI policies.

Also, the White House's National Security Advisor must develop a "memorandum" addressing "the governance of AI used as a component of a national security system or for military and intelligence purposes. The memorandum shall take into account current efforts to govern the development of AI for national security systems."

The bottom line is that the EO's authors appear to accept the reality that DoD already is addressing the EO's key issues in the following: 2022 DoD Responsible AI Implementation and Strategy, 2023 DoD Data, Analytics, and Artificial Intelligence Adoption Strategy, and the various service's AI policies embedded with ethics throughout acquisition/development and deployment/retraining. Other issues can be associated with DoD initiatives such as the

following examples (the list is not exhaustive): promoting innovation and competition (e.g., the "Tradewinds" initiative under DoD's Chief Digital and AI Office); promoting U.S. AI talent ("500 new researchers by 2025" and various DoD AI education efforts); development of training resources (various DoD AI education efforts); establishing new service-connected AI Research Institutes (Department of the Air Force MIT AI Accelerator, Department of the Army's work with Carnegie Mellon University, Department of the Navy efforts to create a DON AI Accelerator homed at NPS); grants for AI Tech Sprint competitions (support for Defense Innovation Unit efforts, Naval Innovation Exchange (NIX), The Navy's Task Force 59, the Naval Applications of Machine Learning (NAML) conferences, and the equivalents across all services).[26] In short, these DoD initiatives help explain the White House's light hand relative to DoD.

The question is whether sufficient thinking has been put into what happens as to the civilian sector spillover when the forcing functions of AI-enabled combat advantages, adversaries' AI advances, and AI vendors' ethical or security neglects inevitably come into play. The impact of this trifecta will be further affected by other technologies changing at warp speed: quantum, nano, and fusion. The AI era is just beginning to outweigh cyber in its transformational effects, including in conflict. Executive orders of the future governing responsible AI must recognize and appreciate the impact that adversarial scenarios will pose for guardrails desperately needed in non-DoD contexts. While the EO did not signal that coming discussion, DoD may need a stronger hand given the bleed-over effect its advances will have on non-DoD capabilities. The military leaders need at least senior leaders' foresight and more collaborative oversight into what are today's exceptionally uncomfortable topics; these dilemmas are likely to be tomorrow's ugly realities.

DISCLAIMER

The views expressed here are those of the authors alone and do not necessarily represent the views, policies, or positions of the U.S. Government, Department of Defense or its components, to include the Department of the Navy or the U.S. Naval War College.

NOTES

1. U.S. Department of Defense, *U.S. Department of Defense Responsible Artificial Intelligence Strategy and Implementation Pathway*, June 2022, https://www.ai.mil/docs/RAI_Strategy_and_Implementation_Pathway_6-21-22.pdf.
2. U.S. Department of Defense, *Remarks by Deputy Secretary of Defense Kathleen H. Hicks on 'The State of AI in the Department of Defense' (As Delivered)*, November 2, 2023, https://www.defense.gov/News/Speeches/Speech/Article/3578046/remarks-by-deputy-secretary-of-defense-kathleen-h-hicks-on-the-state-of-ai-in-t/.
3. U.S. Government Accountability Office (GAO) "Artificial Intelligence: Agencies Have Begun Implementation but Need to Complete Key Requirements" (December 12, 2023) https://www.gao.gov/assets/d24105980.pdf
4. "Executive Order 14110 of October 30, 2023," *Federal Register* 88, no. 210 (November 1, 2023), 75191, https://www.govinfo.gov/content/pkg/FR-2023-11-01/pdf/2023-24283.pdf.
5. Executive Order 14110 of October 30, 2023," 75210.
6. Charli Carpenter, "How scared are people of "killer robots" and why does it matter?" *Open Democracy*, July 4, 2013, https://www.opendemocracy.net/en/how-scared-are-people-of-killer-robots-and-why-does-it-matter/; Jay Stanley, "It's simply too dangerous to arm robots," *ACLU*, December 16, 2022, https://www.aclu.org/news/privacy-technology/its-simply-too-dangerous-to-arm-robots.
7. Stanley, "It's simply too dangerous to arm robots."
8. See discussion in George Galdorisi and Sam J. Tangredi, *Algorithms of Armageddon: The Impact of Artificial Intelligence on Future Wars* (Annapolis, MD: Naval Institute Press, 2024), 125-144.
9. Galdorisi and Tangredi, 74-75;
10. Eric Jensen and Carolyn Sharp, "Reentering the Loop," *Articles of War*, February 9, 2022, https://lieber.westpoint.edu/reentering-the-loop/.
11. Brad Dress, "Pentagon's new AI drone initiative seeks 'game-changing shift' to global defense," *The Hill*, September 6, 2023, https://thehill.com/homenews/4189864-pentagons-new-ai-drone-initiative-seeks-game-changing-shift-to-global-defense/.
12. Congressional Research Service, Defense Primer: *U.S. Policy on Lethal Autonomous Weapons Systems*, February 1, 2024, https://crsreports.congress.gov/product/pdf/IF/IF11150#.
13. Dress, "Pentagon's new AI drone initiative seeks 'game-changing shift' to global defense." For a critical view of 'Replicator,' see Sam J. Tangredi, "Replicate Ordnance, Not Cheap Drones," U.S. Naval *Institute Proceedings* 150, no. 3 (March 2024), https://www.usni.org/magazines/proceedings/2024/march/replicate-ordnance-not-cheap-drones.
14. Samuel Bendett, "Putin Urges AI Limits — But for Thee, Not Me?" *Defense One*, December 3, 2020, https://www.defenseone.com/ideas/2020/12/putin-urges-ai-limits-thee-not-me/170458/; Guy Faulconbridge, "Putin says West cannot have AI monopoly so Russia must up its game, Reuters, November 24, 2023, https://www.reuters.com/technology/putin-approve-new-ai-strategy-calls-boost-supercomputers-2023-11-24/.
15. Ionut Arghire, "Over a Dozen Exploitable Vulnerabilities Found in AI/ML Tools," *Security Week*, November 17, 2023, https://www.securityweek.com/over-a-dozen-exploitable-vulnerabilities-found-in-ai-ml-tools/.
16. James Vincent, "Putin says the nation that leads in AI 'will be the ruler of the world,'" *The Verge*, September 4, 2017, https://www.theverge.com/2017/9/4/16251226/russia-ai-putin-rule-the-world; Galdorisi and Tangredi, 1-4.
17. Ulrich Jochheim, European Parliamentary Research Service, "China's Ambition in Artificial Intelligence," European Parliament (official site), September 2021, https://www.europarl.europa.eu/RegData/etudes/ATAG/2021/696206/EPRS_ATA%282021%29696206_EN.pdf.
18. Kantaro Komiya, "US, Japan authorities warn of China-linked hacking group BlackTech," *Reuters*, September 28, 2023, https://www.reuters.com/technology/us-japan-authorities-warn-china-linked-hacking-group-blacktech-2023-09-28/; Daryna Antoniuk, "China-based spies are hacking East Asian semiconductor companies, report says," *The Record*, October 6, 2023, https://therecord.media/china-budworm-apt27-east-asia-semiconductor-companies.
19. "Fast Thinking: A turning point on Chinese hacking," *Atlantic Council*, July 19, 2021, https://www.atlanticcouncil.org/content-series/fastthinking/fast-thinking-a-turning-point-on-chinese-hacking/.
20. Jane Cai and Willian Zheng, "China launches new data agency as ambitions in AI and digital economy soar," *South China Morning Post*, November 20, 2023, https://www.scmp.com/news/china/politics/article/3242067/china-launches-new-data-agency-ambitions-ai-and-digital-economy-soar.

NOTES

21. U.S. Cybersecurity and Infrastructure Security Agency, "Cyber Security Advisory: People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection," May 24, 2023, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a.
22. David Roza, "How China's PLA Could Use Tech Like ChatGPT, And What Could Hold It Back," *Air & Space Forces,* August 24, 2023, https://www.airandspaceforces.com/china-generative-ai-chatgpt/.
23. Congressional Research Service, *Defense Primer: U.S. Defense Industrial Base*, April 17, 2023, https://crsreports.congress.gov/product/pdf/IF/IF10548.
24. Ionut Arghire, "Over a Dozen Exploitable Vulnerabilities Found in AI/ML Tools."
25. U.S. Cybersecurity and Infrastructure Security Agency, "Defense Industrial Base Sector: Council Charters and Membership," n.d. (accessed March 4, 2024), https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/defense-industrial-base-sector/sector-charters-and-membership.
25. U.S. Cybersecurity and Infrastructure Security Agency, "Defense Industrial Base Sector: Council Charters and Membership," n.d. (accessed March 4, 2024), https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/defense-industrial-base-sector/sector-charters-and-membership.
26. Joseph Clark, "DoD Releases AI Adoption Strategy," *U.S. Department of Defense*, November 2, 2023, https://www.defense.gov/News/News-Stories/Article/Article/3578219/DoD-releases-ai-adoption-strategy/.

The Cyber Defense Review

Research Articles

Mission Thread Analysis: Establishing a Common Framework

in a Multi-discipline Domain to Enhance Defensive Cyberspace Operations

Colonel George I. Corbari
Colonel Neil Khatod
Colonel John F. Popiak
Pete Sinclair

ABSTRACT

The multi-disciplinary nature of Cybersecurity, Cyberspace Security, and Defensive Cyberspace Operations (DCO) has resulted in different interpretations of cyber-related terms among various groups. The communication gap between cybersecurity professionals and operational professionals has increased over time. Cybersecurity professionals struggle to establish priorities of work as they define and frame the risks differently from mission-focused operating professionals. Miscommunication results in a different understanding of mission requirements and different expectations between those requesting support and those providing support. Despite progress in cybersecurity tools and processes, the communication gap endures. Presently, ARCYBER is challenged to balance the demands of mission commanders requesting defense of critical missions, Congress directing actions to defend critical resources, and intelligence reports, all resulting in diversion of resources to address perceived threats. Mission Thread Analysis (MTA) is a process to help build understanding and consensus between customers (operational force) and providers (network operators and defenders), offering an analytical framework where both sides detail

COL George I. Corbari is an Army Strategist who has served in U.S. Army Cyber Command and U.S. Cyber Command for the past 7 years. He is currently a Strategic Advisor to the Commander, ARCYBER. During the past seven years, he has served as the ARCYBER G5, Director of the Commander's Strategic Initiatives Group (ARCYBER), and Director of the Combined Action Group (USCYBERCOM). Over a 30-year career he has served throughout the United States, in the Indo-Pacific, Europe, and Afghanistan. He began his career as an Interrogator/Russian Linguist and served as an Air Defense Officer. COL Corbari holds an M.S. from the Eisenhower School for National Security and Resource Strategy, a M.Ed. in Human Performance Enhancement from Western Washington University and a B.A. in Education from Bethany College, KS.

their operational and technical requirements. MTA requires mission owners to analyze, prioritize, and depict a mission as a series of steps within a Mission Process Thread (MPT), including the data pathways or Mission Engineering Threads (MEngTs) required to complete the mission. Integrating MTA results with threat intelligence enables appropriate planning and coordination to apply the right capability to perform DCO in support of Army requirements. ARCYBER redesigned and formalized the MTA process to help inform prioritization, training, team employment, and optimization of Defensive Cyber Forces. This new MTA process, or a similar adaptation, will prove useful in planning and coordination of cybersecurity efforts across a broad range of actors, including, but not limited to: Interagency Partners; State, Local, Tribal, and Territory (SLLT) Partners; the private sector, and international partners by defining cyber defense requirements in terms in common all actors.

INTRODUCTION

Over time network operators and network defenders created terminology to describe how they mitigated vulnerabilities and contended with threats. For example, as the terms Cybersecurity,[1] Cyberspace Security,[2] Cyberspace Defense,[3] and Defensive Cyberspace Operations (DCO)[4] evolved and came into use by cybersecurity professionals, the nuances in the different definitions created gaps in understanding between cybersecurity professionals and operational professionals.[5] The different terms, often used interchangeably by operational professionals, contribute to confusion when addressing support requirements. It is particularly important when determining the degree of protection or defense required within cyberspace (see Textbox 1:

COL Neil Khatod recently retired from serving as the ARCYBER G-3, Director of Operations Officer. He has served in various leadership and staff positions during his 29-year career. Recent positions include serving the Chief of Defensive Operations (G36) for ARCYBER and as the commander of the 2nd Theater Signal Brigade in Germany. Colonel Khatod received his commission through the United States Military Academy at West Point where he graduated in 1994 with a Bachelor's degree in Spanish and French. He also has advanced degrees from the University of Oklahoma (Master's in Human Relations), the University of Maryland (Master's in Information Technology), and the National War College (Master's in National Strategy and Policy). He recently became the Chief Information Officer and Veterans Outreach lead at Hays Americas.

Differing Terminology

Cybersecurity vs Cyberspace Security vs Cyber Space Defense vs Defensive Cyber Operations vs Defensive Cyber Actions…

Consistent across multiple Department of Defense publications and strategies, oint doctrine uses the term "cyberspace security" to distinguish the tactical-level cyberspace action from the policy and programmatic term "cybersecurity" used in the Department of Defense (DoD) and United States Government (USG) policy. In order to enable more effective planning, execution, and assessment, joint doctrine distinguishes between cyberspace security and defensive cyberspace actions. DoD and USG cybersecurity policy make no such distinction, instead employing the term cybersecurity, to include the ideas of both security and defense. Doctrine uses "cyberspace security" to describe specific actions as described in this paper and "cybersecurity" only in reference to DoD or national policies for protecting cyberspace.

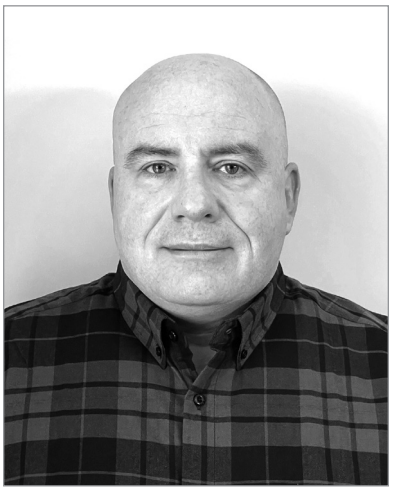
Textbox 1

Differing Terminology). To put it another way, the distinction between a proactive mitigation of vulnerabilities to prevent exploitation and execution of DCO while contending with an active threat is often lost in translation between mission owners and cyberspace professionals.[6] As a result, cybersecurity professionals struggle to establish priorities of work as they define and frame the risks differently from the operating professionals who are focused on mission accomplishment. Each group uses the same or similar words, but with different intentions or meaning. As an example, FM 3-90 defines "Disrupt" as "…a tactical mission task in which a unit upsets an enemy's formation or tempo and causes the enemy force to attack prematurely or in a piecemeal fashion."[7] However, FM 3-12 Cyberspace Operations and Electromagnetic Warfare[8] and JP 3-12 Cyberspace Operations defines "Disrupt" as "to completely but temporarily deny access to, or operation of, a target for a period of time. A desired start and stop time are normally specified. Disruption can be considered a special case of degradation where the degradation level is 100 percent."[9]

COL John F. Popiak is a cyberwarfare officer who has held command and staff positions across the Army, Cyber Command, and National Security Agency with assignments in the United States, the Republic of Korea, Europe, Africa, and Afghanistan. COL Popiak has served in a wide variety of tactical, operational and strategic cyberspace assignments. COL Popiak's previous green-tab leadership experience ranges from airborne rifle platoon leader through brigade commander of the US Army Cyber Protection Brigade.

Miscommunication results in a different understanding of mission requirements and expectations between those requesting support and those providing support within the cyberspace domain. However, where cyberspace is concerned, the breakdown results in stark differences between a mission commander's ability to operate and the technical requirements needed to securely support critical operations via cyberspace capabilities. The tension between mission command requirements and network and system security requirements adds to the challenge of those charged with DCO. Despite progress in cybersecurity tools and responses, the communication gap endures, leading to a growing disconnect between customers (mission commanders) and providers of cybersecurity. As the Cyber Mission Force (CMF)[10] has matured, so have their techniques, tactics, and procedures. What was once considered the most effective approach to defending "assets" is now considered ineffective because no asset exists separate from the systems and networks it is connected to within cyberspace. Additionally, missions commonly extend beyond the Department of Defense Information Network (DoDIN) assets to off-DoDIN systems and networks.[11]

ARCYBER presently faces numerous demands by mission commanders requesting support to defend critical missions, Congressional directives[12] to defend critical systems, and intelligence reports highlighting that the Internet is a dangerous place, resulting in diversion of resources to address perceived threats. Such demands prevent ARCYBER from effectively planning, affecting training and readiness as well as resource allocation. Finally, without a comprehensive understanding of residual risk, Army leaders are unable to understand well enough when and where they are accepting risk to systems and networks. When a crisis such as "Solar Winds"[13] occurs, Cyber Protection Teams (CPT) and analytic support capabilities are redirected from



Mr. Pete Sinclair is currently employed by Peraton as a Cyberspace Operations Planner in support of the Army Cyber G5. He retired from the Army after serving in three different branches over twenty-one years and six deployments. He is a graduate of Northern Michigan University and the School of Advanced Military Studies. He is also a graduate of the Harvard Kennedy School's Executive Education Leadership in Homeland Security program and the Homeland Protection Course at the Massachusetts Institute of Technology's Lincoln Laboratory.

their current missions to address the crisis. Prior to 2022,[14] the Army had no process for determining where it would accept risk when re-missioning capabilities to concentrate on an emerging crisis, instead relying solely upon the ARCYBER CDR to make decisions and accept risk beyond his/her scope.

In June 2020, Headquarters Department of the Army (HQDA) published HQDA Execution Order (EXORD) 211-22 requiring planners to identify Commander Critical Mission Threads and their corresponding Mission Engineering Threads, and the intelligence community to provide known and perceived threats. Finally, ARCYBER planners match those findings against the existing capabilities and capacity of ARCYBER and other Army resources to conduct DCO or provide mitigation. EXORD 211-22 outlines a process to prioritize DCO missions and related mitigation activities for approval by Army senior leaders and identifies residual risk which those leaders either accept or direct additional resources for action (see Figure 1). To address the various communication gaps and minimize confusion among all parties, we propose Mission Thread Analysis (MTA) by providing an analytical framework where all stakeholders detail their operational and technical requirements, while providing threat-informed analysis to advise and optimize DCO planning and execution.

In 2013, the Department of Defense (DoD), in collaboration with Carnegie Mellon University's Software Engineering Institute, developed the concept of a "Mission Thread Workshop." The collaboration resulted in defining "mission thread" as a sequence of end-to-end activities and events, given a series of steps, that provide one or more of the capabilities that the "system of systems" supports.[16] The introduction of a mission thread perspective has shifted focus from individual systems or equipment as stand-alone components to the realization that effective cybersecurity

must involve the identification of end-to-end data flows, usually across multiple systems.[17] Out of this understanding and the lessons learned over numerous defensive cyber operations,[18] ARCYBER planners designed the concept of Mission Thread Analysis to improve the efficiency and capacity of CPTs[19] and to support increased support from the ARCYBER staff.

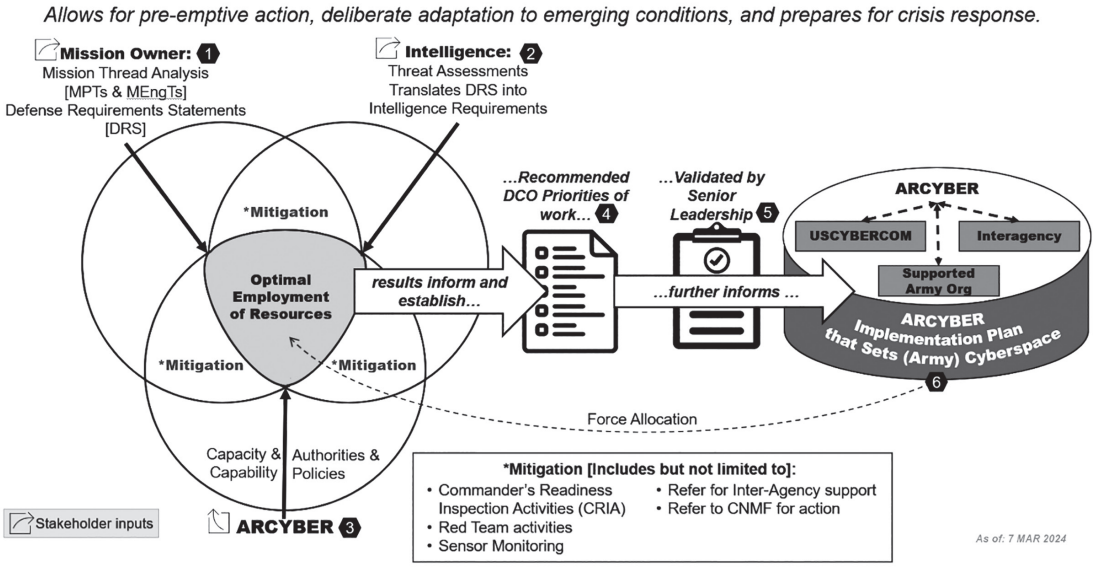


Figure 1. Optimization of Defensive Cyber Operations.[15]

Figure 1 starts with an MTA. This step requires mission owners to analyze and prioritize their critical missions and conduct and MTA to determine their DCO requirements. Mission owners depict the process of a mission as a series of steps or actions required to achieve successful accomplishment. For clarity, we call this the Mission Process Thread (MPT).[20] See Textbox 2, Mission Process Thread.[21] The MPT could be as simple as articulating a "kill chain." For example, an air defense radar detects enemy aircraft sending information to an engagement control station, and the personnel in the engagement control station communicate with the air space coordination authority to confirm the target and gain clearance of fires (see Table 1). Once cleared to fire, the battery fires a surface-to-air missile against the enemy aircraft on order of the engagement control officer. While that kill chain scenario is only part of the story, the steps tell us "what" and a little about "who" and "how," but not the details or the systems and networks involved. To get those details we need to examine the second part of MTA, the Mission Engineering Thread.

Defining "Mission Process Thread"

Based upon classified reports, notes, and AAR data following efforts to plan for and execute defensive cyberspace operations, we identified patterns of confusion across supported commands. In practice, we discovered that participants confused and interchangeably used the terms Mission Thread and Mission Engineering Thread. To alleviate the confusion of participants in MTA efforts, ARCYBER uses the term Mission Process Thread to distinguish between the two original terms. Mission Process Thread and Mission Thread share the same definition found within the "DoD Mission Engineering Guide."

Textbox 2

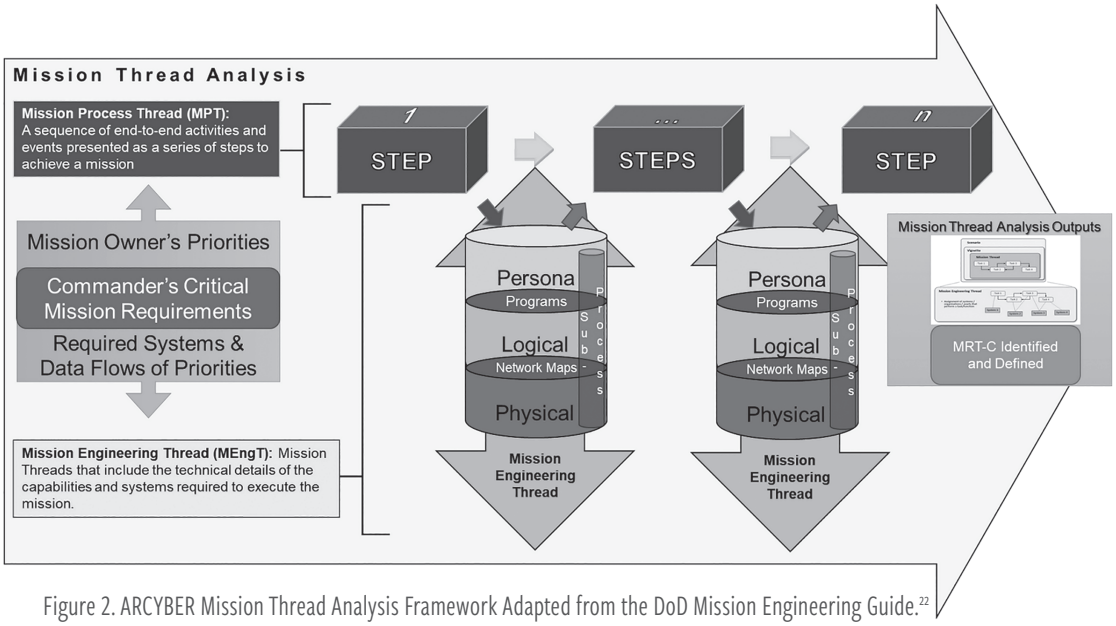


Figure 2. ARCYBER Mission Thread Analysis Framework Adapted from the DoD Mission Engineering Guide.[22]

The Mission Engineering Thread[23] (MEngT[24]) includes the hardware, systems, and networks that support the data pathways across the Persona, Logical, and Physical layers of cyberspace required to complete the mission, as described by the MPT.[25] In the example above, we would

Components of ARCYBER's Mission Thread Analysis

Mission Process Thread (simplified)	Mission Engineering Thread (simplified)
Sense to observe and identify air threats	Radar, detects aircraft through electromagnetic spectrum detection, communicates air picture through data passed to engagement control station via fiber network
Identify aircraft, detect track, provide early warning	Engagement control station receives and analyzes data portraying the target on the engagement control screen; the engagement control system identifies the track as hostile based on internal database prompting early warning alert sent as digital message over multiple command and control networks (SIPR, Mission Command Systems, Link16, fiber to big voice, and cellular messaging systems
Track aircraft, determine friend or foe	Radar and engagement control station continue to communicate track updates via fiber, track data is forwarded to the area air defense coordination cell for awareness via Link16
Confirm enemy track, gain clearance of fires	Voice and or data messaging used to confirm enemy aircraft via HF radio, TACSAT, Link16, and VOIP to communicate clearance of fires
Confirm track, fire missile, engage aircraft	Radar and engagement control station continue communicating updates via fiber, order to fire provided to system manually initiating engagement and missile launch via fiber and or line-of-sight communications
Track missile engagement, confirm battle damage assessment	Radar continues to communicate track data to the engagement control station via fiber, receives data regarding missile launch via line-of-sight communications and begins communicating with the missile in flight via HF encrypted messages to provide course correction; radar detects engagement via electromagnetic spectrum observation noting the destruction of track
Return to previous status: sense to observe and identify air threats	Operators confirm engagement with the airspace coordinator via voice or data systems and return all detection and firing systems to previous status via commands over fiber in order to observe additional threats

Table 1. Example: Fictional Kill Chain to Represent Application of MTA.

identify the MEngT from the point of detection by the radar to the system communication with the engagement control station, voice or data communication with the airspace coordination authority, continued communication between the engagement control system and the radar system, followed by the transmission of "fire" to the launching station and the follow-on data flows between various systems to complete the engagement. Identifying these MPTs and MEngT provides a complete MTA. Table 1 provides more detail on this MTA.

This fictional "kill chain" is an oversimplification to provide a broad overview of the nuances between MPT and MEngT. In the Army, we typically receive the MPT from the Operations Officer (S3 or G3). The organization's Signal Officer or Communications Officer typically provides the MEngT that includes the technical elements necessary to execute the data flows associated with all the systems and networks required to accomplish the mission. In the past, Mission Commanders would express their need to execute critical missions and request "protection" or the need to have "mission assurance." This approach required significant research and understanding by CPTs prior to their mission execution. Additionally, CPTs required very detailed technical data on specific systems or portions of networks. Although systems and databases exist to provide this information, they tend to be outdated due to lacking organizational/system owner compliance.[26] Only through gaining a full understanding of the processes and systems involved in a particular mission can CPTs have a running start to execute their mission most efficiently and effectively. The coherent identification of requirements resulting from the MTA enables ARCYBER to begin prioritizing missions and identifying risks in preparation for planning DCO missions over time.

With MPTs and MEngTs developed, the MTA provides both non-cyber and cyber representatives a common framework and shared understanding of the problem. Capturing the results of an MTA in a Defense Requirements Statement (DRS)[27] enables ARCYBER to make informed decisions about establishing priorities of work for DCF employment. The DRS is a simple fill-in-the-blank or "Mad-Libs" format that a mission owner uses to articulate its protection and defense requirements in cyberspace. The DRS allows easier understanding by mission owners of their own requirement. Further, the blanks guide the mission owner to provide the basic information required to start DCO planning and prioritization. The DRS also supports ARCYBER participation in USCYBERCOM's Cyber Forces Mission Allocation Process (CFMAP).[28] The CFMAP allows USCYBERCOM to make informed decisions on mission prioritization and apportionment of forces across the services and the various Joint Force Headquarters - Cyber (JFHQ-C). MTA also enables identification of DCF training requirements to be completed before rendering assistance. MTA enables development of the rough time estimates for a DCF to complete the mission. The MTA and the DRS serve as a confirmation brief between all parties related to the DCO mission. Finally, with the definition of MRT-C above, MTA allows for a mission analysis that will support discussions and planning with IA partners regarding the protection of MRT-C that resides outside of DoD Cyberspace.

Another value of the DRS is that it serves to start the creation of intelligence requirements within ARCYBER and the larger Intelligence Community. As captured by Figure 1 in step two, the DRS start to inform existing collection management, single source reporting, and ultimately synthesis into an all-source intelligence product regarding threats to known MRT-C. With this intelligence in hand, determinations are made regarding threats to MRT-C and if any action needs to be taken. If a response is required, step three covers determining what form that response takes. A specific response takes into account existing priorities of work and existing authorities. From there the response takes the form of a CPT under the direction of ARCYBER or if a broader response from USCYBERCOM or an interagency response is required. MTA enables ARCYBER to move from being asked to "Cyber all the things," to focus on defending specific Mission Relevant Terrain-Cyber (MRT-C)[29] for a specific Mission Owner purpose.

While the DCO-Optimization process, supports timely tactical execution of DCO, the MTA and its results also support long-term strategic decisions made by ARCYBER and beyond in steps four and five. USCYBERCOM allocates CPTs to the Army to conduct DCO through both active defense missions and providing passive measure plans to network operators based on data analytics and intelligence reports. By ARCYBER consolidating and submitting DRS to USCYBERCOM, it helps inform future force allocation decisions. Further, those same DRS help inform priority of work decisions by ARCYBER and HQDA. The MTA informs prioritization, force allocation decisions, and future intelligence requirements. MTA enables prioritization of DCO missions through a more coherent understanding of the processes and systems involved, compared to Army priorities further supported by intelligence reporting that enables better risk analysis. So while the other Army Service Component Commands (ASCCs) have "Set the Theater" tasks; as depicted in step six ARCYBER has a "Set Cyberspace" task for the Army and for portions of the Joint force.

For the Army, the MTA process helps ARCYBER to prioritize, train, employ, and resource Defensive Cyber Forces (DCF),[30] optimizing employment of these limited resources by matching the requirement with the right-sized DCF element and skill set. The MTA is not designed to be Army specific, it was designed to be service and department agnostic. MTA also identifies remaining gaps requiring mitigation or acceptance of risk at by the appropriate decision-making authority. Appropriate prioritization allows ARCYBER to apply limited capacity against the highest concerns and risks from the Army's perspective. Effective optimization of the Cyber Protection Force (CPF) allows ARCYBER to apply the right capabilities against appropriate problem sets, which sometimes requires significant training or even certification prior to mission execution. For example, training personnel to defend data appropriately in the Amazon Web Services (AWS) cloud requires X months of training and certification, while training personnel to defend Microsoft (MS) Azure cloud requires separate training lasting Y months. Finally, the combination of prioritization and optimization better positions ARCYBER to recommend which forces to re-mission during crises when emerging requirements dictate a shift in resources.

Different cultures and lexicons of customers (operations and mission commanders), cybersecurity and cyberspace security providers (like those across the DoD), Inter-Agency (IA) partners, the private sector, and non-federal jurisdictions all create friction that negatively impacts the government's ability to contend with the effects caused by Malicious Cyber Actors (MCA). MTA helps translate the needs and requirements among the cultures by providing a framework that utilizes definitions used in common that are easily understood by all cultures and varying levels of cyber expertise. To overcome this friction, ARCYBER is incorporating concepts from the DoD Mission Engineering Guide, Carnegie Mellon University's Software Engineering Institute's "Introduction to the Mission Thread Workshop," and RAND Corporation's "Cyber Mission Thread Analysis: A Prototype Framework for Assessing Impact to Missions from Cyber Attacks to Weapon Systems," to inform and establish MTA as a formal process in support of HQDA EXORD 211-22 "Army Support to Defensive Cyberspace."

ARCYBER's Operational Lessons Learned

This ARCYBER depiction of Mission Thread Analysis takes the original model established within the DoD Mission Engineering Guide and expands Mission Engineering Threads into an abstraction that depicts the detail required to support Defensive Cyberspace Operation planning and execution. A detailed abstraction requires Mission Owners to start identifying, defining, and depicting Mission Relevant Terrain – Cyber both on and off DODIN required for the successful completion of a mission.

Textbox 3

Based on ARCYBER's operational lessons learned over the past several years,[31] a thorough MTA enables a common framework to facilitate discussions, establish common understanding of the problem across cultures, and establish priorities of work for conducting DCO, with impacts on cybersecurity and cyberspace security efforts writ large. Establishing MTA as a common framework to facilitate DCO planning and execution allows cyber and non-cyber

Data Rationalization Effort as a Way of Understanding MTA

In the summer of 2023, ARCYBER commissioned a study to provide an end-to-end visualization and analysis of the DoDIN-A enterprise information systems data environment, including DoDIN Operations and Defensive Cyberspace Operations processes. The process generated a complex diagram depicting the "ARCYBER Data Ecosystem Current State." The undertaking involved surveying and mapping hundreds of data feeds being ingested and used across the ARCYBER Enterprise considered mission essential for operating and defending the DoDIN-A. The exhaustive effort included nearly 300 interviews across 13 organizations within the ARCYBER Enterprise. The deliverable included a current state, high-level visual overview of ARCYBER's data ecosystem. To achieve this outcome, planners researched the following questions:

1) What data does ARCYBER have?
2) Where are the data going?
3) What decisions are made with the data?
4) Who uses the data?
5) What are the data gaps?

The results provided the ARCYBER Commander with a mission commander's understanding of various MPT, along with seven actionable recommendations, which included improvement to empower cyber defenders to defend critical networks and associated mission process threads more proactively. The power of the "ARCYBER Data Ecosystem Current State" visualization has led the ARCYBER Commander and Technical Warfare Center leadership team to brief the findings to the Secretary of the Army, the Chief of Staff of the Army, the Principal Cyber Advisor, the Army Chief Information Officer, and the HQDA G-6, as well as numerous Congressional Delegations.33

ARCYBER Example

stakeholders to have a common understanding of the problem and effectively communicate priorities and identify risk. More importantly, MTA helps leaders more clearly sense and better understand[32] threats and vulnerabilities within the cyberspace domain, enabling well-informed decisions, and allowing the optimal employment of cyber protection forces as they act in partnership with Inter-Agency, industry, and allied partners.

Mission Thread Origins

Various definitions of "Mission Threads" are in use within systems engineering, mission engineering, and software engineering disciplines to describe and depict processes. While the disciplines share a common use of process maps, they differ radically in how they depict the processes they describe. While acknowledging the differences in the definitions used by the disciplines, the ARCYBER MTA process is grounded in the Mission Thread and Mission Engineering Thread definitions found within the DoD Mission Engineering Guide. The Mission Engineering approach recognizes the cross-disciplinary nature of the systems within a system-of-systems required to execute and accomplish a mission. Mission Engineering also shows the distinction between accounting for the steps required to achieve a mission and the technical details behind the systems that support the data flow within and between systems to support a mission. Given this background, Mission Thread Analysis uses the terms Mission Process Thread and Mission Engineering Thread to capture both the operational and the technical process details to better support DCO planning and execution in support of mission owners.

ARCYBER's Cyber Protection Brigade has been performing mission analysis based on Mission Threads with mission owners for several years. One of the benefits of MTA is that earlier mission analysis enables optimization of limited DCO capacity. Advanced analysis prior to mission execution allows the CPT to focus on mission planning rather than having to research the technical details of the mission environment, enabling significant time savings. This optimization of resources makes it possible for Defensive Cyber Forces (DCF) to perform more missions over a given period.

Mission Thread Analysis Process

The MTA starts with the identification of a Mission Process Thread. Developing Mission Process Threads is a G3/S3/Mission Owner responsibility and is based on the commander's prioritization of missions/key processes (see Textbox 4). Without established priorities from the commander/G3/S3/Mission Owner, the G6/S6/Chief Information Officer (CIO) and supporting Information Technology Department must make educated guesses about the criticality and potential risk to mission processes and associated systems. Conversely, if the commander focuses protection requirements on missions, a G6/S6/CIO will gain a better understanding of potential vulnerabilities and protection requirements. Moreover, asset-focused requirements obscure the entirety of mission requirements, particularly those that *reside off-DoDIN or outside*

Elements of Mission Thread Analysis

"Developing..." is an iterative process of Identifying, Defining, and Depicting Mission Process Threads and Mission Engineering Threads collaboratively.

Identify, Define, and Depict, cover an ever-increasing amount of detail:

- **Identify** is only the name of the task or system requiring further analysis.
- **Define** covers answering basic questions in words that include, but not limited to the steps of the process, where MRT-C resides, who is responsible for the MRT-C, etc...
- **Depict** provides the most detail and the term is used for the final graphics or network map that show a MT and/or MEngT.

This stratification establishes the different levels of details required to make certain decisions, making clear this is an iterative process to increase understanding. Previously, directives tasked organizations to engage in the daunting task of creating comprehensive network maps without any priorities. Progressing iteratively provides priorities of work for mapping/depicting efforts. Additionally, the stratification provides for a demarcation where the effort must stop if it starts to identify MRT-C that resides off-DDIN. For off-DDIN MRT-C, the task is to identify and define resources only to the extent that it is useful for conversations with IA Partners. The intent is not to depict off-DDIN MRT-C and run afoul of Intelligence Oversight concerns or to violate limitations of authorities.

Textbox 4

the span of control or responsibility of the commander/mission owner. Focusing on a Mission Process Thread, rather than specific assets, assists in more accurately identifying MRT-C outside of a unit's responsibilities and/or off DoDIN. In other words, focusing on assets that an organization owns versus focusing on what it uses as a customer, omits potential vulnerabilities and systems required for operations/mission execution.

Once the G3/S3 or a commander approves final MPT products, the development of Mission Engineering Threads (MEngT) can begin in earnest. An MEngT describes and depicts the processes and systems that handle data connecting the operational steps outlined in the Mission Process Thread. An MPT will have more than one MEngT and those MEngTs are likely to grow in complexity as analysis continues into further steps of the MTA. MEngTs include, but are not limited to systems, information exchanges, nodes, and data storage. In the context of relevant cyber capabilities, the MEngTs include the Persona, Logical, and Physical layers of cyberspace as defined by JP 3-12[34] and within FM 3-12.[35] *In simpler terms, a MEngT is comprised of the programs and pathways that the data take to move from one step to the next within the MPT.*[36] Developing MEngTs is an iterative process, increasing technical detail with each iteration. For the sake of understanding how much detail is within an MEngT, ARCYBER uses the term "Identify, Define, and Depict" to measure the amount of detail at hand. "Identify" is simply the naming convention of processes or systems requiring protection. "Define" covers the answers to the "5Ws" and captures "who" is responsible for the system (and how to contact them) and "where" the system is physically located. "Depict" covers the network map of the processes and systems requiring protection. These three levels of detail help measure progress, support prioritization decisions, support force allocation decisions, and capture technical details required by DCF to plan and execute DCO.

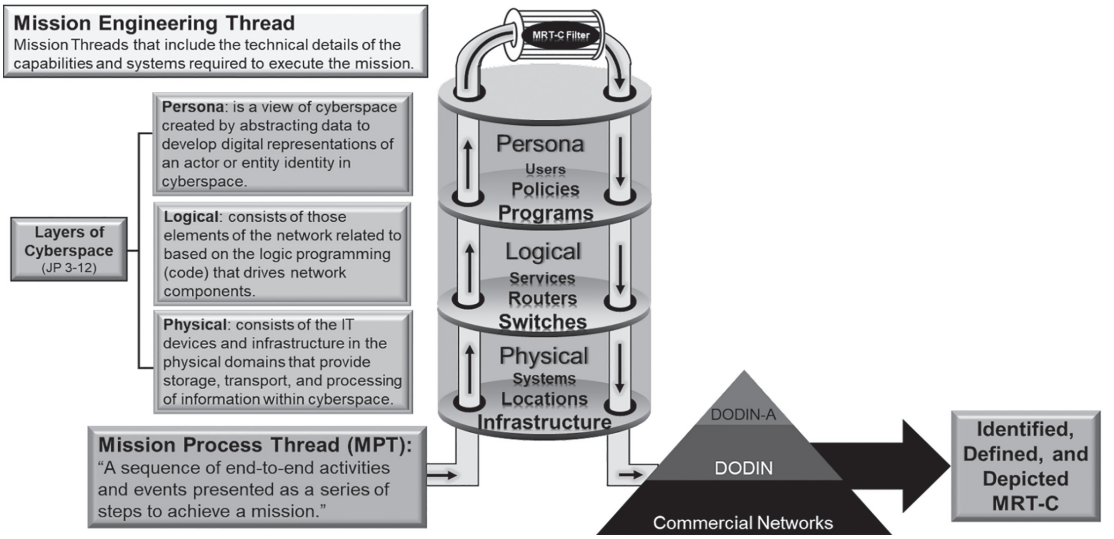


Figure 3. ARCYBER Mission Thread Analysis Framework

For the sake of Mission Thread Analysis, the first iteration of developing MEngTs should identify, in broad terms, what MRT-C[37] is required to complete a step and move to the next step within an MPT across the three layers of cyberspace (physical, logical, and Persona) and where the MRT-C resides (in terms of DoDIN-A, elsewhere on DoDIN, or within Commercial Networks). The first iteration of MEngT development also identifies the responsible organization for those programs/networks and their physical location.

Before going further, it is important to cover and reconcile the different definitions of MRT-C. Failure to reconcile these MRT-C definitions used by Defensive Cyberspace Operations and Mission Assurance has created confusion and considerable friction in the conduct of DCO over the past six years. Different from asset-focused approaches, MTA efforts focus on identifying MRT-C more broadly. The current definition of MRT-C is contained in USCYBERCOM Cyber Warfare Publication 3-0.1 – "Identification of Mission Relevant Terrain in Cyberspace (MRT-C)," 20 August 2021. It defines MRT-C as "All devices, internal/external links, operating systems, services, applications, ports, protocols, hardware, and software on servers, required to enable the function of a critical asset; may exist external to the DoD cyberspace."[38] This definition of MRT-C is in keeping with the original intent of the various series of orders that originally coined the term back in 2017 by acknowledging MRT-C can exist off-DoDIN,[39] and overcomes the friction caused by truncated versions of the MRT-C definition that have emerged since.

MRT-C Depiction

Compromises occur across all the three layers of cyberspace (Physical, Logical, and Persona). A portion of MTA is to determine what MRT-C exists before employment of any DCF and to capture information about MRT-C. Example: Where does the MRT-C reside physically, who is responsible for the MRT-C, and contract information. Determining where MRT-C resides and who is responsible for said MRT-C is critical for determining who within the federal government has the authorities for responding to threats to MRT-C.

Textbox 5

Mission Assurance professionals define MRT-C as "Cyber analysis that includes documenting devices, internal and external links, operating systems, services, applications, ports, protocols, hardware, software, and other technical aspects of a system required for the function of a critical asset."[40] The omission of "may exist external to DoD cyberspace" within the Mission Assurance definition of MRT-C leads planners to focus solely on assets owned by an organization (or only on/within DoDIN), but overlook what MRT-C exists elsewhere, specifically off-DoDIN. The unintended consequence of this omission is that units limit their Mission Assurance analysis to the MRT-C under their direct control. Such analysis comes at the expense of overlooking MRT-C that is within the commander's Area of Interest that the unit requires to accomplish its mission. This has unwittingly created a gap in understanding what processes or systems require consideration for protection and what is needed to frame that understanding in a way that allows mutual support with the interagency in a crisis.

Using different definitions of MRT-C in Mission Assurance and Defensive Cyberspace Operations results in units duplicating efforts and creates a gap between identified unit-owned MRT-C protection requirements and protection requirements for MRT-C used by a unit to accomplish its mission that reside elsewhere, whether on or off DoDIN. What follows is an attempt to reunify both efforts by providing one definition across both Mission Assurance and Defensive Cyberspace Operations. To overcome friction caused by differing definitions, we define MRT-C as, "All devices, internal/external links, operating systems, services, applications, ports, protocols, hardware, and software on services required to enable the function of a critical asset *and/or for the completion of a mission;* ***may exist external to DoD Cyberspace***." Inclusion of the emphasized portion of the definition of MRT-C accounts for both Mission Assurance and DCO requirements, enabling more effective planning and reduction of cybersecurity related

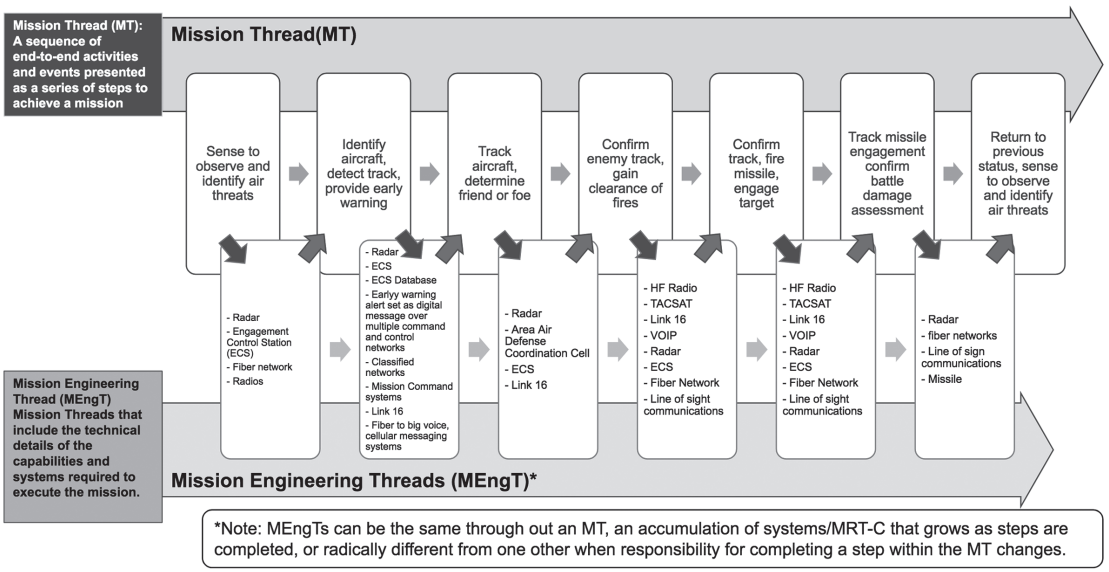


Figure 4. Visualization of Table 1 Mission Thread Analysis of Air Defense Kill Chain Engagement.[41]

risk. Following ARCYBER's back-brief on HQDA EXORD 211-22, Army senior leaders approved this definition during an Army Synchronization Meeting in October 2022 for socialization with other stakeholders and for incorporation into future doctrine and policy.

The completion of MTA triggers the initiation of Mission Thread Defense (MTD) by the Cyber Protection Brigade based on its priorities of work. MTD is the deliberate defense of MEngT (including MRT-C) to support a Mission Owner's designated MPT or critical operational missions by another name (e.g., air defense kill chain). The process identified as MPTs (e.g. detect, provide early warning, track, engage, BDA) during the MTA are those processes, that if compromised, would lead to overall mission failure (e.g. failure to destroy air threat). A successful MTA establishes priorities of work for DCF (by prioritizing excess demands against limited capacity), the details required for a successful MTD (analytics, threat, MRT-C), where (and if) IA support is required (beyond DoD authorities or access), and the identification of risk and authority of risk acceptance if the volume of requirements exceeds the capacity of USCYBERCOM and the IA.

CONCLUSION

MTA enables military organizations and private-sector companies to articulate their cybersecurity and cyberspace security needs more effectively to cyberspace security professionals across the DoD, the Interagency, and private cybersecurity partners. Using clear and concise terms in a manner designed to overcome institutional and cognitive biases enables more effective support and greater potential for optimizing limited resources. As organizations develop MPTs and MEngTs they translate their cyber protection needs across operational and technical frames of reference that can be used by ARCYBER, elsewhere within USCYBERCOM, and by the Interagency when and where appropriate. The MTA approach is also useful when the cyber protection function is performed by allies, sister service defensive cyber forces, Inter-agency partners, the private sector, or any other party – regardless of whether the protection teams are familiar with the process they are protecting. The Army's use of Mission Thread Analysis informs critical training requirements, force management decisions, and helps establish priorities of work for Cyber Mission Forces. A unit's completion of a Mission Thread Analysis helps gather technical details that support DCO execution and gives the unit an opportunity to articulate their priorities more effectively for protection. By encouraging the use of Mission Thread Analysis across the Army, ARCYBER intends to increase efficiency and optimize employment of limited resources, while addressing the different approaches by various stakeholders to counter or mitigate the efforts of Malicious Cyber Actors. These benefits will also accrue to others who implement MTA or a suitable adaptation.

DISCLAIMER

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

NOTES

1. George W. Bush, "National Security Presidential Directive-54," and "Homeland Security Presidential Directive-23," (January 2008). Cybersecurity is defined as the "Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. More commonly, "The process of protecting information by preventing, detecting, and responding to attacks. See also NIST: https://csrc.nist.gov/glossary/term/cybersecurity.
2. Department of Defense Dictionary of Military and Associated Terms (2023): 49. Department of Defense, Joint Publication 3-12 (December 2022): II-6. Department of the Army Field Manual 3-12 (August 2021): 2-6. Note: Each of these publications define "Cyberspace Security" as: "Actions taken within protected cyberspace to prevent unauthorized access to, exploitation of, or damage to computers and networks, including platform information technology."
3. Department of Defense, "Joint Publication 3-12 Joint Cyberspace Operations" (December 2022): II-6. Note: Cyberspace Defense: actions are taken during DCO-IDM missions, within protected cyberspace, to discover and defeat specific threats that breach, threaten to breach, or are suspected to have breached the cyberspace security measures, to include actions that detect, characterize, fix, contain, clear, and recover/restore from Malicious Cyber Activity, including malware or the unauthorized activities of authorized users.
4. Department of Defense, "Joint Publication 3-12 Joint Cyberspace Operations," (December 2022): II-4. Note: Cyber Protection Forces conduct "Defensive Cyberspace Operations," or "DCO missions," to defend blue cyberspace from imminent or active threats in cyberspace. Specifically, DCO missions preserve the ability to utilize blue cyberspace capabilities and protect data, networks, cyberspace-enabled devices, and other designated systems by defeating ongoing or imminent malicious cyber activities.
5. Donald Firesmith, "Mission thread Analysis Using End-to-End Data Flows – Part I," SEI Blog, Software Engineering Institute, Carnegie Mellon University. https://insights.sei.cmu.edu/blog/mission-thread-analysis-using-end-to-end-data-flows-part-1/
6. ARCYBER lessons learned in operational archives 2015-2022, from named, classified operations: UTMOST GOLF (Logistics), UTMOST CHESS (Power Projection), ROMAN GUARDIAN (Mission Partner Environment), UTMOST SASQUATCH (Critical Production Lines). Authors' note: The classified reports associated with each of these operations (and others) are not available publicly. Where appropriate and necessary, the authors can provide real-world examples based on clearance and need-to-know.
7. Department of the Army, "Field Manual 3-90 Tactics" (May 2023): 6-7.
8. Department of the Army, "Field Manual 3-12 Cyberspace Operations and Electromagnetic Warfare," (August 2021): 2-7.
9. Department of Defense, "Joint Publication 3-12 Joint Cyberspace Operations," (December 2022): II-7
10. Mark Esper, "Definition of 'Department of Defense Cyberspace Operations Forces (DoD COF)'" (official memorandum, Washington, DC, Department of Defense) 2019. NOTE: The term Defensive Cyber Forces (DCF) captures Cybersecurity Service Providers (CSSPs), Cyber Protection Teams (CPTs), CPT Mission Elements, USAF Mission Defense Teams (MDTs), and other forces whose primary functions are to protect or defend Department of Defense Information Networks. Commonly used terminology within USCYBERCOM and Cyber Mission Forces, but not included in the Department of Defense Dictionary of Military and Associated Terms.
11. ARCYBER Lessons Learned in Operational Archives 2015-2022, from named, classified operations: UTMOST GOLF (Logistics), UTMOST CHESS (Power Projection), ROMAN GUARDIAN (Mission Partner Environment), UTMOST SASQUATCH (Critical Production Lines).
12. United States Congress, National Defense Authorization Acts 2015-2024, Congress.gov | Library of Congress: FY2024 HR 2670 (PUBLIC LAW 118-31—DEC. 22, 2023), Sections 1511, 1512, 1517, and 1553; FY2023 HR 7776 (PUBLIC LAW 117–263—DEC. 23, 2022), Sections 1504, 1509,1510, 1511, 1559, 1636, and 1656; FY2022 S 1605 (PUBLIC LAW 117–81—DEC. 27, 2021), Sections 1505, 1525, 1542, and 1543; FY2021 HR 6395 (PUBLIC LAW 116–283—JAN. 1, 2021), Sections 1721, 1724, and 1736; FY2020 S1790 (PUBLIC LAW 116–92—DEC. 20, 2019), Sections 1638, 1660, and 6504; FY2019 HR 5515 (PUBLIC LAW 115–232—AUG. 13, 2018), Sections 1642, 1647, 1648 and 1650; FY2018 HR 2810 (PUBLIC LAW 115–91—DEC. 12, 2017), Sections, 1638, 1643, and 1651; FY2017 S 2943 (PUBLIC LAW 114–328—DEC. 23, 2016), Sections 1645 and 1650; FY2016 S1356 (PUBLIC LAW 114–92—NOV. 25, 2015), Section 1647; FY2015 HR 3979 (PUBLIC LAW 113–291—DEC. 19, 2014), Sections 1632 and 1634. Each of these National Defense Authorization Acts directed United States Cyber Command and the military services to conduct a variety of cyber security related assessments and defensive cyber operations activities that the Army and USCYBERCOM routinely assign to ARCYBER for execution by Defensive Cyber Forces, specifically Cyber Protection Teams, their analytic support elements, and network operators.

NOTES

13. Dina Temple-Raston, "A 'Worst Nightmare' Cyberattack: The Untold Story of the SolarWinds Hack," National Public Radio. https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack
14. Department of the Army, "HQDA EXORD 211-22 Army Support to Defensive Cyberspace," (Jun 2022): 6. A classified document outlining the process to optimize Defensive Cyber Operations and assess risks to the force.
15. George Corbari, Paul Stanton, and John Popiak, "ARCYBER Confirmation Briefing" provided to Army Synchronization Meeting September 2022 and multiple follow-on Army Senior Leader briefings to the Secretary of the Army, Army Chief of Staff, Army Principal Cyber Advisor, and Army Chief Information Officer between October 2022 and October 2023.
16. Michael Gagliardi, William Wood, Timothy Morrow, "Introduction to the Mission Thread Workshop," Software Engineering Institute, Carnegie Mellon University. https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=63148
17. Donald Firesmith, "Mission thread Analysis Using End-to-End Data Flows – Part I," SEI Blog, Software Engineering Institute, Carnegie Mellon University. https://insights.sei.cmu.edu/blog/mission-thread-analysis-using-end-to-end-data-flows-part-1/.
18. ARCYBER Lessons Learned in Operational Archives 2015-2022, from named, classified operations: UTMOST GOLF (Logistics), UTMOST CHESS (Power Projection), ROMAN GUARDIAN (Mission Partner Environment), UTMOST SASQUATCH (Critical Production Lines). Authors' note: The classified reports associated with each of these operations (and others) are not available publicly. Where appropriate and necessary, the authors can provide real-world examples based on clearance and need-to-know.
19. Department of Defense, "The DoD Mission Engineering Guide," (NOV 2020): 38. Note: The guide defines a Mission Thread as, "A sequence of end-to-end activities and events presented as a series of steps to achieve a mission."
20. Department of Defense, "The DoD Mission Engineering Guide," (NOV 2020): 38. Note: The guide defines a Mission Thread as, "A sequence of end-to-end activities and events presented as a series of steps to achieve a mission."
21. US Army Cyber Command, Internal Lessons Learned from After Action Reports from deliberate, named Defensive Cyberspace Operations (2014-present). ARCYBER lessons learned including classified operations: UTMOST GOLF (Logistics), UTMOST CHESS (Power Projection), ROMAN GUARDIAN (Mission Partner Environment), UTMOST SASQUATCH (Critical Production Lines). These specific operations enabled ARCYBER planners to identify gaps and apply lessons learned in the development and validation of the concepts Mission Process Thread and Mission Thread Analysis.
22. Department of Defense, "The DoD Mission Engineering Guide," (NOV 2020): 14-19. Note: Authors adapted Figures 2-5 and 2-9 (pages 14 and 19) when creating these proposals.
23. Department of Defense, "The DoD Mission Engineering Guide," (NOV 2020): 37. Note: Defines Mission Engineering Threads as "Mission threads that include the technical details of the capabilities and systems required to execute the mission."
24. Department of Defense, "The DoD Mission Engineering Guide," (NOV 2020): 37. Note: The authors use MEngT as an acronym to prevent confusion with Mission Essential Task and its acronym "MET."
25. Department of Defense, "The DoD Mission Engineering Guide," (NOV 2020): 37. Note: Defines Mission Engineering threads as "Mission threads that include the technical details of the capabilities and systems required to execute the mission."
26. US Army Cyber Command, Internal Lessons Learned from After Action Reports from deliberate, named Defensive Cyberspace Operations (2014-present). ARCYBER lessons learned including classified operations: UTMOST GOLF (Logistics), UTMOST CHESS (Power Projection), ROMAN GUARDIAN (Mission Partner Environment), UTMOST SASQUATCH (Critical Production Lines). These specific operations enabled ARCYBER planners to identify gaps and apply lessons learned in the development and validation of the concepts Mission Process Thread and Mission Thread Analysis.
27. United States Cyber Command, "(U) CFMAP Info Paper – DCO Requirements," (8 June 2022): 2-4. Authors Note: "Defense Requirements Statement" is an ARCYBER an attempt to translate the information requested by USCYBERCOM into a sentence for easier development of DCO needs and leader understanding of the requirement. Example: (fill in the blank) I*n support of [Plan] and [Sector] to perform [Objective/Effect], assist [Terrain Owner] within [DoDIN AO] by performing CPT functions upon [System/MRT-C] in order to protect [JMET/Mission] from [Threat].*
28. United States Cyber Command, "(U) Relationship between the Cyberspace Forces Mission Alignment Process (CFMAP) and the Global Force Management Allocation Plan," 5 March 2021: 1. NOTE: Cyber Force Mission Allocation Process (CFMAP) is a bi-annual USCYBERCOM process of assessing CCMD and Service requirements in cyberspace and, if or when necessary, recommends to the Secretary of Defense, the adjustment or re-allocation of capacity and missions of Cyber Mission Force.

NOTES

29. United States Cyber Command, "Cyber Warfare Publication 3-0.1 – Identification of Mission Relevant Terrain in Cyberspace (MRT-C)," (August 2021): GL-3.
30. Mark Esper, "Definition of 'Department of Defense Cyberspace Operations Forces (DoD COF)'" (official memorandum, Washington, DC, Department of Defense) 2019. NOTE: The term Defensive Cyber Forces (DCF) captures Cybersecurity Service Providers (CSSPs), Cyber Protection Teams (CPTs), CPT Mission Elements, USAF Mission Defense Teams (MDTs), and other forces whose primary functions are to protect or defend Department of Defense Information Networks. Commonly used terminology within USCYBERCOM and Cyber Mission Forces, but not included in the Department of Defense Dictionary of Military and Associated Terms.
31. US Army Cyber Command, Internal Lessons Learned from After Action Reports from deliberate, named Defensive Cyberspace Operations (2014-present). ARCYBER lessons learned including classified operations: UTMOST GOLF (Logistics), UTMOST CHESS (Power Projection), ROMAN GUARDIAN (Mission Partner Environment), UTMOST SASQUATCH (Critical Production Lines). These specific operations enabled ARCYBER planners to identify gaps and apply lessons learned in the development and validation of the concepts Mission Process Thread and Mission Thread Analysis.
32. Sydney Freedberg, "Army's New Aim is Decision Dominance," Breaking Defense, https://breakingdefense.com/2021/03/armys-new-aim-is-decision-dominance/. Note: Reports the ongoing work of the Combined Arms Center, Fort Leavenworth, ARCYBER and others; based on Army Senior Leader statements and guidance supporting the establishment of "Information Advantage Detachments" and "Information Advantage Task Forces. See also "Army Doctrinal Publication 3-13, Information," (November 27, 2023): 1-1 – 1-12.
33. Paul Son (US Army) and Michelle Paul (IT Cadre), "ARCYBER Data Rationalization Current State Visualization Report," (December 8, 2023): 1-5. NOTE: This report is classified as *Controlled Unclassified Information* and as such not publicly released.
34. Department of Defense, "Joint Publication 3-12 Joint Cyberspace Operations," (December 2022): I-2 – I-4.
35. Department of the Army, "Field Manual 3-12 Cyberspace Operations and Electromagnetic Warfare," (August 2021): 1-5.
36. Department of Defense, "The DoD Mission Engineering Guide," (NOV 2020): 37
37. United States Cyber Command, "Cyber Warfare Publication 3-0.1 – Identification of Mission Relevant Terrain in Cyberspace (MRT-C)," (August 2021): GL-3.
38. United States Cyber Command, "Cyber Warfare Publication 3-0.1 – Identification of Mission Relevant Terrain in Cyberspace (MRT-C)," (August 2021): GL-3.
39. Chairman of the Joint Chiefs of Staff PLANORD, "Identification of Mission Relevant Cyberspace Terrain Supporting Critical Assets," (18 April 2017); United States Strategic Command, "USSTRATCOM PLANORD 17-05, Identification of Mission Relevant Cyberspace Terrain Supporting Critical Assets, (17 May 2017); United States Cyber Command. "USCYBERCOM OPORD 17-0106, Identification of and Mapping of Mission Relevant Cyber Terrain Supporting Critical Assets," (29 July 2017).
40. Department of Defense Instruction (DoDI), "DoDI 3020.45, Mission Assurance Construct," (August 2018), Change 1, May 2, 2022: 72.
41. ARCYBER lessons learned in operational archives 2015-2022, from named, classified operations: UTMOST GOLF (Logistics), UTMOST CHESS (Power Projection), ROMAN GUARDIAN (Mission Partner Environment), UTMOST SASQUATCH (Critical Production Lines). Authors' note: Providing an accurate or real-world example of a complete Mission Thread Analysis would increase the classification of this article. To facilitate the widest possible dissemination of this document, the authors created an example to illustrate what an MTA might look like based on lessons learned from actual operations. By design, some details were left out to reduce potential targeting or threats to industry or systems within the example. Where appropriate and necessary, the authors can provide real-world examples based on clearance and need-to-know.

Beyond USCYBERCOM: The Need to Establish a Dedicated U.S. Cyber Military Force

COL Jeffrey Couillard

ABSTRACT

This paper explores whether the United States should establish a separate Cyber Military Force. The article begins with a brief review of current cyber threats to the United States, followed by a review of historical precedent and great power competition. It then analyzes the current cyber military structure to help identify potential gaps within the current approach to offensive and defensive cyber operations. To provide a possible course of action in the context of a recommended framework, the article proposes using a well-known military framework called DOTMLPF-P (Doctrine, Organization, Training, Materiel, Leadership & Education, Personnel, Facilities, and Policy). The methodology used is a qualitative literature review, including journal articles, military doctrine, historical references, subject matter expert articles, U.S. Government Accounting Office reports, cyber industry reports, and legislation. The research aims to bring readers to the conclusion that it is time to establish a separate U.S. Cyber Force.

Keywords *– Cyber, Cyber Defense, Cyberspace, National Security Strategy, National Cyber Strategy, Cyber Domain, Department of Defense*

INTRODUCTION

In 1947, President Harry S. Truman signed the National Security Act.[1] This act made numerous changes to the nation's defense and intelligence organizations including the establishment of the Department of the Air Force. In 2019, President Trump signed the National Defense Authorization Act (NDAA)[2] establishing the U.S. Space Force as a component under the Department of the Air Force, after roughly twenty years

Colonel Jeffrey (Jeff) Couillard is a war college graduate of the College of Information and Cyberspace at the National Defense University. He started his Army career as an enlisted Infantryman in 1988. He received a direct commission to the Signal Corps in 2005. During his 35 years of service, he has commanded at the company level and led a Regional Cyber Center. In addition to his command and leadership assignments, Colonel Couillard has served on staff at Headquarters, Department of the Army, the Army National Guard Bureau, Multi-National Forces – Iraq, and Joint Task Force Guantanamo. Colonel Couillard has been deployed numerous times, in support of Operation Desert Shield/Storm, Operation Iraqi Freedom, and Operation Enduring Freedom. He earned a Bachelor of Business Administration degree from Davenport University; a Master of Arts from Webster University; and a Master of Science from the College of Information and Cyberspace.

of effort and a congressional report on Space Matters.[3] This aligned a dedicated organization to the Space Warfighting Domain. The FY23 NDAA directed a Department of Defense (DoD) report on Cyber Matters,[4] echoing an FY00 DoD report on Space Matters.[5] The topic of Cyber Matters within the NDAA covers a wide range of questions, including total force generation.[6]

The question of a Cyber Military Force is not new, although most studies lack practical solutions.[7] The research details multiple problems but falls short of proposing actionable solutions. This article explores the requirement to establish a separate U.S. Cyber Military Force, detailing threats, precedent, and current gaps. Finally, the author provides a framework for the DoD to recommend Congress establish a separate U.S. Cyber Military Force.

Some suggest, including the former Commander of U.S. Cyber Command (USCYBERCOM), General Paul M. Nakasone,[8] that there is no need to establish a separate Cyber Military Force. When asked by U.S. Representative Pat Fallon, during the House Armed Services Subcommittee on Cyber, Innovative Technologies, and Information Systems, if Gen. Nakasone would "...accept command of a cyber service?"[9] Gen. Nakasone responded with the following:

> So Congressman, I would offer that you know that is obviously as you said a policy decision, but let me just provide a thought on this in terms of how we model ourselves and I think as you asked a number of different who (is)...in charge of special operations? Special Operations is not run by any specific service yet it is the lead service and capability that our nation has. That's what we have modeled ourselves at U.S. Cyber Command (after). This idea of having special and unique authorities that we're able to train and man and equip our force and agility to maneuver.[10]

This article counters Gen. Nakasone's view by highlighting the distinct need for cyber defense. Unlike U.S. Special Operations Command's (USSOCOM) non-permanent defensive role, USCYBERCOM must continuously defend the Department of Defense Information Network (DoDIN), the world's largest network.[11] Additionally, USSOCOM specializes in small-group tactics, offensive operations, and providing specialized training. While small-group tactics may work for Cyber Protection Teams (CPTs) responding to cyber-related incidents, it is not applicable to defending a global network.

This article proposes using the DOTMLPF-P (Doctrine, Organization, Training, Materiel, Leadership & Education, Personnel, Facilities, and Policy) framework to analyze and develop a Cyber Military Force, not as a panacea but as a starting point.

Threats

In March 2022, the Federal Bureau of Investigation's (FBI) Internet Crime Compliant Center (IC3) released its 2021 Internet Crime Report[12] showing a year-over-year increase in Internet Crime between 2017 and 2021, roughly a 68% increase each year. The total reported losses for 2021 were $6.9 billion.[13] Applying that same 68% increase to 2022 and 2023, the anticipated losses could be $11.6 billion and $19.5 billion, respectively. A way to reduce those losses is by identifying those supporting internet crime and cyber-attacks. Within the FY22 National Defense Strategy, the Pentagon stated that "China remains the 'pacing challenge'" and "identifies Russia as an 'acute threat.'"[14] Additionally, the Cybersecurity & Infrastructure Security Agency (CISA), under the Department of Homeland Security (DHS), published to their website Alerts (AA22-110A)[15] and (AA22-279A)[16] pointing to Russian and Chinese state-sponsored cyber threats. Continuing to pull that thread, North Korea and Iran both rise in relevance as state sponsors in CISA Alerts (AA22-187A)[17] and (AA22-320A).[18]

However, it is not just state-sponsored actors conducting these attacks. Mieke Eoyang, the Deputy Assistant Secretary of Defense for Cyber Policy, is quoted as saying,

> But I think we've seen over time with the development of the non-state actor – the criminal cyber market – is that capabilities that were once reserved for state actors are available on the dark web for purchase."[19]

According to Eoyang, the criminals "...are motivated by money." She said. "They're in it for the ransom. They're not necessarily in it for harming [the United States.]"[20]

What does this mean to the cyber defense of the United States? According to a September 2022 U.S. Government Accountability Office (GAO) report on Opportunities and Threats to the DoD's National Security Mission, the GAO found:

> Given the ubiquitous nature of the information environment, both DoD and adversaries can conduct operations and activities in the information environment from anywhere in the world. Additionally, with DoD capabilities dependent on IT and the electromagnetic spectrum (EMS), its ability to conduct operations and activities in any of the physical domains (land, maritime, air, and space) is reliant on protecting the information environment.[21]

Specific to threat actors, the GAO report offered that "National and DoD strategies recognize that nation-states...have demonstrated that they are threat actors in the information environment..."[22] Of the institutional challenges, the GAO report continues with:

> The challenges include a lack of leadership emphasis, lack of resources, the implications of new technologies, and dated processes. DoD components identified personnel, funding, IT, organization, and training as the most important institutional challenges they face related to the information environment.[23]

From the GAO report, with the specific details above, one can understand that the DoD and its components are not focusing on the cyber domain as much as necessary, which is critical to the other four warfighting domains.

Precedent for Organizing the Cyber Mission in DoD

From the time of Brigadier General Billy Mitchell in World War I to the 1947 National Security Act, which established the U.S. Air Force, aviators had continuously struggled to convince the U.S. Army that Air Power was more than a supporting effort to the land warfighting domain. In his doctoral thesis Dr. James P. Tate, Lt. Col. U.S. Air Force (Retired) stated, "Within the Army it was the conflict over budget as much as anything else that fueled the Air Corp's drive for independence."[24] Tate also includes in his thesis the congressional testimony of several aviators stating:

> During the hearings, the points of the airmen's argument emerged. The flyers argued that there were military missions for the air arm independent of the surface forces; that the airplane had an almost unlimited potential as a weapon; that the full power of the airplane could be reached only by an air arm controlled by men with knowledge and interest in aviation; that the leadership of the Army, especially the General Staff, lacked interest and knowledge in aviation and had subordinated the needs of the air arm to those of other combat arms; that a separate air service would prevent expensive duplication by concentrating the government's aviation activities under central control; that such an independent air service had been successful in Britain; and finally, that development of aviation under an independent air service would provide support, direction, and encouragement for the country's aviation industry which depended so heavily upon the military market. The best way to take advantage of the new technology in aviation was to create a new military organization.[25]

Within the above quote, one could easily replace "air" and "airplane" with "cyber" and present the same compelling argument. Of note, for use later, is the concept of the Air Force supplying pilots and support to the U.S. commercial air sector. Again, replacing "air" with "cyber" is something to remember when talking about the deficit of cyber talent for positions available within the United States.

Lastly, from Tate's thesis, "Congress passed the National Defense Act of 1920, which gave permanent legislative authority to the Air Service..."[26] Additionally, "The Air Service received authority to procure equipment."[27] Similarly, as Mark Pomerleau details in a Defense Scoop article, the FY22 National Defense Authorization Act "granted Cybercom enhanced budget authority... to maintain the cyber mission force."[28] It appears USCYBEROM is already following the same steps the U.S. Air Force took to separate from the U.S. Army.

Some suggest that a Cyber Military Force should mirror the development of the U.S. Air Force before founding Cyber as a separate military service. Of significance, the U.S. Air Force was established after World War II (WWII). This was a time when the nation was recovering from the war and the world was generally at peace, so the focus turned to reorganizing defense and intelligence organizations, including establishing the U.S. Air Force. Today, there is no similar armistice or peace treaty to end the ongoing cyberattacks commonly described as operating just below the threshold of armed conflict.

Additionally, if one uses the FY00 NDAA as the starting point, it took nearly twenty years to establish the U.S. Space Force. The FY00 National Defense Authorization Act (NDAA) compelled the DoD to produce a Report of the Commission to Assess United States National Security Space Management and Organization.[29] This report detailed how to establish a U.S. Space Force. Similar to the request for the report on Space Matters in the FY00 NDAA, Congress included language in the FY23 NDAA compelling the DoD to address the question of cyber matters.

The U.S. is not the only nation to establish new cyber military organizations. The German government created its Cyber Military Force in 2017. They established the organization to counter challenges perceived within the cyber domain. According to a recent German report, the German Cyber Military Force includes Cyber Security, Infrastructure, Intelligence, Applications, IT Management, Project Management, and Enterprise Architecture.[30] The German Cyber Military Force also conducts the organize, train and equip mission, providing a cyber-specific career pipeline. In 2022, this force began an effort to restructure based on experiences gained from the previous five years of operations.

Similarly, on October 28, 2022, Singapore established its cyber-focused Digital and Intelligence Service (DIS). According to Mike Yoe, an Asia correspondent for *Defense News*, the intel directorate within DIS,

> will support Singaporean military decision-making and operations through research and analysis, doctrines, standards, and best practices...

The article continues,

> (t)he DIS will also have four separate commands, plus a digital operations technology center. The four commands are tasked with joint intelligence, C4 [command, control, communication, and computers] cybersecurity, digital defense and training.[31]

In 2015, China established the Strategic Support Force (SSF) to consolidate their space, cyber, and electronic warfare (EW) efforts under a single unified force. According to Elsa B. Kania and John K. Costello,

> ...the SSF has integrated the PLA's [People's Liberation Army] capabilities for cyber, electronic, and psychological warfare into a single force within its Network Systems Department, which could enable it to take advantage of key synergies among operations in these domains.[32]

Relative to China's cyber force, in 2017 RAND Corporation published a report on "The Creation of the PLA Strategic Support Force (SSF) and Its Implications for Chinese Military Space Operations."[33] While focusing on space, the RAND report highlights that "The SSF is charged with overseeing Chinese military space, cyber, and electronic warfare capabilities..."[34] Within the report, RAND interviewed former Second Artillery officer, Song Zhongping of the PLA who said, "... that the SSF is an independent service 'unique in the world'." Song continues, "The goal of the SSF is to achieve cyber and electromagnetic superiority."[35] If China is the main competitor in global power competition, the SSF already has an eight-year lead maturing tools and tactics.

The Wrong Structure for the Job

Information Technology systems evolve over time. Information Technology support groups have iteratively reinvented themselves to react to that evolution. The same is true of IT organizations within DoD. In the U.S. Army, IT organizations have included: Data Processing, Information Systems and Support, Department of Information Management, Network Enterprise Centers, Theater Network Operations and Security Centers, and Regional Cyber Centers (RCCs) to name a few. One could assume the same to be true of the other services within the DoD, as it certainly is with USCYBERCOM as shown on their website history page.[36] USCYBERCOM is a functional combatant command, like U.S. Strategic Command (USSTRATCOM) and U.S. Transportation Command (USTRANSCOM), but supports global cyber operations for all DoD and all combatant commands. The Commander of USCYBERCOM is also the Director of the National Security Agency (NSA). Within USCYBERCOM are the Cyber National Mission Force (CNMF) and Joint Forces Headquarters – DoDIN (JFHQ-DoDIN). The Commander of JFHQ-DoDIN is also the Director of the Defense Information Systems Agency (DISA), an agency within the DoD (Figure 1).[37]

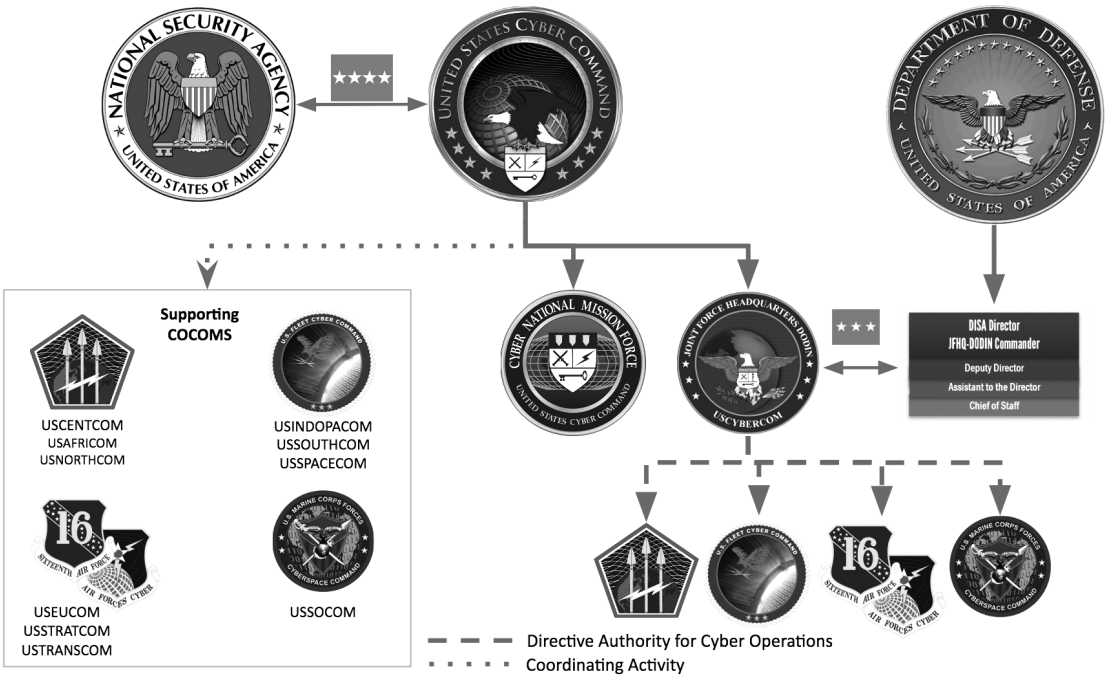


Figure 1: U.S. Army IT Organizations.

While the above figure shows some of the complexity, it is only the beginning. According to Maj. Eric Pederson, Maj. Don Palermo, Maj. Stephen Fancey, and Lt. Cdr. (Retired) Tim Blevins "The DoDIN is the biggest network in the world..."[38] and "...is composed of 44 different DoD components (and) constructed networks[39] across approximately 3,500 locations in 26 nations."[40] Just within the Army there are six RCCs, aligned with the Continental United States (CONUS), Europe, Pacific, Southwest Asia, Korea, and the National Guard. The RCCs support their portion of the DoDIN, including the Joint Regional Security Stacks (JRSS) provisioned by DISA. As shown in Figure 1, the various service Cyber Commands each support a Geographic Combatant Command. Although, even with that support, in 2023, U.S. Indo-Pacific Command (USINDOPACOM), according to the C4ISRNET website, "asked Congress for an additional $274 million to fund offensive and defensive cyber capabilities."[41] Of note, each service cyber command approaches its assigned combatant commands with different tools, methods, policies, and procedures.

Combatant Commanders rely on IT infrastructure to enable all aspects of operations and support (pay, health care, personnel actions, logistics, etc.). Each Combatant Commander's IT infrastructure becomes the defensive position the DoD must protect for orchestrating multi-domain operations. Additionally, that infrastructure is a regional portion of the global DoDIN. The greater the number of organizations charged with defending sections of that IT infrastructure, the greater the chances for holes in those defenses.

At some point, the scope of managing those defenses becomes clouded with bureaucracy. For example, suppose a security vendor discovers a new zero-day exploit. That security vendor alerts the producer of the product about the vulnerability. The producer then works to develop a patch. The producer alerts the public and, by proxy, the DoD. USCYBERCOM takes the lead and pushes an order to JFHQ-DoDIN. JFHQ-DoDIN then produces an order directing service agencies connected to the DoDIN to implement the patch. In the case of the Army, U.S. Army Cyber Command (ARCYBER) receives the order and produces a separate order to U.S. Army Network Enterprise Technology Command (NETCOM). NETCOM digests the ARCYBER order, issues any Requests for Information (RFIs) for clarification, then issues a NETCOM order to all six RCCs and Theater Signal Commands. The Theater Signal Commands in turn issue their own orders to subordinate Signal brigades, which manage the Network Enterprise Centers (NECs) at each base, post, camp, and station (collectively called posts). The NECs manage the IT infrastructure contained within each post.

When viewing defensive capabilities, the structure is inefficient and ripe for missing key linkages to ensure appropriately hardened enterprise defenses. Simply consolidating key elements, along with JFHQ-DoDIN, DISA, and the six Army RCCs into a single Cyber Military Force while properly aligning the budget to address the lifecycle requirement of equipment across the DoDIN, down to the customer edge equipment, could streamline operations and ensure a stronger defense.

Force Design

Congress compelled the DoD to answer "Cyber Matters" in the FY23 NDAA – specifically in section 1533.[42] This is probably one of the most challenging tasks to "compel" based on the complexity, dispersion, authorities, service requirements vs. domain requirements, and lexicon used across the services within the DoD. Yet this task is critical, as the previously discussed GAO report stated, "It's [the DoD's] ability to conduct operations and activities in any of the physical domains (land, maritime, air, and space) that is reliant on protecting the information environment."[43] This study will use the DOTMLPF-P framework to address the scope of this problem. Organizational change is hard. It is apparent from the above that the Air Force and Space Force broke away from their parent services to prioritize niche warfare capabilities. Both services have focused on doctrine, equipping, and funding, enabling them to fully explore and implement domain-specific capabilities.

Cyber Doctrine: The Challenge of Parent-service Bias

The U.S. Army writes doctrine specific to supporting operations in the land warfighting domain. With this focus, the U.S. Army should not be the primary entity responsible for developing cyber doctrine for the cyber warfighting domain. Similar to a statement offered in Dr. Tate's thesis, "The best way to take advantage of the new technology in aviation was to create a new military organization."[44] Cyber needs its own service to develop doctrine specific to warfighting in the cyber domain.

The U.S. Army has been developing doctrine for nearly 250 years, incorporating lessons learned from previous military engagements, as well as the theory and philosophy of warfare. The U.S. Army's capabilities and doctrine are forged to support its mission "To deploy, fight and win our nation's wars by providing ready, prompt and sustained land dominance by Army forces across the full spectrum of conflict as part of the joint force."[45] The Army also says its "mission is vital to the nation because we are the service capable of defeating enemy ground forces and indefinitely seizing and controlling those things an adversary prized most – its land, its resources and its population."[46] The emphasis on land warfare was another key factor in the Army Air Corps' need to separate from the Army, highlighting the specialized nature of each domain.

Currently, there is only one joint cyber doctrine manual for the cyber warfighting domain. This manual, influenced by the Army's focus on land warfare, provides only a basic understanding of cyber operations. A highly skilled team must actively analyze and integrate offensive and defensive capabilities specific to the cyber domain to support other warfighting domains and geographic combatant commanders while considering the actions of allies and adversaries. This approach mirrors the success achieved by the U.S. Air Force in developing air domain doctrine and provides a road map for cyber to do the same.

Organization

Establishing a cyber military service can be achieved with minimal personnel increases by consolidating existing organizations such as DISA, JFHQ-DoDIN, ARCYBER, parts of NETCOM, the six Army RCCs, and cyber staff from the Air Force, Navy, and Marines. However, current military services will still require organic cyber staff to meet their IT and cyber requirements and support for cyber activities. Additionally, non-cyber specialties like the Judge Advocate General (JAG), Intelligence, and Public Affairs, which focus on cyber aspects, must be integrated. These specialties, especially JAG, need a thorough understanding of their field's application in cyberspace, including national and international law relevant to U.S. defensive and offensive cyber operations.

The Department of the Army would be the most appropriate department to constitute this new cyber force. According to the U.S. Army Cyber Command website, "The Army was the first service to create cyber career fields for both Soldiers and Civilians."[47] Comparatively speaking, the Army has spent more time developing a greater cyber capability than other services. Additionally, the Department of the Air Force includes the the U.S. Space Force, and the Department of the Navy includes the U.S. Marine Corps. The Department of the Army does not currently have a similar military service component. However, like the U.S. Space Force, the new U.S. Cyber Force must have autonomy to allow for growth within the cyber domain.

The need for a separate cyber military force is not a new idea. James Stavridis, a U.S. Navy retired four-star Admiral, co-wrote an article with David Weinstein in 2014 on the need to establish a separate U.S. Cyber Force.[48] Stavridis makes several excellent points about the

reasons why there is a need for a separate cyber force, many included in this paper from other sources. However, Stavridis asserts that this separate force should remain constrained by the Posse Comitatus Act, like the U.S. Army. According to an article on the Brennan Center for Justice website, "The Posse Comitatus Act bars federal troops from participating in civilian law enforcement except when expressly authorized by law."[49] Domestic police activities are a key difference between U.S. Code Title 10 and Title 32 missions, where Title 10 is Federal and subject to Posse Comitatus, and Title 32 is a state National Guard mission.

A new U.S. Cyber Force, addressing national cyber threats across all sectors, must incorporate a National Guard component. In a cyber emergency, whether state or local government or private sectors, state or territory Governors could mobilize their National Guard Cyber forces upon request. These Guard units, equipped with the same training and tools as the full-time cyber force, offer the added benefit of being locally based in the states they serve.

The Guard Cyber force could offer immediate emergency response and support to local law enforcement. It could provide state-specific vulnerability assessments, reporting findings to the Governor. Additionally, these forces would aid their parent service's Title 10 missions, having the same training and equipment as the active-duty force, similar to the current Army and Air Guard. The Cyber National Guard could recruit volunteers from their local commercial industries. Some of these professionals are already part of state and territory-aligned CPTs. Integrating these CPTs into a separate cyber military force as the Cyber National Guard component would standardize training, equipment, and doctrine for both Title 32 and Title 10 missions.

Cyber Training: Lifelong Learning Culture

Training in today's military is generally based on the crawl-walk-run method to develop task-specific skills. For example, basic rifleman's marksmanship follows this construct. The crawl phase begins with fundamentals: body position and grip, sight picture, trigger squeeze, and breath control.[50] The walk phase covers disassembly, reassembly, a functions check, and dry-fire exercises. The run phase culminates with weapons qualification at a firing range.

Most skills-based training activities have applied the above training method. While designed for basic skills, this method fails to develop skills necessary for success in a dynamically evolving technical environment, like offensive and defensive cyber operations. In this case, the DoD should incorporate the concept of perishable skills. Reporter, Mark Gibson, references a book titled *A New Culture of Learning*, in which the authors Douglas Thomas and John Seely Brown suggest that "The half-life of a learned skill is 5-years."[51] With the continuous evolution of technology, half of what you learned 5 years ago is now obsolete.[52] However, in the basic rifleman's marksmanship example, firing a weapon system does not fundamentally change unless the basic weapon system changes. In the case of more technical

or professional-level skills, there must be a better way to address skill atrophy paired with the rapid evolution of technology and exploits in cyber.

Matthew J. Daniel, a principal consultant with Guild Education, described three distinct categories of skills, including: perishable skills (half-life of less than two and a half years), semi-durable skills (half-life of two and a half to seven and a half years), and durable skills (half-life of more than seven and a half years)."[53] This illustration provides a framework for building an adaptive training model.

This framework can be used to codify cyber training into durable, semi-durable, and perishable skills. Military history and traditions can be foundational and established as durable skills, giving new members the structure to identify with a specific military culture. The semi-perishable is equivalent to the basic rifleman's marksmanship skills – to maintain the "run" phase, you must continue to practice, but the skills will not become obsolete in short order. For perishable skills, there must be a revolution in training.

The DoD can revolutionize cyber training in two steps: First, teach cyber warriors essential skills for their specific roles. Second, provide biennial training to enhance and learn new skills. Initially, recruits attend a modified basic training on military conduct, history, performance, and expectations, coupled with six months of foundational cyber training. After their first 18-month assignment, they would attend a six-month study program, followed by another 18-month assignment. This four-year cycle would greatly enhance their technical skills. The cyber warrior could then progress from defensive to offensive operations, possibly reserving offensive training for those who re-enlist for another four years. Those leaving service after their first term would return home with substantial defensive cyber skills, enabling them to secure a well-paid career, indirectly bolstering the nation's cyber defense.

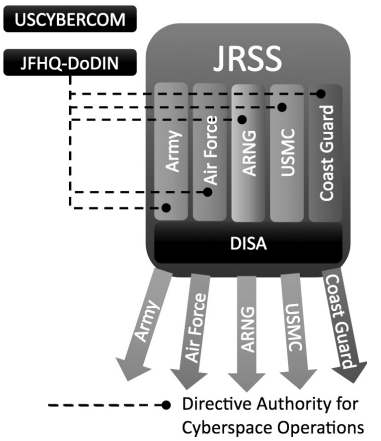


Figure 2: Multi-tenant Model.

Cyber Materiel: The DMARC

The current problems with Materiel include issues with both offensive tools and especially with defensive tools. In this context, “materiel” is the hardware or software solution provided to satisfy unit or mission requirements. For example, if the requirement is to view data crossing a network, the materiel solution might be packet capture software installed on a government-provided computer. In the FY22 NDAA, USCYBERCOM received enhanced budget authority.[54] This is a good start, but the U.S. military needs much more. Each of the services has procurement authority for both offensive and defensive cyber tools, leading to each service doing its own thing. For defensive tools, the cyber terrain is even more

complicated with the DISA providing Information Systems and Services to the various military branches.

A case in point is JRSS. DISA is currently working to replace JRSS with a project named Thunderdome.[55] The benefit of JRSS was the eventual capability of a rich suite of equipment and systems built specifically to secure the Non-Secure Internet Protocol Router (NIPR) portion of the DoDIN. The problem is the multi-tenant model (Figure 2)[56] DISA employes for its customers.

DISA retains advanced access to the systems within JRSS but does not manage them. DISA provisions virtual space for each customer within JRSS providing customers with a graphical user interface (GUI) to manage their virtual space across JRSS. This includes access to advanced tools for monitoring alerts, traffic volume, and troubleshooting traffic flow, immediately requiring each customer to have staff capable of using the DISA tools within JRSS. Those tools may be significantly different than what the military services had been using within their own environments. Additionally, DISA did not originally provide any formal training for the tools in JRSS. Further complicating JRSS was the cumbersome process used to gain access to manage JRSS.

Using JRSS as a model, a single cyber-service would excel by providing a single point of contact and standardized management across JRSS. Combining key defensive cyber elements from each of the military services, along with JFHQ-DoDIN and DISA, would allow for a single service to manage the DoDIN (using NIPR as the example) down to and including the customer edge router. Doing so would allow for a single service provider to have end-to-end visibility across the DoDIN with a team fully trained to use the defensive tools provided (Figure 3),[57] while dramatically reducing redundant support forces across the services.

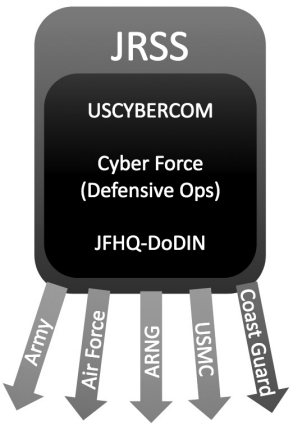


Figure 3: JRSS Model.

Additionally, this would allow for the rapid migration to future technology to enable greater capacity and throughput across the DoDIN. If a single service owned the security stacks across DoDIN, the circuits connecting each base, post, camp, station, state, ship, airbase, and customer edge router, that service could gain economies of scale when upgrading or migrating systems. This would enable the other military services to focus on their post, camps, stations, and domain-specific capabilities instead of each managing transport into and across the DoDIN.

Leadership & Education

The current single publication of cyber doctrine, produced by the Joint Staff,[58] generically addresses offensive and defensive operations and includes the structure of the U.S. Cyber

Command, a functional Combatant Command, and its subordinate and assigned organizations. When considering the land warfighting domain, the U.S. Army has sixteen different doctrinal references.[59] Additionally, the U.S. Army does not focus just on offensive and defensive operations; its doctrine describes a variety of capabilities to use in concert. This concept must extend to cyber to inform training and tactics required to achieve cyber dominance, both offensively and defensively.

The Cybersecurity & Infrastructure Security Agency (CISA) recently published the Workforce Framework for Cybersecurity,[60] based on the National Initiative for Cybersecurity Education (NICE) Framework. CISA outlined seven categories with thirty-three specialty areas and fifty-two work roles, all specific to cyber defensive roles.[61] The CISA categories do not apply to the DoD, but they highlight the complexity and broad skills required just for defense. Recently, the DoD published its Cyber Workforce Framework tool. This tool lists all the DoD cyber workforce roles, both offensive and defensive.[62] Each of these roles includes an exhaustive list of required skills, but no detail of that list is the minimum required for the achievement of expert status, signaling and guiding staff progression.

Personnel

Alternative manning options are currently not possible (or frowned upon) within the existing military services. Alternative generally refers to a person who would normally be physically or medically disqualified for service. A cyber-service would not be constrained by as those disqualifying factors. If the bulk of a cyber warrior's career will be sitting at a computer terminal doing some level of cyber activity, then many of the reasons other services use to exclude potential candidates become irrelevant, such as increasing the mandatory retirement age to bring in experienced talent, reducing physical fitness standards, changing medical requirements to allow for a greater number of approved disabilities, or following the U.S. Space Force's lead by using health monitoring instead of physical training tests.

Additionally, recruiting specifically for cyber will have a generative follow-on effect of increasing the cyber-skilled talent across the U.S. as trained cyber warriors transition back to the civilian workforce. History has proven this, as U.S. Air Force pilots transitioned from active service back to the commercial air industry.[63]

Facilities

Possible locations for the new Cyber Force could include the following. However, this list is not exclusive, and further research should be conducted to adequately capture the full requirement.

- Ft Meade, MD (USCYBERCOM / DISA / JFHQ-DoDIN)
- Scott Air Force Base, IL (DISA)

- Ft Eisenhower, GA (Army Cyber Command)
- Joint Base Lewis-McChord, WA (West coast point of presence)
- Guam – To establish a solid point of presence in the Pacific region

Policy

Very similar to doctrine, policy can help to drive the total force to gain dominance within the associated warfighting domain. Leaving cyber policy to a force built specifically to operate in cyber would allow for innovative changes to positively impact all warfighting domains and improve support to combat commanders. USCYBERCOM currently deals with at least four different sets of service policies specific to its assigned service members. Each service establishes policy specific to supporting its service members. This causes an unnecessary burden to offensive and defensive cyber operators working across mission sets.

For example, enlisted soldiers in the Army are required to complete certain activities to be eligible for promotion. Through these activities, they compete directly with their peer group across the Army, in rank and in their job category. These activities include the Army Combat Fitness Test, weapons qualification, professional military education (PME), civilian education, and annual evaluations.The results of these activities produce a rank-ordered list, by points, of those eligible for promotion. Each military service has a different process and requirements for enlisted promotions. To support the Army requirements, USCYBERCOM must allow Army enlisted soldiers the opportunity to complete these required activities, which may conflict with timing established by other services for their enlisted promotions, or ongoing operations. Establishing a single cyber military service would resolve this issue.

CONCLUSION

Considering the compelling arguments presented throughout this article, it is apparent that now is the time to establish a separate cyber military force under the Department of the Army. The current cyber threats facing the United States, the historical precedent set by the establishment of other military branches, and the existing gaps from of an overly complex and disjointed offensive and defensive cyber organization all point to the necessity of a dedicated cyber military force.

The evolving cyber threat landscape requires a robust response that can only be achieved through a dedicated cyber military force. The increasing frequency and sophistication of cyberattacks on U.S. infrastructure and systems echo similar risks to the DoDIN, demonstrating the need for a consolidated service to defend the nation's cyber domain. By centralizing resources, expertise, and command structure, a separate cyber military force will be better positioned to defend the United States from adversaries.

Moreover, the historical precedent of establishing separate military branches, such as the Department of the Air Force in 1947 and the U.S. Space Force in 2019, underscores the importance of a dedicated cyber military force. Furthermore, countries like Germany, Singapore, and China have also recognized the necessity of a separate cyber military force, leading them to establish dedicated branches. This global trend highlights the importance of the United States maintaining its competitive edge in the cyber domain. A dedicated cyber military force will enable the United States to develop the advanced cyber capabilities required to achieve dominance within the cyber domain, counter adversaries and maintain a technological edge in this ever-evolving domain.

Current gaps in both offensive and defensive cyber strategies further demonstrate the need for a separate cyber military force. As the thesis has shown, the disjointed multi-service model that exists today hinders the effectiveness and efficiency of our cyber operations, especially defensive cyber operations. A unified cyber military force could streamline the decision-making process, optimize resource allocation, and promote the development of advanced cyber capabilities that are essential to maintaining a competitive advantage in the cyber domain. Additionally, by reducing unnecessary redundancy, a separate cyber military force could have the added benefit of dramatically reducing costs currently expended by four different military branches all defending the same terrain.

Utilizing the DOTMLPF-P framework, the DoD can develop a comprehensive cyber military force structure that addresses the unique challenges and requirements of the cyber domain. This framework will also enable the DoD to avoid potential pitfalls and ensure the success of this new branch.

In conclusion, establishing a separate cyber military force under the Department of the Army is a critical and necessary step in addressing the evolving cyber threats facing the United States. By creating a dedicated force, the U.S. will be better positioned to defend its national interests in the cyber domain, develop advanced capabilities, and maintain a competitive advantage over potential adversaries. By using the DOTMLPF-P framework as a starting point, the DoD can ensure the successful development and implementation of this new branch, ultimately strengthening the nation's overall security posture.

NOTES

1. "Uslaw.Link," accessed February 3, 2023, https://uslaw.link/citation/us-law/public/80/253.
2. "Trump Signs Law Establishing U.S. Space Force," U.S. Department of Defense, December 20, 2019, https://www.defense.gov/News/News-Stories/Article/Article/2046035/trump-signs-law-establishing-us-space-force/https%3A%2F%2Fwww.defense.gov%2FNews%2FNews-Stories%2FArticle%2FArticle%2F2046035%2F-trump-signs-law-establishing-us-space-force%2F.
3. Donald H. Rumsfeld, "Report to the Commission to Assess United States National Security Space Management and Organization," January 11, 2001, https://aerospace.csis.org/wp-content/uploads/2018/09/RumsfeldCommission.pdf.
4. Peter A. DeFazio, "H.R. 7776, the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023," December 23, 2022, https://rules.house.gov/sites/democrats.rules.house.gov/files/BILLS-117HR7776EAS-RCP117-70.pdf.
5. Rumsfeld, "Report to the Commission to Assess United States National Security Space Management and Organization."
6. DeFazio, "FY23 NDAA," 509.
7. Winn, Jacob. "U.S. Can't Wait Any Longer for a Cyber Force." Nationaldefensemagazine.org. Accessed September 22, 2022. https://www.nationaldefensemagazine.org/articles/2022/4/22/us-cant-wait-any-longer-for-a-cyber-force.; Senate.gov, 2021. https://www.warner.senate.gov/public/_cache/files/f/2/f26e92ba-2b05-4e65-bbda-10d3a8dc-1c81/0CE82FCBF5172B642C7B6F9C2440B778.hainesnakasonewraywales-ssci-09feb21.pdf.; Aylward, Mary Kate. "The Air Force Isn't Doing Information Technology Right." *War on the Rocks,* December 20, 2021. https://warontherocks.com/2021/12/the-air-force-isnt-doing-it-right/.; Curley, Michael. "The US Military Needs a Seventh Branch: The Cyber Force." *The Hill.* September 2, 2021. https://thehill.com/opinion/cybersecurity/570634-the-us-military-needs-a-seventh-branch-the-cyber-force/.
8. "U.S. Cyber Command Leadership," U.S. Cyber Command, accessed April 26, 2023, https://www.cybercom.mil/Leadership/.
9. *Pat Fallon Supports a Cyber Service | C-SPAN.Org,* mp4, Senior Military Officials Testify on Cyber Operations (Washington, D.C., 2023), https://www.c-span.org/video/?c5064510/user-clip-pat-fallon-supports-cyber-service.
10. *Pat Fallon Supports a Cyber Service | C-SPAN.Org.*
11. Eric Pederson et al., "DoD Cyberspace: Establishing a Shared Understanding and How to Protect It," Air Land Sea Space Application (ALSSA) Center, January 1, 2022, https://www.alsa.mil/News/Article/2891794/DoD-cyberspace-establishing-a-shared-understanding-and-how-to-protect-it/.
12. "Federal Bureau of Investigation Internet Crime Report 2021," March 22, 2022, https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.
13. "Federal Bureau of Investigation Internet Crime Report 2021."
14. Eleanor Watson, "Pentagon Reviews: China Is 'Pacing Challenge' and Russia Poses 'Acute Threat' - CBS News," CBS News, October 27, 2022, https://www.cbsnews.com/news/pentagon-reviews-say-china-poses-greatest-security-challenge-to-u-s-while-russia-is-acute-threat/.
15. "Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure | CISA," April 20, 2022, https://www.cisa.gov/uscert/ncas/alerts/aa22-110a.
16. "Top CVEs Actively Exploited By People's Republic of China State-Sponsored Cyber Actors | CISA," October 6, 2022, https://www.cisa.gov/uscert/ncas/alerts/aa22-279a.
17. "North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector | CISA," July 6, 2022, https://www.cisa.gov/uscert/ncas/alerts/aa22-187a.
18. "Iranian Government-Sponsored APT Actors Compromise Federal Network, Deploy Crypto Miner, Credential Harvester | CISA," November 16, 2022, https://www.cisa.gov/uscert/ncas/alerts/aa22-320a.
19. C. Todd Lopez, "DoD: It's Not Just State Actors Who Pose Cyber Threat to U.S.," U.S. Department of Defense, May 20, 2022, https://www.defense.gov/News/News-Stories/Article/Article/3039462/DoD-its-not-just-state-actors-who-pose-cyber-threat-to-us/.
20. Lopez, "DoD: It's Not Just State Actors Who Pose Cyber Threat to U.S.,".
21. Joseph W. Kirschbaum, "Information Environment: Opportunities and Threats to DoD's National Security Mission," U.S. Government Accountability Office, September 2022, https://www.gao.gov/assets/gao-22-104714.pdf, 2.

NOTES

22. Kirschbaum, 3.
23. Kirschbaum, 3.
24. Dr James P Tate, "The Army and Its Air Corps: Army Policy toward Aviation 1919-1941" (Maxwell Air Force Base, Alabama, Air University Press, 1998), https://www.airuniversity.af.edu/Portals/10/AUPress/Books/B_0062_TATE_ARMY_AIR_CORPS.pdf, 187.
25. Tate, 12.
26. Tate, 20.
27. Tate, 20.
28. Mark Pomerleau, "US Cyber Command Releases First Full Budget," *DefenseScoop* (blog), March 13, 2023, https://defensescoop.com/2023/03/13/us-cyber-command-releases-first-full-budget/.
29. Rumsfeld, "Report to the Commission to Assess United States National Security Space Management and Organization."
30. Bundeswehr, The Cyber and Information Domain Service, accessed March 3, 2024 at https://www.bundeswehr.de/en/organization/the-cyber-and-information-domain-service, translated by google.
31. Mike Yeo, "Singapore Unveils New Cyber-Focused Military Service," *Defense News*, November 2, 2022, https://www.defensenews.com/global/asia-pacific/2022/11/02/singapore-unveils-new-cyber-focused-military-service/.
32. Elsa B. Kania and John K. Costello, "The Strategic Support Force and the Future of Chinese Information Operations," *The Cyber Defense Review* 3, no. 1 (Spring 2018), 105.
33. Kevin L. Pollpeter, Michael S. Chase, and Eric Heginbotham, "The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations | RAND," 2017, https://www.rand.org/pubs/research_reports/RR2058.html.
34. Pollpeter, Chase, and Heginbotham, iii.
35. Pollpeter, Chase, and Heginbotham, 16.
36. "Command History," accessed April 7, 2023, https://www.cybercom.mil/About/History/.
37. "Command History."
38. Pederson et al., "DoD Cyberspace."
39. Pederson et al.
40. Pederson et al.
41. Colin Demarest, "US Indo-Pacific Command Seeks Extra $274 Million for Cyber," C4ISRNet, March 27, 2023, https://www.c4isrnet.com/cyber/2023/03/27/us-indo-pacific-command-seeks-extra-274-million-for-cyber/.
42. DeFazio, "FY23 NDAA."
43. Kirschbaum, "Information Environment: Opportunities and Threats to DoD's National Security Mission.", 2.
44. Tate, "The Army and Its Air Corps: Army Policy toward Aviation 1919-1941."
45. "U.S. Army Mission - The Army's Vision and Strategy | The United States Army," accessed October 19, 2022, https://www.army.mil/about/.
46. "U.S. Army Mission - The Army's Vision and Strategy | The United States Army."
47. "About Army Cyber," U.S. Army Cyber Command, accessed April 23, 2023, https://www.arcyber.army.mil/About/About-Army-Cyber/#:~:text=The%20Army%20was%20the%20first,into%20Cyberspace%20Operations%20Officer%20underway.
48. James Stavridis and David Weinstein, "Time for a U.S. Cyber Force," *U.S. Naval Institute* 140, no. 1 (January 1, 2014), https://www.usni.org/magazines/proceedings/2014/january/time-us-cyber-force.
49. Joseph Nunn, "The Posse Comitatus Act Explained | Brennan Center for Justice," October 14, 2021, https://www.brennancenter.org/our-work/research-reports/posse-comitatus-act-explained.
50. David R. James and Jean L. Dyer, "Rifle Marksmanship Diagnostic and Training Guide:" (Fort Belvoir, VA: Defense Technical Information Center, May 1, 2011), https://doi.org/10.21236/ADA544533.
51. Mark Gibson, "The Half Life of a Learned Skill Is 5 Years - Toward a New Culture of Learning," Why Change Selling, April 11, 2015, https://www.whychangeselling.com/inbound-marketing-messaging-sales-performance-blog/bid/113040/the-half-life-of-a-learned-skill-is-5-years-toward-a-new-culture-of-learning.

NOTES

52. Gibson, "The Half Life of a Learned Skill Is 5 Years - Toward a New Culture of Learning,".
53. Matthew J. Daniel, "Skills Aren't Soft or Hard — They're Durable or Perishable," October 29, 2020, https://www.chieflearningofficer.com/2020/10/29/skills-arent-soft-or-hard-theyre-durable-or-perishable/.
54. Rick Scott, "Text - S.1605 - 117th Congress (2021-2022): National Defense Authorization Act for Fiscal Year 2022 | Congress.Gov | Library of Congress," Congress.gov, December 27, 2021, https://www.congress.gov/bill/117th-congress/senate-bill/1605/text.
55. Alexandra Lohr, "Thunderdome Hits Its Targets, DISA Moves to next Phase of Zero Trust," Federal News Network, February 20, 2023, https://federalnewsnetwork.com/defense-news/2023/02/thunderdome-hits-its-targets-disa-moves-to-next-phase-of-zero-trust/.
56. Jeffrey A Couillard, Image produced by the paper's author from several years of experience managing the Army National Guard's portion of the DoDIN, including the Joint Regional Security Stacks (JRSS), to provide a high-level conceptual image of the complexity and redundancy in managing JRSS, January 22, 2023.
57. Couillard, Image produced by the paper's author to conceptualize the efficiency and economies of scale gained by establishing a separate Cyber Military Force, January 22, 2023.
58. "Joint Publication 3-12 Cyberspace Operations," Joint Chiefs of Staff, June 8, 2018, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.
59. "Army Doctrine Publications," Army Publishing Directorate, access April 26, 2023, https://armypubs.army.mil/ProductMaps/PubForm/ADP.aspx.
60. "Workforce Framework for Cybersecurity (NICE Framework) | NICCS," accessed December 1, 2022, https://niccs.cisa.gov/workforce-development/nice-framework.
61. "Workforce Framework for Cybersecurity (NICE Framework) | NICCS."
62. "DoD Cyber Workforce Framework – DoD Cyber Exchange," accessed April 3, 2023, https://public.cyber.mil/wid/dcwf/.
63. Meredith Metsker, "Three Reasons Why the U.S. Is Running Out of Pilots," June 26, 2019, https://stradaeducation.org/adult-learners/three-reasons-why-the-u-s-is-running-out-of-pilots-2/.

Violent Limitation: Cyber Effects Reveal Gaps in Clausewitzian Theory

Major David Greggs

ABSTRACT

The theoretical foundation remains fundamental to U.S. military policy and doctrine. Carl von Clausewitz provides the core understanding of war and warfare in U.S. military doctrine. As a result, the U.S. military describes and understands war within the Clausewitzian frame of physical violence to accomplish a political goal by enforcing will on the military of an opposing state through physical actions. However, the cyber domain and the effect of cyber actions reveal that our understanding of war can no longer be restricted to the Clausewitz paradigm.

Cyber effects can cause destruction without kinetic actions. The cyber domain's emergence has brought the cognitive dimension to the forefront of many military leaders' and planners' thinking. Cyber activities reveal that while new technology may not have changed war, a theoretical foundation built upon Clausewitz restricts the understanding of war too narrowly for the modern era.

The theoretical references within U.S. military policy and doctrine are no longer sufficient to provide an understanding of war. War is more than just physical violence, but military policy restricts war to just that. This research reveals that U.S. military leadership may need to adopt new or additional theoretical references that encompass all domains of modern war.

David Greggs is a Major in the U.S. Army. He is a cyber operations officer with a background in intelligence. He has deployed to Afghanistan and completed a Master's Degree in Information Technology Management. He is also a graduate of the Advanced Military Studies Program and the Command and General Staff College.

INTRODUCTION: AN INSUFFICIENT THEORY

Cyberattacks remain a significant and growing risk, with the potential for increasing cost, scope, scale, and physical consequences. As costs due to cyber incidents increase, and the United States spends billions on cyber security, the question arises, why has the U.S. not committed to fighting cybercrime or cyber terrorism as it did after September 11?[1] Why are cyberattacks not viewed the same as physical attacks, regardless of the damage they cause? The problem lies in the insufficient theoretical foundation on which U.S. military leaders and planners rely.

These theoretical considerations serve a critical and implicit role in shaping U.S. military policy and doctrine. They shape how senior leaders think about war and the assumptions regarding how it should be carried out – even what constitutes war. They are largely based on an old collection of theoretical references that provide the foundation for the development of today's policies and doctrine. Our U.S. national security and military policies then draw on these theories to conceptualize what war is and how it should be conducted. These theories in turn provide the basis for the development of military doctrine which dictates how military forces should think about and approach warfare. Thus, this paper examines the theoretical references within U.S. military policy and doctrine and concludes that the theoretical references that shape military leaders' and planners' assumptions, conceptions, and practices are insufficient to provide for a war theory that incorporates the cyber domain.

U.S. doctrine often cites such theorists as Carl Von Clausewitz, Sun Tzu, Thucydides, and Alfred Thayer Mahan. These war theorists, but especially Clausewitz, continue to shape U.S. military policy and doctrine, yet their ideas poorly conceptualize war in the cyber age. Warfare has changed dramatically from the

era of swords, muskets, and battleships to today, and while cyber may not have fundamentally changed the nature of war, it has fundamentally altered the conduct of war. The cyber domain may continue to serve primarily as an enabler for other domains. However, cyber can also deliver effects historically restricted to the physical domains. If there is a particular effect required, cyber can likely accomplish it.

This paper explores U.S. military policy and doctrine to provide a U.S.-centric understanding of war and warfare. It then explores the limits of the U.S. understanding of war and warfare and defines how cyber may or may not fit within those boundaries. Then, through historical examples, the paper explores how the cyber domain can result in effects traditionally associated with kinetic actions in warfare, concluding that the theoretical foundation in U.S. military policy and doctrine is inadequate, insufficient, and remains too restrictive for today's U.S. military leaders and planners.

The Foundation: Theoretical References in U.S. Policy and Doctrine

Theory serves as the critical component to support the thought processes of senior military leaders and planners. Theory undergirds how senior leaders and planners respond as a nation faces war, where chance and chaos persist. Today, U.S. military doctrine and policy draw their theoretical foundation almost exclusively from the Napoleonic period and its most prolific theorist, Carl Von Clausewitz. This exclusivity, drawing on a fixed point in time, has prevented a broader examination of modern warfare. If war never changed, this might not matter. But the technology, equipment, tactics, and essential practice of war do change. War looks different today than it did in the past.

Joint Publication (JP) 1 Volume (Vol) 1, Joint Warfighting provides overarching guidance and delivers fundamental principles for the employment of the Armed Forces of the United States.[2] This capstone publication also bridges other policy documents, such as the National Security Strategy (NSS) and the National Defense Strategy (NDS), and serves as the foundation for other publications.[3] As such, JP 1 Vol 1 is one of the most significant and consequential manuals for the U.S. Armed Forces.

Yet, this capstone doctrine only allots minimal space for discussion on the theory of war and only refers to a single theorist, Carl von Clausewitz, as a reference for understanding and describing war. JP 1 Vol 1 states that "the nature of war is immutable,"[4] describing it as a "violent clash of wills" characterized by the trinity of forces of emotion (passion), chance, and reason.[5] Clausewitz further described war as an act of violence to compel an enemy to do the will of the friendly state, and ultimately a "continuation of politics by other means," an idea that this document affirms.[6] In sum, JP 1 Vol 1—the foundation of U.S. military doctrine—describes war as physical violence toward achieving a political objective to enforce will on an enemy. JP 1 Vol 1 also describes warfare as the "the how," or ways, of waging armed conflict.[7] It may also be called the character of war. New technologies and domains do not

change the nature of war, but they alter how it is conducted.[8] Yet the Clausewitzian conception of warfare focuses on physical violence as the means of war, equating the destruction of the enemy military force or conquering territory with defeating the enemy overall.[9] Despite dramatic changes in technology and the world since Clausewitz's *On War*, these concepts find a home in doctrine. JP 1 Vol 1 describes defeating enemy forces through attrition and annihilation.[10] Considering two types of warfare, conventional and irregular, both remain armed forces-centric and physical violence-centric.[11]

Service-specific doctrine echoes joint doctrine in its foundational references. Air Force Doctrine Publication 1, the Air Force capstone publication, cites Clausewitz to describe war as an "extension of politics by other means."[12] The U.S. Navy follows suit in its capstone publication by citing Clausewitz to describe the art of war and using naval means in combat, asserting the naval domain as primary.[13] Similarly, U.S. Army doctrine also references Clausewitz but maintains the decisive nature of the land domain. Ultimately, joint and service doctrine publications remain restricted to very few theoretical references but overwhelmingly focus on Clausewitz and his description of war to serve as the foundation.

While U.S. policy documents such as the NSS and the NDS do not specifically cite theorists, when addressing modern threats like cyberattacks, these strategic documents muddy the waters, confusing rather than clarifying the issue. The 2017 NSS distinguished between cyber and physical threats, while acknowledging that cyberattacks are a feature of modern conflict, and actions may occur in cyberspace without physical border crossings.[14] The 2022 NSS builds on these concepts and acknowledges that international law applies both online and offline.[15] However, while acknowledging state-sponsored actors may extort citizens or attack critical infrastructure through cyber means, the idea of war remains absent from the conversation. The 2022 NDS recognizes that China may leverage the cyber domain in joint warfare but ignores the possibility that effects may take place in the cyber domain independent of other domains.[16]

U.S. policy treats cyberspace as an enabler or supporter of war, but incapable of war in and of itself. Cyberattacks persist, but U.S. policy does not acknowledge cyberattacks in the same way as physical attacks. The result is that the U.S. strategic documents disconnect physical effects from cyber activities and capabilities.[17] This strategic formulation separates the means of creating the effects from the effects themselves and elevates how an activity takes place to greater importance than the impact of that action. Military policy and doctrine are the documents to which planners, strategists, and decision-makers refer, but the theoretical foundation remains fundamental.

On Violence: Clausewitz and U.S. Policy Agree

Carl von Clausewitz provides the reader an opportunity to think about war at varying and increasing levels of complexity, building on the idea that war is a simple duel to the

understanding of war as part of a more complex political discourse and an extension of politics. He also provides a complex trinity where passion, chance, and reason all work in concert and in opposition with one another as he describes war. While Clausewitz acknowledges the complexity and variety of inputs to war, he ultimately describes war as basic physical violence. It is this framing of war by Clausewitz and now by U.S. military leadership, strategists, and warfighters that ignores other possibilities and the learned experiences of recent conflicts in which cyber has played a pivotal role in shaping the battlefield, supporting the warfighter, and even achieving political objectives. Furthermore, this implies that if the objective can be reached without violent action, perhaps these other means would be preferable and less costly to the attacker. Additionally, if the conception of the nature of war—that is, politically centric and exclusively physically violent—does not change and Clausewitz was correct, then new discussion on the nature of war serves little purpose. However, as we have seen, warfare involving cyberspace with today's modern equipment looks vastly different than the warfare Clausewitz observed in 1800.

As an example, in 2007, Estonia was preparing to move a WWII memorial statue that had been in place for 70 years. In protest of the movement, attackers conducted cyberattacks against Estonian government resources and the banking system for 22 days. This event continues to drive considerations of state sovereignty in cyberspace, a topic exacerbated by the lack of an accepted cyber border.[18] Regardless of whether the attackers were state-sponsored or not, the cyberattacks demonstrated the capabilities to disrupt or destroy government operations to motivate political action without physical violence.[19]

Limiting the concept of war to physical violence narrows the basic understanding of war and warfare while also failing to capture the diverse capabilities and effects that occur in war beyond the physical. Of particular interest are those activities that occur within and against belligerents' minds and the possibility for cognitive influence. War itself has always been about more than the destruction of material things and violence remains just a means to an end.[20] Antulio Echevarria said it simply enough: "The essence of war may be the violent clash of arms, but war itself is much more."[21] While war is usually violent, strategy requires more than just the application of violence and destructive force.[22] Violence is not a principle of war. Yet, unfortunately, that is how Clausewitz is often read and interpreted.

To be clear on this point, the nature of war has not suddenly changed, but rather the Clausewitzian description and understanding of war is not adequate for today. The cyber domain has revealed that it is possible to have corporal effects without physical violence, and cognitive effects by changing minds without employing violent means. The cyber domain and the new character of war reveal just how inadequate Clausewitz's description of the nature of war is today.

Cyber Incidents Revealing New Possibilities in the Character of War

Just as no one goes to war for war's sake; no one hacks something for the sake of hacking.[23] Cyberattacks can cause direct physical destruction in addition to indirect disruption and confusion. However, the primary destructive effect of an attack may matter much less than the second and third-order effects. How that happens might look different than what many people are used to.

By examining several historical events, this paper will demonstrate that cyber effects can cause the same or similar effects as traditional kinetic munitions. These incidents demonstrate that acts of warfare are better recognized by their effects than their causes. In addition, it is possible to influence an adversary's strategies, policies, and decisions without taking physical actions altogether.

Stuxnet – A Precision Time Delayed Bomb

The Stuxnet incident, discovered in 2010, was like a bomb in place at least one year before being found, and only after it had done irreparable damage.[24] Symantec, a global cybersecurity company, described Stuxnet as a complex threat with dramatic real-world implications and a "type of threat we hope to never see again."[25] This virus was even called a "cyber missile" after it caused extensive physical damage by destroying approximately 1,000 centrifuges within Iran's Natanz nuclear facility. [26]

Stuxnet was one of the most complex pieces of malware ever developed when it was deployed, resulting in the infection of 100,000 hosts in 155 countries.[27] Notably, the additional infections were unintentional and more due to the nature of the complexity of the Stuxnet virus and its coding to seek out vulnerable targets.[28] Computer worms can self-propagate and infect many more hosts than originally intended, much like one of the first computer worms did in 1988.[29]

Stuxnet resembled a living biological weapon. The Stuxnet virus self-propagated and exploited four vulnerabilities before infecting thousands of computers.[30] It also demonstrated how a cyberattack could be successful even if the exact physical location of the victim is unknown, something impossible with physical bombs.[31] This fact does not eliminate geography as a significant factor but certainly changes how geography can be understood and what limiting factors may or may not exist. When Clausewitz spoke of geography, he assumed the weeks or months it might take to move an army from one theater to another.[32] With Stuxnet, physical geography ceased to be a limiting factor as it wreaked havoc on Iranian centrifuges irrespective of distance.

The attack caused Iran to halt its nuclear program at Natanz, and it took a year for Iran to recover the losses from the attack.[33] Stuxnet was a precision weapon that caused physical and psychological damage far beyond the initially intended victim in a way that resembles a living and thinking weapon.[34] No state has officially taken responsibility for Stuxnet, but

allegations persist that it was a combination of the United States and/or Israel.[35] The complexity of Stuxnet alone led Symantec to believe that only a few attackers could produce a threat like it.[36] Stuxnet remains critical for examination because of the amount of physical damage done, and the politically connected effect of preventing Iran from becoming a nuclear power.

There are differences in means, but the damage is similar to the effects from physical warfare. The attack took place a year or more before the effect was felt, which has changed the conception of the calculus of time and space resulting from a cyberattack. The quantitative damage was not immediately apparent, while the qualitative damage persists today. This challenges the meaning and understanding of surprise.

NotPetya

In June 2017, Russia conducted a cyberattack against Ukraine that was perhaps the most destructive and costly to date.[37] Known as "NotPetya" because analysts initially thought that the virus was avariation of an older "Petya" ransomware virus from 2016.[38] NotPetya caused more damage than the previous virus because it took advantage of a Windows vulnerability and encrypted the hard drives of the infected computers.[39] With ransomware, the victim can usually pay money to get the password to unlock their computer. But with NotPetya, there was no way to unlock the infected machines.[40]

The White House called NotPetya a Russian, and specifically Kremlin, effort to destabilize Ukraine.[41] The UK Government echoed the U.S. statement and even said that Russia had violated Ukrainian sovereignty.[42] The Russian government disrupted Ukrainian systems, effectively destroying hard drives, and made the computers inoperable and unusable until the victims acquired new hard drives and installed the required software.[43] Cost estimates for NotPetya were over $10 billion.[44]

The international shipping organization Maersk had so many computers affected by the virus that their capability to move cargo—one-fifth of worldwide shipping—was disrupted and nearly stopped due to the virus.[45] Merck Pharmaceuticals lost 15,000 computers to the virus, and the attack cost them $870 million.[46]

In all, the NotPetya attack caused billions of dollars in damage, disrupted global supply, and effectively destroyed up to 10 percent of all computers in Ukraine.[47] This computer-based non-kinetic and non-physical attack further demonstrates the destructive capability of cyberattacks, the extensive costs associated with such attacks, and the ripple effects that a significant cyberattack can have. The United States and its critical infrastructure were not targeted or damaged by NotPetya, but an attack in 2021 would change that.

Cyberattacks: The Shockwave May Reach Unintended Victims

The WannaCry ransomware virus attack in 2017 highlighted new possibilities when the cyberattack infected over 230,000 computers and reached 150 countries in just one day.[48]

Although individuals could recover their computers by paying $300 in Bitcoin to retrieve the password and get their computers back, WannaCry was not a simple ransomware virus.[49] Notably, the WannaCry attack directly affected hospitals. The attack prevented doctors from seeing patient data or recording medication changes. Patients missed surgeries because doctors could not access their systems to approve them.[50] Caregivers could not monitor even the most critical patients due to lost computer access.[51] Medical equipment like X-ray machines may not be running a Windows system, but the computer to read the X-ray was, which limited the doctors' ability to read the image.[52] Doctors in British hospitals even canceled surgeries or turned patients away altogether.[53]

In 2020, another ransomware attack—this one relatively minor—targeted a hospital in Düsseldorf, Germany, which crashed computer systems.[54] As a result, a woman who was sent to another hospital much further away died in transit.[55] The attacked hospital may not even have been the primary target, and the woman who died almost certainly was not the target.[56] If a future attack were crafted to cause death, it requires little imagination to envision that real possibility from happening. This type of attack was impossible only a few years ago, much less in the 1800s when Clausewitz wrote *On War*.

Colonial Pipeline

The Texas-based Colonial Pipeline cyberattack in 2021 was significant because it was an attack against U.S. critical infrastructure.[57] The attack began on May 7, 2021, and the company shut down its operations until May 13, 2021.[58] Some of the digital control systems were infected, and shutting down operations caused gas shortages and a dramatic rise in fuel prices.[59]

Darkside, the group that claimed responsibility for the attack, said that its "goal is to make money and not create problems for society."[60] Darkside accomplished its goal when Colonial Pipeline paid a $5 million ransom the day after the attack.[61] However, the psychological (cognitive) effects were more relevant and long-lasting. Many U.S. citizens panicked. People bought containers and filled fuel tanks as they feared fuel shortages.[62] While the attack and its physical effects did not last long, and the pipeline was only shut down for a matter of days, the amount of fear created in that short period was remarkable. The emotional and mental effects remain the most critical factors.

Cyberattacks Cause Physical and Cognitive Disruption and Destruction

As the Stuxnet attack demonstrated, cyber effects can reach equipment or devices on a network and destroy them, regardless of whether the network connects to the internet.[63] Critical infrastructure can be exploited and destroyed through cyberspace, though physical destruction may not be required. In 2021, an attacker hacked into a water treatment plant in Florida, making the water unsafe to drink.[64] What we see is the potential in warfare for cyberattacks

against critical infrastructure to create destruction and confusion in areas once considered sanctuaries. Such deep attacks into enemy territory could involve power loss across a city, including hospitals, water and sewage treatment, and infrastructure destruction—all without any traditional physical actions. More, not fewer, civilians will be at risk.

Confusion and disruption that spreads beyond the realm of the conventional battlefield are not future threats; they are possible now. This type of warfare would not look like a war Clausewitz wrote about, but it would be war nonetheless. More importantly, these effects could go on for months before a traditional attack happens. As a result, the U.S. could be under attack before any U.S. leader or planner realizes what is happening.

Examining just a few cyberattacks and their effects brings several things to the forefront. First, cyberattacks can cause physical destruction. Second, cyberattacks can cause tactical effects such as disruption and degradation of operations. Third, cyberattacks can cause death. The computer virus itself does not kill anyone, but the connection remains clear. Finally, and perhaps most importantly, cyberattacks can have significant and deep psychological and emotional effects. Cyberattacks can make people afraid and disrupt an individual's rational thinking.

War and Cyber Violence

While war will likely always include physical violence, war does not exclusively involve violence. This is not new, but violence is the primary focus Clausewitz and U.S. military doctrine account for in the nature of war. Nation-states only consider war and the use of violence to get something they want.[65] Political discussion can transition from a friendly negotiation to strongly worded letters and ultimately to the point where one or both sides feel it necessary to negotiate violently, including killing or destroying to bring about a resolution. To the contrary, Thomas Rid argues in his book *Cyber War Will Not Take Place* that violence is a prerequisite for war, so cyberattacks will never be the same as physical attacks.[66]

However, war is not about physical violence but is about the political objective: the original reason for escalating from negotiation to war, the act of forcing an opponent to bend their will. Dr. Aaron Brantly stated in his article, "The Violence of Hacking: State Violence and Cyberspace," that restricting the consideration of violence to the physical world ignores the impact of other manifestations of violence that achieve strategic, operational, and tactical objectives that were once only achievable through physical means.[67] Indirect attacks and cyberattacks can affect an enemy system and support achieving goals across the spectrum of conflict. Dr. Brantly stated that "when a murder occurs, police do not absolve the murderer if he used a gun. Despite the disconnect in both physical and temporal space between the action, pulling the trigger, and the effect, a bullet entering and harming a victim, the two parts of the causal chain are linked inexorably."[68] The impact of something remains more important to consider because it recognizes that not all attacks involve traditional armed violence.[69]

The lack of physical violence in a cyberattack, a consistent inclusion in "traditional" war, could imply that cyberwar is simply not war. However, as this paper has already demonstrated, cyber effects can cause destruction and death without physical means. Even if a war must always involve violence, cyberattacks can also fulfill that requirement. Cyberattacks can be physically, logically, or cognitively destructive.

Since there has not been a global war in recent years, observers have yet to see the full range of what cyberattacks may accomplish when world powers are pressed to leverage those capabilities across the full spectrum of operations. While it may be that a cyberattack will not physically blow up an enemy system, it could disable its firing mechanism or targeting computer.[70] If a tank gets destroyed because of cyber-enabled operations, it does not matter how it happened. Just as muskets increased the range of direct fire and nuclear weapons increased the destructive power of bombs, cyberspace expanded the deadly potential and distance forces may reach.[71] Cyber can affect other domains, but it can also broaden other capabilities.

The nature of war itself remains a competition that involves many disparate factors. In past wars, opposing forces targeted civilian support infrastructure with military forces, such as ball-bearing plants in Germany during WWII. It would be no surprise for home station power, water, and logistic networks to come under a cyberattack in modern war. Rather than consider whether violence occurs in cyberspace or if the information dimension should or could constitute violence, the effects of action must remain of primary consideration.

CONCLUSION

U.S. policy and doctrine rely on a war theory that remains incapable of explaining the modern character of war, in particular cyberwar. Today's doctrine relies heavily on Clausewitz and his relatively narrow description of war and warfare that the modern possibilities of warfare barely make sense when viewed through a Clausewitzian lens. Due to doctrine and policy's overt and overwhelming reliance on Clausewitz, his descriptions remain the ripest for criticism.

Clausewitz within his framing of war does not fully account for cyber operations or their capabilities. Nor does he adequately capture the dramatic change in how forces can traverse physical geography, the criticality of computer network logical geography and how it connects systems, or an appreciation for a systemic effect beyond a singular physical center of gravity. Clausewitz also does not fully capture the importance of information warfare and its application to changing an enemy's will.

War should not be reduced to merely physical violence, which unfortunately remains largely how U.S. policy and doctrine conceptualize war. As has been demonstrated, cyber effects can exert warfare wholly apart from kinetic actions. Clausewitz and military policy do not

account for this fact. The rise of the cyber domain also reveals the importance of the information dimension and the preeminence of influencing the minds of decision-makers.

Furthermore, today's leaders should avoid the temptation to re-interpret Clausewitz to modernize him or his theory. Today's doctrine and policy related to war should be firmly rooted in theory informed by an understanding of war and warfare that accurately captures the effects of all domains. The nature of war is complex. U.S. policy and doctrine provide a simple and woefully inadequate description. The current theoretical references within doctrine and policy need to expand to capture a greater range of ideas about war. Theory should overcome this ambiguity with principles, fill knowledge gaps, and enable action when unknowns persist. With current theory firmly anchored in Clausewitz, removed from the cyber domain, and wholly disconnected from the complexity of modern systems, senior military leaders and planners have little to rely on to provide fundamental knowledge when a crisis occurs.

Anchoring on Clausewitzian theory serves to limit the U.S. military's understanding of war to industrial-age ideas and fails to account for two essential truths. First, war is about more than physical violence. Second, cognitive effects in warfare may be as or more important than physical effects. U.S. policy and doctrine narrowly focus on war as an act of violence, specifically physical violence, against military forces. This idea has been repeated so often that it is ingrained in U.S. policymakers, senior military leaders, and planners.

Leaders must concern themselves with the war that will be fought in the future: The next war. Yet our thinking largely remains rooted in the past. With such a focus, U.S. policy and doctrine lack a theoretical foundation to accurately and holistically describe the nature of war that is relevant and complete enough for the current possibilities in the character of war. As a result, the United States and its allies are not well-positioned to recognize the next war when it comes, or to appreciate the nuances and intricacies of warfare before it is too late.

DISCLAIMER

The views expressed here are those of the author alone and do not necessarily represent the views, policies, or positions of the U.S. Government, Department of Defense or its components, to include the Department of the Army, or the United States Military Academy.

NOTES

1. Steve Morgan, "Cybercrime To Cost The World $10.5 Trillion Annually By 2025," *Cybercrime Magazine*, January 18, 2022, Accessed October 8, 2021, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.; Cybersecurity & Infrastructure Security Agency, "Cost of a Cyber Incident: Systematic Review and Cross-Validation," 1-146, October 26, 2020, Accessed January 18, 2022, https://www.cisa.gov/sites/default/files/publications/CISA-OCE_Cost_of_Cyber_Incidents_Study-FINAL_508.pdf, 12.
2. US Department of Defense, Joint Staff, Joint Publication (JP)1 Volume 1, *Joint Warfighting*, (Washington DC: Government Publishing Office, 2023), xiv.
3. US Joint Staff, JP 1 Volume 1 (2023), vi-vii.
4. US Joint Staff, JP 1 Volume 1 (2023), viii, II-14
5. US Joint Staff, JP 1 Volume 1 (2023), II-10-II-12
6. Carl von Clausewitz, *On War*, (Oxford University Press, 2007), 75, 87; US Joint Staff, JP 1 Vol 1 (2023), viii, II-10.
7. US Joint Staff, JP 1, Volume 1 (2023), II-5.
8. Nicholas Michael Sambaluk, *Myths and Realities of Cyber Warfare: Conflict in the Digital Realm*, (Santa Barbara: Praeger, 2020), 2.
9. Clausewitz, *On War*, 75, 94.
10. US Joint Staff, JP 1, Volume 1 (2023), III-15.
11. US Joint Staff, JP 1, Volume 1 (2023), II-6-II-7.
12. US Department of the Air Force, Air Force Doctrine Publication (AFDP) 1, *The Air Force*, (Washington DC: Government Publishing Office, 2021), 1; Clausewitz, On War, 87.
13. US Department of the Navy, Naval Doctrine Publication (NDP) 1, *Naval Warfare*, (Washington DC: Government Publishing Office, 2020), 33.
14. United States, "National Security Strategy of the United States of America," President of the United States, (Washington DC: Government Publishing Office, 2017), 12, 23, 31.
15. President of the United States, National Security Strategy, 34.
16. President of the United States, National Security Strategy, 4, 6.
17. President of the United States, National Security Strategy, 18.; Department of Defense, "Summary: Department of Defense Cyber Strategy," (Washington DC: Government Publishing Office, 2018), 7; United States, "National Security Strategy of the United States of America," 23.; United States, "National Security Strategy of the United States of America," President of the United States, (Washington DC: Government Publishing Office, 2017), 4.
18. Herzog, Stephen. "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses." Journal of Strategic Security 4, no. 2 (2011): 49–60, Accessed June 28, 2023, http://www.jstor.org/stable/26463926., 50.; David Greggs, "Asserting a Cyber Border," Real Clear Defense, April 8, 2023, Accessed June 28, 2023, https://www.realcleardefense.com/articles/2023/04/08/asserting_a_cyber_border_892656.html.
19. Herzog, "Revisiting the Estonian Cyber Attacks," 60.
20. David Lonsdale, "*Clausewitz in the Twenty-First Century*," ed. by Hew Strachan, & Andreas Herberg-Rothe, (Oxford: Oxford University Press, 2007), 247.
21. Antulio J. Echevarria, "Preparing for One War and Getting Another?," Strategic Studies Institute, US Army War College, September 1, 2010, Accessed February 22, 2023, https://www.jstor.org/stable/resrep11589., 25.
22. Lonsdale, *Clausewitz in the Twenty-First Century*, 247.
23. Clausewitz, *On War*, 80-81, 87.
24. Falliere et al., *W32.Stuxnet Dossier*, Symantec Security Threat Report, (Cupertino, CA: Symantec, 2010), 1-64. Accessed February 22, 2023. https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf., 2.
25. Falliere et al., *W32.Stuxnet Dossier*, 50.
26. Michael Holloway, "Stuxnet Worm Attack on Iranian Nuclear Facilities," July 16, 2015, Accessed February 22, 2023, http://large.stanford.edu/courses/2015/ph241/holloway1/; David E. Sanger, *The Perfect Weapon*, (New York: Crown Publishing, 2018), 41-42.; Mark Clayton, "How Stuxnet cyber weapon targeted Iran nuclear plant," *Christian Science Monitor*, November 16, 2010, Accessed February 22, 2023, https://www.csmonitor.com/USA/2010/1116/How-Stuxnet-cyber-weapon-targeted-Iran-nuclear-plant.
27. Falliere et al., *W32.Stuxnet Dossier* 1, 5-6.

NOTES

28. Falliere et al., *W32.Stuxnet Dossier* 1, 7.
29. "The Morris Worm," Federal Bureau of Investigation, November 2, 2018, Accessed February 22, 2023, https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218.
30. Falliere et al., *W32.Stuxnet Dossier*, 2.
31. "Better than bunker busters: The virtual Chinese water torture," Langner, November 15, 2010, Accessed February 22, 2023, https://www.langner.com/2010/11/better-than-bunker-busters-the-virtual-chinese-water-torture/.; Clayton, "How Stuxnet cyber weapon targeted Iran nuclear plant."
32. Clausewitz, *On War*, 214.
33. Sanger, *The Perfect Weapon*, 41-42.
34. Sanger, *The Perfect Weapon*, 42.
35. Josh Fruhlinger, "What is Stuxnet, who created it and how does it work?," CSO, August 31, 2022, Accessed February 22, 2023, https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html.
36. Falliere et al., *W32.Stuxnet Dossier*, 50.
37. "Statement from the Press Secretary," Press Secretary, White House, February 15, 2018, Accessed Accessed February 22, 2023, https://trumpwhitehouse.archives.gov/briefings-statements/statement-press-secretary-25/.
38. Josh Fruhlinger, "Petya ransomware and NotPetya malware: What you need to know now," CSO, October 17, 2017, Accessed February 22, 2023, https://www.csoonline.com/article/3233210/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html.
39. Ivan Belcic, "What is Petya Ransomware, and Why is it so Dangerous?," Avast, September 21, 2021, Accessed February 22, 2023, https://www.avast.com/c-petya.
40. Belcic, "What is Petya Ransomware, and Why is it so Dangerous?"
41. "Statement from the Press Secretary," Press Secretary.
42. "Russian military 'almost certainly' responsible for destructive 2017 cyber attack," National Cyber Security Centre, February 14, 2018, Accessed February 22, 2023, https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack.; "Foreign Office Minister condemns Russia for NotPetya attacks," Foreign Office Minister Lord Ahmad, February 15, 2018, Accessed February 22, 2023, https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks.
43. Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," Wired, August 22, 2018, Accessed February 22, 2023, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.
44. Carly Burdova, "What Is EternalBlue and Why Is the MS17-010 Exploit Still Relevant?," Avast, October 1, 2021, Accessed February 22, 2023, https://www.avast.com/c-eternalblue#topic-2.
45. Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History."
46. Nica Latto, "What is WannaCry?," Avast, August 25, 2021, Accessed February 22, 2023, https://www.avast.com/c-wannacry.
47. Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History."
48. Carly Burdova, "What Is EternalBlue and Why Is the MS17-010 Exploit Still Relevant?," Avast, October 1, 2021, Accessed February 22, 2023, https://www.avast.com/c-eternalblue#topic-2.
49. Nica Latto, "What is WannaCry?," Avast, August 25, 2021, Accessed February 22, 2023, https://www.avast.com/c-wannacry.
50. Burdova, "What Is EternalBlue and Why Is the MS17-010 Exploit Still Relevant?."
51. Andy Greenberg, "How the Worst Cyberattack in History Hit American Hospitals," Slate, November 5, 2019, Accessed February 22, 2023, https://slate.com/technology/2019/11/sandworm-andy-greenberg-excerpt-notpetya-hospitals.html.
52. Greenberg, "How the Worst Cyberattack in History Hit American Hospitals."
53. Melissa Eddy and Nicole Perlroth, "Cyber Attack Suspected in German Woman's Death," *NY Times*, September 18, 2020, Accessed February 22, 2023, https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html.
54. Eddy and Perlroth, "Cyber Attack Suspected in German Woman's Death."

NOTES

55. Eddy and Perlroth, "Cyber Attack Suspected in German Woman's Death."
56. "First Death from a Cyberattack Reported in Germany," Chivaroli Insurance, October 6, 2020, Accessed February 22, 2023, https://chivaroli.com/first-death-from-a-cyberattack-reported-in-germany/.
57. "Pipeline," Cybersecurity & Infrastructure Security Agency, Accessed November 17, 2021, https://www.cisa.gov/keywords/pipeline; "Critical Infrastructure Sectors," Cybersecurity & Infrastructure Security Agency, Accessed February 22, 2023, https://www.cisa.gov/critical-infrastructure-sectors; "Energy Sector," Cybersecurity & Infrastructure Security Agency, Accessed February 22, 2023, https://www.cisa.gov/energy-sector.
58. "Colonial Pipeline Cyber Incident," Office of Cybersecurity, Energy Security, and Emergency Response, Accessed February 22, 2023, https://www.energy.gov/ceser/colonial-pipeline-cyber-incident.
59. Sean Michael Kerner, "Colonial Pipeline hack explained: Everything you need to know," TechTarget, April 26, 2022, Accessed February 22, 2023, https://whatis.techtarget.com/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know; Brian Fung, "Colonial Pipeline says ransomware attack also led to personal information being stolen," CNN, August 16, 2021, Accessed February 22, 2023, https://www.cnn.com/2021/08/16/tech/colonial-pipeline-ransomware/index.html.
60. Mary-Ann Russon, "US fuel pipeline hackers 'didn't mean to create problems,'" BBC, May 10, 2021, Accessed February 22, 2023, https://www.bbc.com/news/business-57050690.
61. Christina Wilkie, "Colonial Pipeline paid $5 million ransom one day after cyberattack, CEO tells Senate," CNBC, June 8, 2021, Accessed February 22, 2023, https://www.cnbc.com/2021/06/08/colonial-pipeline-ceo-testifies-on-first-hours-of-ransomware-attack.html.
62. Mark Gonloff, "Americans Are Now Hoarding Gas Instead of Toilet Paper," Bloomberg, May 11, 2021, Accessed February 22, 2023, https://www.bloomberg.com/opinion/articles/2021-05-11/gas-shortage-panic-buying-makes-colonial-pipeline-hack-worse.; Christine Fernando, "Gasoline in plastic bags? Panic buying after Colonial Pipeline cyberattack won't solve the problem, experts say," *USA Today*, May 12, 2021, Accessed February 22, 2023, https://www.usatoday.com/story/news/nation/2021/05/12/colonial-pipeline-cyberattack-anxiety-gasoline-panic-buying/5059184001/?gnt-cfr=1.
63. Falliere et al., *W32.Stuxnet Dossier*, 3.
64. Maria Henriquez, "Hacker breaks into Florida water treatment facility, changes chemical levels," Security Magazine, February 9, 2021, Accessed February 22, 2023, https://www.securitymagazine.com/articles/94552-hacker-breaks-into-florida-water-treatment-facility-changes-chemical-levels.
65. Donald Stoker, *Why America Loses Wars, Limited War and US Strategy from the Korean War to the Present*, (Cambridge: Cambridge University Press, 2019), 22.
66. Thomas Rid, *Cyber War Will Not Take Place,* (Oxford: Oxford University Press, 2013), 1.
67. Aaron F. Brantly, "The Violence of Hacking: State Violence and Cyberspace," *Cyber Defense Review*, (Winter 2017): 73-91, Accessed February 22, 2023, https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/The%20Violence%20of%20Hacking_Brantly.pdf?ver=2018-07-31-093713-703, 76.
68. Brantly, "The Violence of Hacking: State Violence and Cyberspace," 77.
69. Singer and Friedman, Cybersecurity and Cyberwar, *What Everyone Needs to Know*, 124.
70. Singer and Friedman, Cybersecurity and Cyberwar, *What Everyone Needs to Know*, 124.
71. Singer and Friedman, Cybersecurity and Cyberwar, *What Everyone Needs to Know*, 88.

Quantum Leap: Improving Cybersecurity for the Next Era of Computing By Focusing on Users

Major W. Stone Holden
Michael Gerardi

ABSTRACT

The need to secure communications is critical for militaries and has offered an advantage in battle across history for those who do it well. The advent of new technologies offers ways of securing information, which appears impenetrable by the standards of their era, and this is true today. Quantum computing seems to provide a variety of benefits in defense applications, including protecting communications and the ability to decrypt information protected by some of today's encryption standards. While it is tempting to focus on investing heavily in quantum communications with the promise that this technology offers in securing communications, it would be foolish to ignore the human elements. This article brings historical parallels that offer insights into the potential weaknesses of heavy investment and application of this technology. Historical examples (specifically the experience of the Germans in World War II with their Enigma encryption machines) show that even the most capable encryption systems can be made ineffective by human error or laziness. Any investment by the defense community into quantum communications must be matched by an equal focus on developing a workforce that is more capable of properly handling and managing those systems, or the investment may be in vain. That investment should include improved cybersecurity training across the workforce and increased focus on Cybersecurity at Professional Military Education waypoints for

Maj W. Stone Holden is a Marine Officer assigned to Marine Aircraft Group 29, supporting the staff and subordinate helicopter squadrons in identifying and responding to emerging threats to operations. Previous assignments include the United States Southern Command, where he held billets in security cooperation and collections management, providing the opportunity to manage various projects implementing cutting-edge technological solutions to a range of threats in the AOR. He also served in the INDOPACOM AOR with 3rd Marine Regiment and Combat Logistics Battalion 3, deploying in support of the PACOM Augmentation Team Philippines (PAT-PHL) and aboard the USNS SACAGAWEA as part of Task Force KOA MOANA 17.

leaders. With these steps, the Department of Defense (DoD) may be able to avoid the mistakes of previous generations who relied too much on the promises of technology without shoring up the fragile humans who were essential to making that technology ultimately successful.

INTRODUCTION

The advantage in warfare often lies with those leaders who can communicate plans and messages to their forces rapidly, consistently, and securely. A further advantage lies with those who can penetrate, disrupt, or manipulate the communications of their adversaries. This is particularly true in the modern era of great power competition, where major international players have the resources and technological savvy to reasonably attempt to do both. Interestingly, emerging technologies hold the potential to secure communications in ways that are impenetrable by today's standards. Conversely, these same technologies can potentially render current encryption used by individuals and organizations around the world completely transparent. The driver behind this potential communications revolution is the promise of quantum computing and communications incorporating the unique properties of quantum physics. This technology has attracted the attention of many governments due to the potential benefits of securing their communications, the dangers of having their data decrypted by adversarial quantum computers, and the potential to do the same to their adversaries.[1] Although several years away from being a feasible technology to impact national security efforts, it is time to begin preparing for its arrival. A close examination of military history shows that relying on technical advances alone to secure communications is foolish. However, tomorrow's U.S. defense sector can avoid past mistakes by accounting for the human element in communications security.

Michael Gerardi is a Team Lead at Control Risks ONE Global Risk and Operations Centre (Americas). Michael manages and supports Senior Risk Consultants to ensure the identification, coordination, and response to real-time and future client risks. Prior to joining Control Risks, Michael served in the U.S. Marine Corps as an intelligence officer. Michael held various roles throughout his tenure, leading teams specializing in tactical aviation intelligence, strategic open source, and crisis intelligence. In 2021, Michael decided to transition from the Marines and further his education by pursuing a master's degree in science and international security from King's College London.

The U.S. Defense Science Board identified three areas of quantum technology that hold particular interest for the Department of Defense (DoD): quantum communications, quantum computing, and quantum sensing.[2] Of particular interest is the arrival of quantum communications and encryption, offering offensive and defensive implications for future communications security. The U.S. is leaping ahead to research and develop quantum technologies, doubling the government investment between 2019 and 2021 and hovering at nearly $1 billion annually since then.[3] As with any new technology, there is a risk of focusing too much on the technology itself and ignoring the users who will ultimately implement or use it. It is critical to pair future communications and cyber systems with improved training and education of personnel. While quantum communications offer a more secure means to pass information, and quantum computing provides the potential for leaps in encryption and decryption capabilities, human factors remain a constant threat to even the most secure technology.

DISCUSSION

The advances offered by quantum technologies have historical analogs that can provide insight into how they may impact national security. Militaries have been trying to intercept and decode the communications of their rivals since antiquity. Encryption is one common way to protect information. It is the process of transforming a form of otherwise readable data (or "plaintext") into a form that obscures the original meaning of the data (or "ciphertext") to prevent it from being known or used without a special piece of information (or "key") which can be applied to turn the data back into a readable form.[4] In antiquity, the Spartans invented a device for message encryption called a scytale, which may have been used to obscure the meaning of communications from adversaries.[5] Efforts to encrypt information more securely contin-

ued in states around the world, with various societies developing manual cryptographic means of securing communications up to the dawn of the industrial age.[6] WWII saw the application of industrial organization and machinery to the task of protecting and acquiring communications. Today's encryption methods vary in technique and strength of protection but generally break into asymmetric and symmetric encryption. Asymmetric encryption (commonly referred to as public key cryptography) is a method that uses two separate keys to exchange data, with one encrypting the data and one decrypting the data.[7] The alternative is symmetric cryptography, which uses the same secret key for encrypting the data being sent and for reversing that encryption by the receiver).[8] The information advantage gained by breaking into the secure communications of an opponent can provide militaries with a defining factor in the success or failure of achieving its objectives.[9] It is critical, therefore, that the U.S. continues the task of breaking encrypted communications while fiercely protecting its own against capable adversaries. This requires the adoption and employment of innovations, including quantum technology, in defense of U.S. information and communications and an offensive means to intercept and understand the communications of adversaries. With the re-emergence of Great Power competition, the need for secure communications is increasingly pressing.[10,11]

Currently, secure military communications employ a series of countermeasures to ensure they are not intercepted or read by others. Frequency hopping is one method, referring to wireless communications that rapidly and randomly change the frequency they are transmitting and receiving to avoid interception.[12] A portion of a message may be intercepted, but not enough to be useful. Encryption, another method for securing communications, scrambles a message in a way that makes it mathematically improbable that an adversary could unscramble the message in a reasonable or helpful amount of time without the "key" for decrypting it.[13] Both of these methodologies are commercially available and employed by U.S. forces but remain challenging for most militaries to implement.

Russian forces have been notorious for communicating "in the clear" during their invasion of Ukraine in 2022. Their failure to use encryption or frequency hopping for their military communications has left the world with access to snippets of some of the most intimate battlefield communications. Failure to use existing communications security measures stems from a lack of capable systems in the Russian military at the operational and tactical levels and a failure of training on how to employ them properly. These security failures allowed Ukrainian forces to intercept and act on Russian radio communications.[14] At the same time, foreign observers gained insights into Russian tactics and operational struggles.[15] Communications security based on state-of-the-art technological methodologies means little when personnel employing them are incapable of doing so or are unwilling to do so correctly.

Quantum technologies have defensive, zero-trust implications for communications security through quantum key distribution (QKD).[16]

> In QKD, an encryption key is transmitted between the two communicating parties in the form of quantum particles called photons. As a result of the quantum nature of these particles, any eavesdropper who intercepts them will, in principle, necessarily leave a signature on the data stream itself; if the protocol is implemented properly, then it is physically impossible to observe the photons without modifying them in a way.[17]

QKD is currently a difficult task, limited by the need for a quantum channel to allow the exchange of photons and restricted by distance for quantum channels built using existing ground-based fiber optic technology,[18] but it provides an interesting alternative that is attractive to many working in industries or agencies requiring secure communications.

Quantum computing also offers a tool with more offensive uses. Standard computers today use "bits" of information composed of a string of binary characters that can either be "1" or "0." Quantum computers harness properties of quantum physics to store and transmit information in "qubits." Instead of reducing information to binary forms, qubits have four different possible positions at any given time. This allows quantum computers to rapidly run special algorithms and perform select functions that take standard computers thousands of years in a matter of days or hours.[19] This could lead to a shift from hackers trying to bypass cryptologic systems to hackers leveraging quantum capabilities to attack the system itself.[20] While current encryption methods employed by the government and military are secure, the potential for hackers to attack the system rather than merely bypass it is still concerning and will need to be addressed. Quantum key distribution and quantum computing represent extraordinary technological advances that have the potential for significant impacts on communications security.

Even amid what may seem like unprecedented times, there are significant echoes of a previous era of Great Power competition and communications security. In WWI, the rise of radio-based wireless communication significantly increased communication speed, but serious security flaws were associated with its use. Skilled radio operators could intercept these communications, using positional data to find transmitters and either read messages in the clear or manually decrypt them. The Germans suffered for their insecure communications in the naval battles of the Pacific, where their losses could at least be partially placed at the feet of insecure communications.[21] This was an example of poor technical security, with operators transmitting in ways that could be intercepted due to a lack of technological capability to encrypt or protect that information adequately. Furthermore, it also demonstrates the human failures of the operators, who were not taking appropriate steps to obscure communications using simple tools available in that era.

In the years leading up to WWII, technological innovations in electrical communication and mechanical engineering allowed the Axis powers to improve their communications technology, taking advantage of the increased speed and security.[22] At the start of WWII, the Germans made a concerted effort to adopt a range of emerging technologies to improve

their communications. The incorporation of radio, the Enigma machine to secure messages with front-line troops, and the even more secure and faster Lorenz machine for high-level messages all drastically changed the pace and security of their communications.[23,24] German capitalization on the speed offered by electronic communications tools, including Enigma, was pivotal in their early Blitzkrieg campaigns. It allowed them to coordinate the masses of troops enabled by industrialization across a large front while maintaining a blistering pace of warfare.[25] While keen to seize the technological edge, the Germans were also highly security conscious and became early adopters of modern communications security protocols and encryption methods.[26]

As part of their security efforts, the Germans adopted the Enigma code machine for employment in military operations.[27] When used properly, the Enigma offered 150 quintillion distinct ways to set it up to encode a message. In an age before modern computers, this should have rendered it practically unbreakable to anyone trying to snoop.[28,29] The machine was revolutionary and created tremendous difficulty for the Allied war effort since code-breaking consumed enormous amounts of British and American resources. Breaking the code eventually occurred with the help of some of the most brilliant minds of the time from Poland, the United Kingdom, and the U.S[30] Successful harnessing of the intellectual capital of their nations was a pivotal element to Allied success. However, more was needed to beat the Enigma system.

A major contributing factor in breaking the Enigma code was consistent human error by well-trained and highly skilled German Enigma operators.[31] Simple mistakes (like failing to completely switch out the coded wheels that adjusted the encryption, typing repetitive messages, and encoding messages in both old and new settings) proved critical shortcomings that allowed Allied cryptanalysts to ultimately penetrate Enigma. The technological promise of completely secure communications had lured operators into a false sense of security. If no one could break this code, why put so much effort into the surrounding security protocols and practices? The human factor of the operators succumbing to natural tendencies to take shortcuts while underestimating the impact of failure to adhere to established protocols. All these factors are amplified in times of conflict, when extreme fatigue, stress, and grueling mental workloads wear away at the finer elements of human precision.[32] Sometimes, it makes little sense to spend time breaking codes when you can bypass them altogether through the system's weakest link.

Contrasting the painstaking labor by the Allies to break Axis codes, Italian agents relied on the laziness of physical security protocols at Allied embassies to acquire cipher books and decrypted communications.[33] Terrible security protocols in vetting employees allowed Italian agents to penetrate U.S. embassies and gain access to office spaces after hours. Once inside, the embassy security protocols (when followed) were ridiculously simple to overcome. Keys were unsecured, documents were left out in the open, and safes required no more

than a screwdriver to remove a back panel. These relaxed security procedures all went to aid Italian agents. The best encryption methods in the world could be easily bypassed by exploiting human laziness and error. In this instance, those tendencies provided a wealth of information to Axis forces. German leaders like Field Marshall Erwin Rommel were able to conduct their early campaigns with a wealth of information that it was like "... a gambler, but one who could read the other player's cards."[34] These types of errors are not a thing that we can toss into the dustbin of history, as something that was solely a flaw of another generation.

Just as Germany capitalized on emerging advances in information security presented by mechanical encryption, the U.S. is investing in its emerging technologies. The U.S. has completed a significant amount of work to prepare for quantum technologies on the technical side of the issue. Since 2019, the U.S. government has spent over $2.5B on quantum research and development.[35] This investment resulted in notable achievements, including the announcement in July 2022 by the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) that it had selected some of the first tools designed specifically to withstand quantum decryption.[36] This is a major technical step toward communications security in the post-quantum world, but more is needed.

In the decades following the Cold War, the U.S. has primarily fought against non-state adversaries who have not enjoyed the sophisticated communications capabilities states can field. This has led to a sense of invulnerability, which contributed to embarrassing communications security failures- like when Iraqi insurgents hacked military unmanned aerial system data feeds.[37] It is tempting to believe that our military forces and populations, in general, have evolved from the kind of human error that proved fatal to the brilliance of the Enigma in WWII. It would be unwise to do so. The threats posed to secure military communications continue to be substantial and will likely be exacerbated by technological advances. The People's Republic of China (PRC) has listed quantum computing as one of the technologies they are pursuing to seize the "technological high ground." The contemporary battlefield is already seeing the application of advanced technology that will significantly impact communications in modern warfare.[38,39] The advances in quantum communications and quantum key distribution offer the allure of making communications so secure that they are practically unbreakable with the current technology.[40,41] These advances can also work against the U.S.

It is plausible that soon, aggressors will be able to use quantum computing tools to attack U.S. communications in novel ways while also using technology like quantum computing to fortify their communications against U.S. penetration.[42] Technology is not the only solution; its advantage is often fleeting and rarely as dominant as first perceived.[43] Any pursuit of a technological solution to the problem of employing quantum technologies to protect U.S. data or to defeat adversary communications security needs to incorporate the human design element of cybersecurity. The most advanced technologies in the hands of someone who mishandles it can be undermined by their actions.

Human error remains a significant attack surface for communications penetration. Every year, millions of dollars are invested worldwide in sophisticated cyberattacks, painstakingly built off of millions of lines of precise coding. Many of these attacks rely on human error to gain their fatal foothold. Spearfishing, failing to update systems, and weak passwords contribute to a substantial number of successful attacks.[44,45] A 2014 study by IBM found that across 130 countries, over 95 percent of all cybersecurity incidents could be traced back to human error at some point.[46] The report showed that these errors included misconfiguration of systems (like with the Enigma wheels), poor patch management (similar to German operators failing to update their codes), bad passwords, and poor control of devices (reminiscent of the poor embassy security exploited by the Italians). A 2022 white paper by Mandiant discussed human error's impact on a cyberattacks success. It noted that poor training of employees contributed to their seeming inability to stop making security mistakes that left their organizations open to penetration.[47] Any system that emerges based on quantum computing must be designed to guard against human errors that can render it vulnerable on either end of the communications link.

Communications protected by quantum technologies are more resistant to interception attempts and decryption, but must still be transferred onto a computer for the end user to consume. This remains vulnerable to hacking or attacks that could reveal the "secured" information.[48] Securing the technical middle, without securing the human operators on either end, ignores the broadest surface for communications penetration. Human error remains a primary contributing factor to the penetration of communications security protocols in the cyber domain, and there is little evidence to suggest that the trend will change.

Despite large amounts of time and resources applied to cybersecurity, DoD currently struggles to maintain cybersecurity across one of the largest workforces of any organization on the planet.[49,50] The Federal government spends over $100 billion annually on cyber and information technology investments.[51] Even with this level of investment, in 2019, the Government Accountability Office revealed over 28,000 reported cybersecurity incidents.[52] While not every incident will be the critical error that unleashes the adversaries waiting in the shadows, the sheer scale of the problem increases the risk it poses to DoD. The DoD is massive, with millions of personnel needing to access systems at different levels and for other purposes.[53] Furthermore, diverse backgrounds and educational experiences make it difficult to adopt and implement sweeping policies effectively. An officer falls for a spearfishing attack; a soldier or sailor leaves their credentials somewhere by accident; a janitor at a facility finds a thumb drive and pops it into a machine to see who owns it; a tired field operator fails to properly execute all of the security protocols for their communications device. These problems will not abate with the emergence of quantum computing.

Current levels of cybersecurity training for DoD members fall well short of where they should be despite its prominence in strategic guidance documents. The 2018 DoD Cyber Strategy lists four objectives. Two of those, defending U.S. critical infrastructure from cyberattacks and

protecting DoD information and systems from cyber threats, demand a greater level of training and education in the general user population.[54] The strategy also identifies the importance of cultivating a more robust cybersecurity culture within the larger workforce and the value of providing training for personnel on cyber topics.[55] In cultivating this cyber-proficient workforce, more effort should be expended on raising the general level of cyber awareness among non-IT professionals. These personnel play a critical role in maintaining the security of information systems.

The annual DoD-mandated cybersecurity training provides little more than a baseline of "what not to do." Improved training should discuss actual threat actors and real compromises and provide tactics, techniques, and procedures for adversaries. Better training would provide users with case studies highlighting why training is so relevant and how adversaries seek to undermine their security. Building upon the foundation of the annual cyber awareness training allows training to progress to more complicated and nuanced issues. Training must also be supplemented with more general education on cyber topics as DoD members progress in their careers. While some courses on cyber topics are available at the Naval Postgraduate School, Army War College, and Air Force Institute of Technology, there is room for improvement.[56,57] Updated rigorous cyber course requirements at each Professional Military Education checkpoint throughout a career are an easy way to improve the cyber-savvy of leaders across the joint force.[58] A mix of improved training and better education of leaders would go a long way toward addressing the human side of information security risks. Nurturing a cyber security-oriented joint force will pave the way to reduced risks associated with implementing quantum communications systems within DoD.

CONCLUSION

While investing in cutting-edge technology is important, the U.S. must apply historical lessons about human vulnerability to its future communications security efforts. People are capable of amazing things, but innate traits are also often the weak link in the chain of communications security. Though failure and accidents will always be a part of technological systems, they must be designed to minimize the chance of error, dull the allure of laziness, and anticipate the friction of war, which could lead to security-compromising behaviors. By embracing the hard-won lessons of WWII and evolving them to apply to the advances of the modern era, the U.S. national security enterprise and DoD can position itself on the road to success in the communications security battles of the future.

DISCLAIMER

The views and opinions expressed herein are those of the authors, alone, and do not necessarily reflect the official policy or position of the United States Marine Corps, the Department of Defense, the U.S. Intelligence Community, or the U.S. Government.

NOTES

1. Michael J. D. Vermeer and Evan D. Peet, "Securing Communications in the Quantum Computing Age: Managing the Risks to Encryption," Santa Monica, CA: RAND Corporation, 2020, https://www.rand.org/pubs/research_reports/RR3102.html, 1.
2. Congressional Research Service, "Defense Primer: Quantum Technology," *In Focus*, September 2022, https://crsreports.congress.gov/product/pdf/IF/IF11836, 1.
3. Subcommittee on Quantum Information Science Committee on Science, "NATIONAL QUANTUM INITIATIVE SUPPLEMENT TO THE PRESIDENT'S FY 2023 BUDGET," National Science and Technology Council, January 2023, https://www.quantum.gov/wp-content/uploads/2023/01/NQI-Annual-Report-FY2023.pdf.
4. National Institute of Standards and Technology, "Encryption," Computer Security Resource Center, accessed 9 Mar 2024, https://csrc.nist.gov/glossary/term/encryption.
5. Martine Diepenbroek, "The Spartan Scytale," https://www.academia.edu/download/65378844/ Diepenbroek.pdf, 46-47.
6. Gustavus J. Simmons, "Cryptology," *Encyclopedia Britannica,* https://www.britannica.com/topic/ cryptology/History-of-cryptology.
7. National Institute for Standards and Technology, "Asymmetric Cryptography," Computer Security Resource Center, accessed March 9,, 2024, https://csrc.nist.gov/glossary/term/asymmetric_cryptography.
8. National Institute for Standards and Technology, "Symmetric Cryptography," Computer Security Resource Center, accessed March 9, 2024, https://csrc.nist.gov/glossary/term/symmetric_cryptography.
9. Jack Detsch and Amy Mackinnon, "'The Ukrainians Are Listening': Russia's Military Radios Are Getting Owned," *Foreign Policy,* 2022, https://foreignpolicy.com/2022/03/22/ukraine-russia-military-radio/.
10. CSIS, "Reversing the Tide: Toward a new U.S. strategy to support democracy and counter authoritarianism," Task Force on US Strategy to Support Democracy and Counter Authoritarianism, April 2021, 5-7, 25-26.
11. US Office of The Director of National Intelligence, 2021 Annual Threat Assessment of the U.S. Intelligence Community, 2021, 5-11.
12. United States Marine Corps, "Communication Equipment B191716 Student Handout," https://www.trngcmd.marines.mil/Portals/207/Docs/TBS/B191716%20Communication%20Equipment.pdf, 11-12.
13. Vivek Wadhwa and Mauritz Kop, "Why Quantum Computing Is Even More Dangerous Than Artificial Intelligence," *Foreign Policy,* August 2022, https://foreignpolicy.com/2022/08/21/quantum-computing-artificial-intelligence-ai-technology-regulation/.
14. Detsch and Mackinnon, "The Ukrainians."
15. *The Economist*, "Why Russian radios in Ukraine are getting spammed with heavy metal," May 2022, https://www.economist.com/the-economist-explains/2022/03/28/why-russian-radios-ukraine-war-intercepted-heavy-metal.
16. Edward Parker, "Commercial and Military Applications and Timelines for Quantum Technology," Santa Monica, CA: RAND Corporation, 2021, https://www.rand.org/content/dam/rand/pubs/research_reports/ RRA1400/RRA1482-4/RAND_RRA1482-4.pdf, 8-9.
17. Parker, "Commercial and Military Applications and Timelines for Quantum Technology," 18
18. Bruno Huttner, Romain Alleaume, et al., "Long-range QKD without trusted nodes is not possible with current technology," npj *Quantum Information* 8, 108 (2022), https://doi.org/10.1038/s41534-022-00613-4.
19. Michael J. D. Vermeer and Evan D. Peet, "Securing Communications in the Quantum Computing Age: Managing the Risks to Encryption," Santa Monica, CA: RAND Corporation, 2020, https://www.rand.org/pubs/research_reports/RR3102.html, 5.
20. Vermeer and Peet, 5-6.
21. John Keegan, *Intelligence in War: Knowledge of the Enemy From Napoleon to Al-Qaeda*, (New York: Random House, 2003), 105-143.
22. Alex Hern, "How did the Enigma machine work?" The Guardian, November 2014, https://www.theguardian.com/technology/2014/nov/14/how-did-enigma-machine-work-imitation-game.
23. The History Press, "How Lorenz was different from Enigma," accessed May 8, 2023, https://www.thehistorypress.co.uk/articles/how-lorenz-was-different-from-enigma/.

NOTES

24. Stanford University, "The Lorenz Schluesselzusatz SZ40/42," accessed May 9, 2023, https://cs.stanford.edu/people/eroberts/courses/soco/projects/2008-09/colossus/lorenzmachine.html.
25. Max Boot, *War Made New: Weapons, Warriors, and the Making of the Modern World,* (New York: Penguin Group Publishing, 2006), 223-236.
26. Max Hastings, *The Secret War: Spies, Ciphers, and Guerillas 1939-1945,* (New York: HarperCollins Publishers, 2016), 7-8.
27. Gershom Gorenberg, *War of Shadows: Codebreakers, Spies, and the Secret Struggle to Drive the Nazis from the Middle East*," (New York: Public Affairs, 2021), 63-70.
28. Gorenberg, 67.
29. Mark Lowenthal and Robert Clark, *The 5 Disciplines of Intelligence Collection*, (Thousand Oaks, CA: Sage Publishing, 2016), 90-95.
30. Gorenberg, 81-92.
31. Gorenberg, 88-92.
32. CL Paul and J Dykstra, "Understanding Operator Fatigue, Frustration, and Cognitive Workload in Tactical Cybersecurity Operations." *Journal of Information Warfare* 16, no. 2 (2017), https://www.jstor.org/ stable/26502752, 2-4.
33. Gorenberg, 349-361.
34. Gorenberg, 311.
35. Subcommittee on Quantum Information Science, "NATIONAL QUANTUM INITIATIVE SUPPLEMENT TO THE PRESIDENT'S FY 2022 BUDGET," National Science and Technology Council, December 2021, https://www.quantum.gov/wp-content/uploads/2021/12/NQI-Annual-Report-FY2022.pdf, 6-8.
36. NIST.gov, "NIST Announces First Four Quantum-Resistant Cryptographic Algorithms," July 2022, https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms.
37. Mike Mount and Elaine Quijano, "Iraqi insurgents hacked Predator drone feeds, U.S. official indicates," CNN, December 2009, http://www.cnn.com/2009/US/12/17/drone.video.hacked/index.html.
38. US Army Training and Doctrine Command, "The Operational Environment and the Changing Character of Future Warfare," 2018, 14.
39. Rush Doshi, *LONG GAME: China's Grand Strategy and the Displacement of American Power,* (Oxford University Press, 2021), 263-265, 286.
40. US Congressional Research Service, "Defense Primer: Quantum Technology," Report IF11836, version 5, December 2021, 2.
41. Edward Parker, "Commercial and Military Application and Timelines for Quantum Technology, RAND Corporation, 2021, 8-10, 14-16.
42. Center for Strategic and International Studies, "Maintaining The Intelligence Edge: Reimagining and Reinventing Intelligence through Innovation," CSIS Technology and Intelligence Task Force, January 2021, 5.
43. Ian Sullivan "300. "Once More unto The Breach Dear Friends": From English Longbows to Azerbaijani Drones, Army Modernization STILL Means More than Materiel," https://madsciblog.tradoc.army.mil/300-once-more-unto-the-breach-dear-friends-from-english-longbows-to-azerbaijani-drones-army-modernization-still-means-more-than-materiel/.
44. Nicole Perlroth, "This Is How They Tell Me the World Ends: The Cyberweapons Arms Race," (New York: Bloomsbury Publishing, 2021), 337, 341, 397.
45. Kaspersky, "The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within," Kaspersky Daily, Kaspersky.com, 2017.
46. IBM Global Technology Services, "IBM Security Services 2014 Cyber Security Intelligence Index," Managed Security Services, 2014, https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom /IBMSecurityServices2014.PDF, 1-4.
47. Mandiant, "Navigating the Cyber Skills Shortage," June 2022, https://www.mandiant.com/sites/default/files/2022-06/navigating-the-cyber-skills-shortage-wp.pdf.
48. Edward Parker, "Commercial and Military Applications and Timelines for Quantum Technology," RAND, https://www.rand.org/content/dam/rand/pubs/research_reports/RRA1400/RRA1482-4/RAND_RRA1482-4.pdf, 2021, 8-9.

NOTES

49. Henry Taylor, "Who is the world's biggest employer? The answer might not be what you expect," The World Economic Forum, Jun 2015, https://www.weforum.org/agenda/2015/06/worlds-10-biggest-employers/#:~:text=It's%20often%20said%20that%20Indian,million%20employees%20on%20its%20roster.
50. Martin Armstrong, "The World's Biggest Employers," Statista, November 2022, https://www.statista.com/chart/3585/the-worlds-biggest-employers/.
51. Government Accountability Office, "Information Technology and Cybersecurity: Using Scorecards to Monitor Agencies' Implementation of Statutory Requirements," GAO.gov, July 2022, https://www.gao.gov/products/gao-22-106105.
52. Government Accountability Office, Cybersecurity," GAO.gov, accessed October 10, 2022, https://www.gao.gov/ cybersecurity.
53. US Government Accountability Office, "CYBERSECURITY: DoD Needs to Take Decisive Actions to Improve Cyber Hygiene," Report to Congressional Committees, April 2020, https://www.gao.gov/assets/gao-20-241.pdf, 1-4.
54. Department of Defense, "Summary: Department of Defense Cyber Strategy," 2018, 3.
55. Department of Defense, "Summary: Department of Defense Cyber Strategy," 2018, 6.
56. US Army War College, "Curriculum," https://ssl.armywarcollege.edu/dde/curriculum.cfm, accessed 12 October 12, 2022.
57. Naval Postgraduate School, "Cyber Security and Operations Courses," https://nps.edu/web/c3o/course-list, accessed October 12, 2022.
58. Erica Borghard, Mark Montgomery, and Brandon Valeriano, "The Challenge of Educating the Military on Cyber Strategy," *War on the Rocks*, June 2021, https://warontherocks.com/2021/06/the-challenge-of-educating-the-military-on-cyber-strategy/.

How the Collapse of the Soviet Union Made Russia a Great Cyber Power

Alec Jackson

INTRODUCTION

As a result of the unique circumstances created by the collapse of the Soviet Union, Russia has developed disproportionate cyber power relative to its economic stature. The Belfer Center for Science and International Affairs defines cyber power as "the effective deployment of cyber capabilities by a state to achieve its national objectives."[1] In general, the operational capacity of a state's national security infrastructure, and especially its cyber power, scales directly with that of its innovation economy.[2] Russia is only the world's eleventh-largest economy by gross domestic product (GDP),[3] and its information technology (IT) sector constituted just under 6% of the country's GDP before Russia's 2022 invasion of Ukraine.[4] Despite these limitations, Russia is commonly recognized as an elite cyber power.[5] Importantly, Russia relies heavily on cyber professionals from outside its security agencies, including talent from the private sector and associated with organized criminal groups (OCGs), to conduct offensive cyber operations on the state's behalf.[6]

In analyzing the ways that Russia leverages non-state cyber talent, this article details how the Soviet Union's history impacted the development of Russia's internet, and the

Alec Jackson works as an analyst in the Office of the Secretary of Defense. He completed the International Security Master of Arts program at George Mason University's Schar School of Policy and Government earlier this year and authored "Managing Russia in the Middle East: The Case for Selective Engagement" (2022).

competitive advantages enjoyed by the Russian IT industry. This article also examines the legal and economic environment that rewards non-state actors that engage in cybercrime, and how the Russian state employs corruption networks to mobilize cyber talent outside the direct control of its security agencies. Corruption is the glue that binds Russian IT professionals, Russian OCGs, and the Russian security apparatus together, and allows the state to leverage cyber talent outside the state to pursue Russian President Vladimir Putin's strategy of "offensive defense" against the West. This article concludes with an analysis of the impacts of the Ukraine invasion and subsequent Western sanctions on Russian cyber power, and recommendations for containment by Western policymakers on Russian cyber power in the future.

The History of the Russian Internet

The development of the Russian internet was largely shaped by the unique circumstances surrounding the collapse of the Soviet Union. These conditions were made possible by Russian government agencies, Russian state-owned entities, domestic commercial actors, foreign corporations, and international non-governmental organizations. In the early 1990s, Russia lacked developed civilian telecommunication networks.[7] Infrastructure that did exist largely consisted of Soviet-era analog telephone lines almost entirely owned by the state operator, Rostelekom.[8] Early internet networks in Russia were mostly concentrated around Moscow and used this analog infrastructure to provide basic services. Many independent Russian internet service providers (ISPs) were founded during the 1990s, but Rostelekom was key to the growth of the Russian internet. In 1996, Rostelekom created the Moscow–Khabarovsk Radio Relay Communication Channel,[9] a network of radio-relay cables from Vladivostok to Novorossiysk that connected Russia's regional ISPs to their counterparts in Moscow.[10] Between 1995 and 1999, Rostelecom also constructed a nationwide

fiber-optic backbone system, which helped link the Russian internet with international networks.[11] By the end of 2000, 6.6 million Russians had access to the internet.[12]

Western businesses like Sprint and non-profit organizations like George Soros's Open Society Institute leveraged Russia's political and economic opening to build Russia's internet infrastructure. The Open Society Institute established major internet centers at 33 Russian universities between 1996 and 1999.[13] The internet infrastructure created for Russia's universities and research centers helped drive internet adoption in Russia outside of Moscow and Saint Petersburg. In addition to enabling internet connectivity, these networks (which included the Moscow State University-affiliated Radio-MSU and MSUnet, as well as the Russian Research Institute for the Development of Public Networks's RELARN-IP) helped to create a market for internet services in the Russian regions.[14] In fact, the university centers themselves became internet service providers in numerous Russian oblasts.[15]

When the Soviet Union collapsed in 1991, so did the primary source of research funding in the territory it controlled. Between 1991 and 1999, Russia's budget for science dropped 90%.[16] In constant 1995 U.S. dollars, Russian funding for research and development dropped from $28.4 billion in 1990 to $7.2 billion in 1998.[18] Similarly, domestic funding for Russian defense procurement fell by at least 80% during the 1990s. Many Russian scientists emigrated abroad as a result. Those who stayed were forced to seek new sources of income. These included large numbers of programmers[19] who found work in the nascent internet economy.[20] Indeed, some say the Russian internet was "born in the kitchens of the intelligentsia."[21] Minimal state regulation of the internet in the 1990s and 2000s allowed early Russian internet entrepreneurs to flourish.

Unlike many pre-fall-of-the-Soviet-Union manufacturing and energy companies that were then captured by Russian oligarchs, no regional or inter-regional civilian telecommunications infrastructure or even physical assets existed to capture.[22] For example, Russian Prime Minister Viktor Chernomyrdin looted energy company Gazprom's assets and sold them to his relatives and associates[23] before Putin began his drive to suborn Russia's oligarchs in 2000. In contrast, Russian IT companies that made use of the newly built internet infrastructure possessed no Soviet Union "legacy assets."[24] Most Russian ISPs, at least at the regional level, were built "from scratch"[25] by their founders in the mid-to-late 1990s. Even as the Russian internet began to take shape, companies building it were too small to attract oligarch attention.

Competitive Advantages of the Russia Information Technology Sector

While the vast expanse of Russia's landmass has posed logistical challenges to expanding remote internet access, internet connectivity is highly affordable to average Russians in areas where it is available. A 2015 World Bank study reports that more than 80% of Russians are able to afford broadband internet access.[26] This is because minimal government regulation of ISPs, at least from a commercial standpoint, even if not from a content standpoint, has promoted healthy competition among Russian ISPs. Rostelekom, still partially state-owned,

enjoys a dominant market position in backbone connectivity, but it is not a monopoly.[27] Literally thousands of ISPs operate in Russia,[28] although many independent ISPs use Rostelekom's infrastructure.[29] The affordability of internet access in Russia is a key contributor to internet-enabled enterprises, commercial or otherwise. It not only helps connect Russian IT professionals with each other and with international clients, it also facilitates the transfer of technical knowledge, whether academic, commercial, or criminal. Finally, internet access is recognized as an important structural factor that influences career choice.[30] The affordability of household internet access in Russia helps encourage young Russians to pursue IT careers.

The U.S., another geographically large country with a comparatively highly regulated telecommunications sector from a commercial standpoint, enjoys very little competition among ISPs. The U.S. market for home internet is an oligopoly dominated by four large ISPs that often enjoy local monopolies[31] and rarely are forced to compete on price in local markets. This limits consumer choice, stifles competition, and raises internet prices for U.S. households. Because cost is the primary barrier to Internet access in the U.S., the result of limited competition between ISPs is that 14% of Americans with annual incomes under $30,000 do not use the Internet,[32] and 43% of American adults with annual household incomes under $30,000 have no broadband internet subscription.[33] Despite massive federal investment in improving broadband access, especially for rural communities, serious affordability challenges remain.[34]

Legacy of the Soviet Union's Science, Technology, Engineering, and Mathematics (STEM) Education

Russian cyber power has benefited from inheriting the Soviet Union's education system, which strongly emphasized STEM education. To this day, "scientific and technical education is particularly valued within Russia"[35] where 37 percent of Russian undergraduate students major in a STEM field,[36] compared to 21 percent of U.S. undergraduate students.[37] Russia also inherited from the Soviet Union a massive system of national research laboratories and research institutes, though it has struggled to maintain this network.[38] The Russian education system also fosters a creative, problem-solving mindset in the IT workers it trains.[39] Indeed, many multinational corporations believe employing Russian IT workers, instead of Chinese or Indian tech workers, give companies a competitive advantage.[40]

Cultural compatibility between Russian IT professionals and their clients, particularly clients in the native English-speaking world, is another important competitive advantage of Russian IT firms. Russian IT firms, especially software offshoring companies, are characterized by small teams of "creative and strong-willed"[41] experts willing to debate client methodologies and timelines. According to one European client of a Russian IT outsourcing firm, these qualities render Russian IT firms highly compatible with American clients.[42] Historically, most customers of Russian IT companies were from the U.S. and Canada,[43] and many U.S. start-ups founded by Russian-born entrepreneurs rely on Russia-based IT professionals.[44]

Incentives for Cybercrime

However, Russia's strong STEM education is no guarantee that Russian IT professionals can find gainful employment. On the one hand, high levels of educational attainment are clearly valued in Russian society. In 2019, 63 percent of Russian 25-34 year-olds had achieved some level of tertiary education, compared with the Organization for Economic Co-operation and Development (OECD) average of 44 percent.[45] Many Russian postsecondary students pursue degrees in IT specifically.[46] Yet the Russian labor market, like those of many other post-Soviet economies, is inefficient and struggles to place well-educated workers in their fields of study.[47] In addition, while many prospective Russian IT students cite job prospects and high wages as their motivation for choosing their field of study, they may have unrealistic expectations regarding entry-level wages.[48] Finally, there may well be more highly-educated IT professionals in Russia than there are legitimate IT jobs.[49] Even the IT professionals who can find jobs work for "economical wages,"[50] at least by international standards. While this represents a great deal for multinational corporations seeking to develop software on the cheap, this presents Russian IT workers with powerful economic incentives to supplement their incomes.

The retributive legal barriers to cyber criminality that might dissuade an underemployed IT professional in other countries are much less compelling in Russia. Cybercrime is profitable globally,[51] but Russia is particularly permissive as it relates to cybercrime. Legal penalties for cybercrime under the Russian Criminal Code are considered quite weak by international standards,[52] and enforcement of those laws is selective, haphazard, and sometimes non-existent. According to Kyle Wilhoit, an internationally-recognized cybersecurity expert, "hackers only really get prosecuted when they attack targets inside Russia."[53] And Russian domestic authorities generally do not cooperate with the international law enforcement agencies that investigate cybercrimes.[54]

In addition, the early geographic concentration of Russia's internet infrastructure has exacerbated cost-of-living concerns for its cyber professionals. The build-out of Russia's early internet infrastructure around the country's academic and scientific institutions, made possible by the financial and technical assistance of foreign benefactors, created an "academic bias"[55] in Russian internet access. For the first two decades of internet connectivity, Russia's internet users, at least outside of the major metropolitan areas of Moscow and St. Petersburg, were concentrated around research centers in places like Novosibirsk. For many years, the Russian software industry was concentrated in those three cities.[56] This spatial polarization had important implications for the geographic distribution of the broader Russian economy. The economic benefits unlocked by digitization and electronic commerce were only available to populations living around places with existing internet infrastructure, places that were already home to most of Russia's most educated workers. Until the advent of mobile broadband, the Internet was a force for further economic concentration around a very few large cities rather than an economic leveler for the Russian regions. As a result, Russia's two

major metropolitan areas, Moscow and Saint Petersburg, are noteworthy for their high cost of living relative to local wages.

As a result, a significant number of Russian IT professionals may supplement legitimate incomes with criminal activity, leveraging professional talents to commit cybercrime that either targets or uses a computer, a computer network, or a networked device.[57] These Russian cybercriminals are representative of the broader Russian criminal population where members of Russian OCGs often straddle criminal and non-criminal careers.[58]

Early Russian cyber criminals operated independently in a disaggregated fashion, seeking to avoid drawing the attention of the state. Beginning in the late 2000s, this changed, with Russian cybercriminal activities increasingly coming under the control of traditional OCGs, which sought to extend their control over criminal activities from physical space to cyberspace.[59] Eight to twelve major nationwide OCGs operate in Russia today, with smaller nodes within these networks focused on particular aspects of criminal activity.[60] Russian OCGs are active across the full spectrum of criminality, engaging in illicit finance, the trafficking of weapons, drugs and people, and assassination for hire.[61] These OCGs now are also heavily involved in cybercrime, including credit card fraud, identity theft, the use of malware and ransomware for financial gain, and malware development for sale to external criminal actors.

One result of the co-opting of disaggregated, independent Russian cyber criminals by Russian OCGs is that cybercrime has become increasingly professionalized, and ironically mirrors somewhat the legitimate Russian IT industry. Today, organized cybercrime teams enable "individuals to branch out into a specific area of expertise,"[62] such as team leaders, coders, network administrators, intrusion specialists, data miners, and even financial specialists. The combination of increased professionalization and financial backing provided by established Russian OCGs has enabled Russian cybercriminal teams to increase the scope and scale of their hacking operations.[63] Recent examples of hacks by Russian OCG-backed cybercriminal groups include the high-profile ransomware attacks against Colonial Pipeline, JBS, and Kaseya,[64] as well as ongoing malicious cyber activities targeting Ukraine.[65]

Leveraging Corruption to Advance Foreign Policy Goals

Russia's pervasive culture of corruption helps explain how Russia's IT professionals are mobilized on the state's behalf to engage in offensive cybercrime in pursuit of Russia's geopolitical goals. While some hackers may be motivated in part by patriotism, corruption is the glue that binds together Russian IT professionals, cyber-criminals, and state security actors. While money is one factor that encourages participation in corrupt practices, self-preservation is another important motivation. In Russia, police and other government agents are known to violently enforce payment of protection money.[66] Paying bribes to government officials, police and tax inspectors by IT firms large and small is often necessary to avoid violence, imprisonment, and the shutdown of one's business. In the 1990s, most Russian IT out-

sourcing companies sought to "keep off the radar of the state and the tax police" until they became large enough to join the formal economy.[67] Importantly, corruption in Russia today extends far beyond the passing of bribes. For some Russian IT companies and professionals, hacking on behalf of the Russian state may be a way to avoid violent disruptions to their workplaces by the security services. While corruption seriously impedes the development of the Russian IT industry as a legitimate business sector, powerful incentives push Russian IT professionals to engage in malicious cyber activity on behalf of the Russian government.

The reciprocal nature of the relationship between organized crime and the state is also key to understanding how Russian cybercriminals mobilize on behalf of Russian foreign policy objectives. Cybercriminals are allowed to enrich themselves financially, provided the Russian state protecting cybercriminals can use their skills in support of Russia's goals.[68] Russian OCGs are also expected to avoid hacking targets within Russia. Committing cybercrimes on behalf of the state obviously allows willing participant OCGs to curry favor with political authorities and maintain their continued access to illicit opportunities.[69]

Relationships between the Russian state and Russian OCGs have their roots in the Soviet era but have shifted dramatically since then. The weakened central state of the 1990s presented OCGs with opportunities for massive financial gain as state assets were privatized.[70] Whereas OCGs concealed wealth from the state and the public during Soviet times, economic liberalization presented these entities the opportunity to convert criminal proceeds to legitimate wealth and ascend the ranks of Russian society.[71] The Russian state ultimately regained the upper hand, but did so without confronting or crushing empowered criminal enterprises.

One account describes the Russian state and Russian OCGs as having engaged in a process of reciprocal assimilation "in which intertwined networks of legality and illegality work in concert"[72] to maintain a grip on power in which the state and OCGs are mutually-dependent, semi-autonomous groups that share ideologies and resources. OCGs have "become an integral part of civil society"[73] and enjoy ties with the state at every level of socio-political power. While the state is the stronger of the two partners, it cooperates with OCGs to gain access to a deniable source of "private violence and illegal expertise."[74] This private expertise is enlisted by the state for its own purposes. Cybercriminal expertise is just one of these specialties, but is perhaps the most relevant criminal skillset to Russia's cyber power and global policy ambitions. The same technical knowledge that allows Russian OCGs to steal as much as trillions of dollars annually[75] can be leveraged for computer network exploitation and computer network attacks against foreign governments.

Cyber and Information Warfare

Cyber warfare, enabled by non-state cyber talent, has become a key tool in Russia's offensive defense strategy.[76] Putin professes that Russia and the West are already engaged in full-spectrum conflict,[77] and that the information sphere is but one key battleground in

this conflict. Putin purports to also believe that various democratic movements across the post-Soviet space, from the Orange Revolution to the Maidan Revolution, were organized by Western intelligence agencies with the ultimate goal of bringing about regime change in Russia.[78] In response, Russia has used its cyber power as part of a holistic information warfare strategy to sow discord across the West[79] and undermine unity between and within Western nations.[80] The cyber blockade of Estonia in 2007 by Russian non-state patriotic hackers and criminals[81] is the first known example of this trend, which arguably reached its apex in the Russian election interference campaigns in the United Kingdom, U.S. and France between 2015 and 2017.[82]

Russian leaders see the internet inside Russia primarily in terms of its potential to undermine regime stability.[83] Domestic legal and regulatory governance of the Russian internet lagged behind the build-out of the actual internet infrastructure,[84] yet state regulation of the Russian internet, or RuNet, increased following Putin's return as Russia's president in 2012. These regulations focus primarily on enabling surveillance of digital communications and restricting information flow that the Putin regime deems subversive to its aims. The origins of this approach can be found in the 2000 Information Security Doctrine of the Russian Federation, which declared that "the national security of the Russian Federation substantially depends on the level of information security." This doctrine defines information security as "national interests in the information sphere," referring to the regime's control over information flow to the public and not the safeguarding of networks and data.[85] In modern Russia, internet governance, cybersecurity, and media policy are all overseen by the same state agency, Roskomnadzor,[86] underscoring Russia's priority for internet governance being information control. Yet in line with Putin's alleged promise of "a decade of free development"[87] to the Russian IT industry at a December 28, 1999 meeting, internet entrepreneurship and commercial activity in Russia remain highly deregulated, a surprising approach for the Russian government, which is inclined towards "active regulation of most spheres of economic activity."[88]

Russia has begun to lay the technical groundwork to isolate the RuNet from the broader World Wide Web. In 2019, the Duma amended Russian federal law to provide a legal framework for the "centralized management of a public communications network." This framework empowers Roskomnadzor to "prohibit the routing of telecommunication messages through communication networks located outside of the territory of the Russian Federation" in the face of certain threats.[89] These amendments also call for the creation of a national Domain Name System (DNS), with its own proprietary infrastructure, which would be the first of its kind if implemented, and would render the RuNet inaccessible to the outside world. It also likely would disable internet users inside Russia from accessing parts of the Internet that use the existing global DNS.[90] This outcome would give Roskomnadzor unparalleled ability to control the flow of information into Russia.

Early Impacts of the Russo-Ukrainian War

Russia's invasion of Ukraine has shaken Russia's IT industry, with potential future consequences for Russian cyber power. In the first weeks after the invasion, tech workers fled Russia in droves. The Russian Association of Electronic Commerce, a Russian tech industry trade group, estimated some 50,000-70,000 tech workers left Russia during the first few weeks of the war.[91] At first, the Russian government sought to reassure the country's tech industry. In his annual address to the Russian Duma in early April 2022, Russian Prime Minister Mikhail Mishustin addressed the Russian IT industry directly, and Russia's government extended several guarantees to Russian IT professionals, including a promise that Russia's IT professionals would not be conscripted into the army. Other incentives included "exemptions from paying income tax, preferential mortgage rates, and additional funding for grants."[92] Yet Putin's so-called "partial mobilization" order in September 2022, seeking to press 300,000 men into military service, prompted a second mass exodus of IT professionals. Nikolay Komlev, director of Russia's Information & Computer Technologies Industry Association, claimed this wave of departures, notwithstanding Kremlin promises to exempt IT professionals from the draft, was "roughly two to three times" the size of the spring wave.[93] Many tech workers fled to other post-Soviet states like Armenia and Kazakhstan, even if they still worked for Russian companies.

The Russian government's crackdown on foreign platforms to more tightly control information flow to its citizens has also intensified. Post-invasion Russia has blocked Facebook, Twitter, and the Russian-language websites of several international news outlets.[94] In announcing the bans, Roskomnadzor accused Facebook, which had blocked the pages of state-controlled Russian media outlets like Russia Today and Sputnik, of violating "the key principles of free dissemination of information."[95]

In the near term, the Ukraine invasion is unlikely to degrade Russia's cyber power. It is likely the Russian IT industry will feel pressure to avoid or accommodate state attention, and this may improve the Kremlin's ability to leverage native IT talent in pursuit of its geopolitical ambitions. Western sanctions and export controls also may have the unintended effect of catalyzing Russian import substitution. Sanctions not only have limited Russia's access to key technologies but also have prompted U.S.-based technology firms like Microsoft to leave the Russian market.[96] This could present a market opportunity for Russian IT firms to develop domestically-produced alternatives to Western products, at least as to software, where the barriers to development are lower. Similarly, many Western research organizations halted collaborative efforts with Russian scientists after the Ukraine invasion.[97] Russians reportedly are increasingly collaborating with Chinese and Indian researchers, which may represent a model for collaboration in the Russian IT sector, although both India and China have deep state involvement in their respective technology sectors, thus making such partnerships less appealing to Russian firms.

In the medium-to-long term, the floodgate of departed Russian IT talent likely will limit Russia's ability to develop high-end cyber capabilities. Importantly, many departures during the first year of the war included those IT workers with international ties and some amount of financial resources. These IT professionals are likely some of Russia's best and brightest.[98] Another big risk Russia faces is that departed IT talent will hamper the education and training of future generations of Russian cyber talent, an effect that could compound as time passes.

CONCLUSION

Russia's disproportionate cyber power stems largely from its unique political, economic, and regulatory circumstances post-dating the collapse of the Soviet Union. Pervasive networks of corruption connect Russian IT professionals, Russian OCGs, and the Russian state, allowing the state to mobilize the tech industry's cyber talent for geopolitical goals. To formulate policies towards Russia that counter Russia's pervasive cybercrimes, Western governments should recognize that failing to address these three entities holistically is a fool's errand. Incentives that bind Russia's networks of corruption are far too strong to be effectively countered with piecemeal high-level diplomatic summits. But Russia's invasion of Ukraine presents the West with a unique opportunity to exploit the mass exodus of human capital Russia desperately needs in order to remain a top-tier cyber power. Western governments should further facilitate this exodus of Russian IT professionals with proactive integration into friendly nation workforces. For example, tens of thousands of Russian IT professionals now reside and work in the nation of Georgia.[99] In response, the Georgian government stood up a task force to help Russian companies and entrepreneurs navigate financial and bureaucratic hurdles. Western governments can and should pursue similar initiatives and find ways to incentivize companies that facilitate this migration.

NOTES

1. Voo, Julia, Irfan Hemani, and Daniel Cassidy. "National Cyber Power Index 2022." (Cambridge: Belfer Center for Science and International Affairs, Harvard Kennedy School, 2022), 7. https://www.belfercenter.org/publication/national-cyber-power-index-2022
2. Whyte, Christopher, and Brian Mazanec. In *Understanding Cyber Warfare: Politics, Policy and Strategy*, (New York: Routledge, 2019), 119-20.
3. "World Economic Outlook Update, January 2024: Moderating Inflation and Steady Growth Open Path to Soft Landing." (World Economic Outlook. International Monetary Fund, January 2024), 6. https://www.imf.org/en/Publications/WEO/Issues/2024/01/30/world-economic-outlook-update-january-2024.
4. Chernova, Yuliya. "Departure of Tech Workers Weighs on Russian Economy." WSJ, November 13, 2022. https://www.wsj.com/articles/departure-of-tech-workers-weighs-on-russian-economy-11668172429.
5. Voo, et al.,. "National Cyber Power Index 2022," 9.
6. Insikt Group. "Dark Covenant 2.0: Cybercrime, the Russian State, and War in Ukraine." Recorded Future, January 31, 2023, 2. https://go.recordedfuture.com/hubfs/reports/cta-2023-0131.pdf.
7. Perfiliev, Yuri. "Development of the Internet in Russia: Preliminary Observations on Its Spatial and Institutional Characteristics." (Eurasian Geography and Economics 43, no. 5, July 2002): 412. https://doi.org/10.2747/1538-7216.43.5.411.
8. Bulashova, Natlia, Dmitri Burkov, Alexey Platonov, and Alexey Soldatov. "An Internet History of Russia in 1990s." In An Asia Internet History: First Decade (1980-1990), edited by Kilnam Chon, 227–64. (Seoul: Seoul National University Press, 2013). Accessed date, Asia Internet History Projects at https://sites.google.com/site/internethistoryasia/book1/ru.
9. Perfiliev. "Development of the Internet in Russia: Preliminary Observations on Its Spatial and Institutional Characteristics," 414.
10. Kolarova, Desislava, Asel Samaganova, Ivan Samson, and Patrick Ternaux. "Spatial Aspects of ICT Development in Russia." The Service Industries Journal 26, no. 8 (2006): 877. https://doi.org/10.1080/02642060601011673.
11. Perfiliev, "Development of the Internet in Russia: Preliminary Observations on Its Spatial and Institutional Characteristics," 414.
12. Bulashova, et al., "An Internet History of Russia in 1990s".
13. Kolarova, et al., "Spatial Aspects of ICT Development in Russia," 876.
14. Bulashova, et al., "An Internet History of Russia in 1990s".
15. Kolarova, et al., "Spatial Aspects of ICT Development in Russia," 876.
16. Loren, Graham. "Science in the New Russia." Issues in Science and Technology (blog), July 1, 2003. https://issues.org/graham-2/.
17. "Science and Engineering Indicators, 2004. Volume 2: Appendix Tables. NSB 04-01." (Arlington: National Science Foundation, 2004).
18. Aslund, Anders, Sergei Guriev, and Andrew Kuchins. *Russia after the Global Economic Crisis*. (Washington: Peterson Institute for International Economics, 2010), 96.
19. Perfiliev. Development of the Internet in Russia: Preliminary Observations on Its Spatial and Institutional Characteristics." 412.
20. Satinsky, Daniel. "The Growth of Russia's IT Outsourcing Industry: The Beginning of Russian Economic Diversification?" Wilson Center, April 17, 2006. https://www.wilsoncenter.org/publication/the-growth-russias-it-outsourcing-industry-the-beginning-russian-economic.
21. Gritsenko, Daria, Mikhail Kopotev, and Mariëlle Wijermars. "Digital Russia Studies: An Introduction." In The Palgrave Handbook of Digital Russia Studies, edited by Daria Gritsenko, Mariëlle Wijermars, and Mikhail Kopotev. (Cham: Springer International Publishing, 2021), 6. https://doi.org/10.1007/978-3-030-42855-6_1.
22. Perfiliev, "Development of the Internet in Russia: Preliminary Observations on Its Spatial and Institutional Characteristics." 412.
23. Goldman, Marshall I. *In Petrostate Putin, Power, and the New Russia.* (Oxford ; Oxford University Press, 2008), 61.
24. Aslund, et al., *Russia after the Global Economic Crisis*, 100.

NOTES

25. Satinsky, "The Growth of Russia's IT Outsourcing Industry: The Beginning of Russian Economic Diversification?'
26. Rossotto, Carlo Maria, Natalija Gelvanovska, Dr Yuri Hohlov, Dr Vaiva Mačiulė, and Sergei Shaposhnik. "A Sector Assessment: Broadband in Russia," (Washington: The World Bank, 2015), accessed via Research Gate at https://www.researchgate.net/publication/293485750_A_Sector_Assessment_Broadband_in_Russia, 30.
27. Rossotto, et al.,. "A Sector Assessment: Broadband in Russia," 7.
28. Galushkin, Alexander. "Internet in Modern Russia: History of Development, Place and Role." Asian Social Science 11 (June 5, 2015): 306. https://doi.org/10.5539/ass.v11n18p305.
29. Rossotto, et al. "A Sector Assessment: Broadband in Russia," 7.
30. Adya, Monica, and Kate M. Kaiser. "Early Determinants of Women in the IT Workforce: A Model of Girls' Career Choices." Information Technology & People 18, no. 3 (2005): 237–238. https://doi.org/10.1108/09593840510615860.
31. Yarrow, Andrew L. "The Scandalous Cost of Internet in America." (Santa Monica: Milken Institute, June 17, 2021). https://www.milkenreview.org/articles/the-scandalous-cost-of-internet-in-america.
32. Pew Research Center. "Internet/Broadband Fact Sheet," April 7, 2021. https://www.pewresearch.org/internet/fact-sheet/internet-broadband/.
33. Powell, Alison, Amelia Bryne, and Dharma Dailey. "The Essential Internet: Digital Exclusion in Low-Income American Communities." *Policy & Internet* 2, no. 2 (January 18, 2010): 159–90. https://doi.org/10.2202/1944-2866.1058.
34. Lee, Nicol Turner, James Seddon, Samantha Lai, and Brooke Tanner. "Why the Federal Government Needs to Step up Efforts to Close the Rural Broadband Divide." *Brookings* (blog), October 4, 2022. https://www.brookings.edu/research/why-the-federal-government-needs-to-step-up-their-efforts-to-close-the-rural-broadband-divide/.
35. Kleist, Virginia Franke, Amy B. Woszcynski, Humayun Zafar, and Pamila Dembla. "The Russian and Ukrainian Information Technology Outsourcing Market: Potential, Barriers and Management Considerations." Journal of Global Information Technology Management 18, no. 1 (January 2, 2015): 7. https://doi.org/10.1080/1097198X.2015.1015824.
36. Oliss, Brendan, Cole McFaul, and Jaret C. Riddick. "The Global Distribution of STEM Graduates: Which Countries Lead the Way?" Center for Security and Emerging Technology (blog), November 27, 2023. https://cset.georgetown.edu/article/the-global-distribution-of-stem-graduates-which-countries-lead-the-way/.
37. National Center for Education Statistics. "COE - Undergraduate Degree Fields," May 2023. https://nces.ed.gov/programs/coe/indicator/cta.
38. Aslund, et al., *Russia after the Global Economic Crisis,* 97.
39. Kleist, Virginia Franke, Amy B. Woszcynski, Humayun Zafar, and Pamila Dembla. "The Russian and Ukrainian Information Technology Outsourcing Market: Potential, Barriers and Management Considerations." Journal of Global Information Technology Management 18, no. 1 (January 2, 2015): 9. https://doi.org/10.1080/1097198X.2015.1015824.
40. Satinsky, "The Growth of Russia's IT Outsourcing Industry: The Beginning of Russian Economic Diversification?"
41. Gibson, Stan. "Outsourcing: The Russian Revelation." eWEEK, June 12, 2006. https://www.eweek.com/it-management/outsourcing-the-russian-revelation/.
42. Gibson, "Outsourcing: The Russian Revelation"
43. Satinsky, "The Growth of Russia's IT Outsourcing Industry: The Beginning of Russian Economic Diversification?"
44. Metz, Cade, and Adam Satariano. "Russian Tech Industry Faces 'Brain Drain' as Workers Flee." The New York Times, April 13, 2022, sec. Technology. https://www.nytimes.com/2022/04/13/technology/russia-tech-workers.html.
45. Organisation for Economic Co-Operation and Development (OECD). Education at a Glance 2019: OECD Indicators. Education at a Glance. 2. https://www.oecd.org/education/education-at-a-glance/
46. Regnum News Agency. "What professions do Russian school graduates choose in 2021?," March 19, 2021. https://regnum.ru/news/3219644, translated by Google.
47. Round, John, Colin C. Williams, and Peter Rodgers. "Corruption in the Post-Soviet Workplace: The Experiences of Recent Graduates in Contemporary Ukraine." Work, Employment and Society 22, no. 1 (March 1, 2008), at 152. https://doi.org/10.1177/0950017007087421.
48. Alekseev, Dmitry. "Increased Demand: Russian Schoolchildren Choose IT Professions." (February 25, 2022). https://iz.ru/1295504/dmitrii-alekseev/povyshennyi-spros-rossiiskie-shkolniki-vybiraiut-it-professii.
49. Kadlecová, "Russian-Speaking Cyber Crime: Reasons behind Its Success." The European Review of Organised Crime, 2015, 8. https://www.academia.edu/16548880/Russian_speaking_Cyber_Crime_Reasons_behind_Its_Success.

NOTES

50. Kleist, Virginia Franke, Amy B. Woszcynski, Humayun Zafar, and Pamila Dembla. "The Russian and Ukrainian Information Technology Outsourcing Market: Potential, Barriers and Management Considerations." Journal of Global Information Technology Management 18, no. 1 (January 2, 2015): 7.
51. Trellix. "Growling Bears Make Thunderous Noise," June 6, 2022. https://www.trellix.com/blogs/research/growling-bears-make-thunderous-noise/.
52. Kadlecová, "Rusasian-Speaking Cyber Crime: Reasons behind Its Success," 10.
53. KNBC News. "Skilled, Cheap Russian Hackers Power American Cybercrime," February 5, 2014. https://www.nbcnews.com/news/world/skilled-cheap-russian-hackers-power-american-cybercrime-n22371.
54. Kadlecová, "Russian-Speaking Cyber Crime: Reasons behind Its Success," 10.
55. Kolarova, et al. "Spatial Aspects of ICT Development in Russia," 877.
56. Kolarova, et al, "Spatial Aspects of ICT Development in Russia," 884.
57. Kaspersky Labs. "What Is Cybercrime? How to Protect Yourself from Cybercrime," June 9, 2023. https://usa.kaspersky.com/resource-center/threats/what-is-cybercrime.
58. Stephenson, Svetlana. "It Takes Two to Tango: The State and Organized Crime in Russia." Current Sociology 65, no. 3 (May 1, 2017): 413. https://doi.org/10.1177/0011392116681384.
59. Kadlecová, "Russian-Speaking Cyber Crime: Reasons behind Its Success," 6.
60. Global Organized Crime Index. "Criminality in Russia - The Organized Crime Index," 2021. https://ocindex.net/.
61. Galeotti, Mark. "Crimintern: How the Kremlin Uses Russia's Criminal Networks in Europe." ECFR, April 18, 2017. https://ecfr.eu/publication/crimintern_how_the_kremlin_uses_russias_criminal_networks_in_europe/.
62. Google Threat Analysis Group. "Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape." Google Threat Analysis Group, February 16, 2023. https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/.
63. Kadlecová, "Russian-Speaking Cyber Crime: Reasons behind Its Success." 6.
64. Dark Covenant: Connections Between the Russian State and Criminal Actors." Recorded Future, September 9, 2021. https://go.recordedfuture.com/hubfs/reports/cta-2021-0909.pdf.
65. Insikt Group. "Dark Covenant 2.0: Cybercrime, the Russian State, and War in Ukraine." Recorded Future, January 31, 2023. https://www.recordedfuture.com/dark-covenant-2-cybercrime-russian-state-war-ukraine.
66. Aslund, et al., *Russia after the Global Economic Crisis*, 123.
67. Satinsky, "The Growth of Russia's IT Outsourcing Industry: The Beginning of Russian Economic Diversification?".
68. Bajak, Frank. "How the Kremlin Provides a Safe Harbor for Ransomware." AP News, April 16, 2021. https://apnews.com/article/business-technology-general-news-government-and-politics-c9dab7eb3841be45dff2d93ed3102999.
69. Stephenson, "It Takes Two to Tango: The State and Organized Crime in Russia," 413.
70. Stephenson, "It Takes Two to Tango: The State and Organized Crime in Russia," 414.
71. Stephenson, "It Takes Two to Tango: The State and Organized Crime in Russia," 416.
72. Stephenson, "It Takes Two to Tango: The State and Organized Crime in Russia," 412.
73. Popov, Mikhail Yu., Andrey P. Mikhaylov, Ilya V. Pechkurov, Alexander A. Korovin, and Dmitriy N. Tishkin. "Relationship of Corruption and Organized Crime Groups in the Russian Society." In *Public Administration and Regional Management in Russia: Challenges and Prospects in a Multicultural Region*, edited by Elena G. Popkova and Konstantin V. Vodenko, 325. Contributions to Economics. (Cham: Springer International Publishing, 2020). https://doi.org/10.1007/978-3-030-38497-5_36.
74. Stephenson, "It Takes Two to Tango: The State and Organized Crime in Russia." 413.
75. Fleck, Anna. "Infographic: Cybercrime Expected To Skyrocket in Coming Years." Statista Daily Data, February 22, 2024. https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027.
76. Hill, Fiona. "Mr. Putin and the Art of the Offensive Defense: Approaches to Foreign Policy (Part Two)." Brookings, March 16, 2014. https://www.brookings.edu/articles/mr-putin-and-the-art-of-the-offensive-defense-approaches-to-foreign-policy-part-two/.
77. Reynolds, Maura. "'Yes, He Would': Fiona Hill on Putin and Nukes." *POLITICO*, February 28, 2022. https://www.politico.com/news/magazine/2022/02/28/world-war-iii-already-there-00012340.

NOTES

78. Wilde, Gavin, and Justin Sherman. "No Water's Edge: Russia's Information War and Regime Security." Carnegie Endowment for International Peace, January 4, 2023. https://carnegieendowment.org/2023/01/04/no-water-s-edge-russia-s-information-war-and-regime-security-pub-88644.
79. Connell, Michael, and Sarah Vogler. "Russia's Approach to Cyber Warfare." CNA, March 24, 2017. https://www.cna.org/reports/2017/russias-approach-to-cyber-warfare.
80. Whyte and Mazanec, *Understanding Cyber Warfare: Politics, Policy and Strategy,* 235.
81. Whyte and Mazanec, *Understanding Cyber Warfare: Politics, Policy and Strategy,* 234.
82. Whyte and Mazanec, *Understanding Cyber Warfare: Politics, Policy and Strategy,* 235.
83. Wilde, Gavin, and Justin Sherman. "No Water's Edge: Russia's Information War and Regime Security." Carnegie Endowment for International Peace, January 4, 2023. https://carnegieendowment.org/2023/01/04/no-water-s-edge-russia-s-information-war-and-regime-security-pub-88644.
84. Sukhodolov, Alexander P., Elena G. Popkova, and Irina M. Kuzlaeva. "Peculiarities of Formation and Development of Internet Economy in Russia," in *Internet Economy vs Classic Economy: Struggle of Contradictions. Studies in Computational Intelligence*, vol 714. (Cham: Springer, 2018), 66 accessed at https://link.springer.com/chapter/10.1007/978-3-319-60273-8_6
85. Wilde and Sherman, "No Water's Edge: Russia's Information War and Regime Security."
86. Maréchal, Nathalie. "Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy." Media and Communication 5, no. 1 (2017): 32. https://doi.org/10.17645/mac.v5i1.808.
87. Gritsenko, et al., "Digital Russia Studies: An Introduction." 7.
88. Sukhodolov,et al., "Peculiarities of Formation and Development of Internet Economy in Russia." 67.
89. Epifanova, Alena. "Deciphering Russia's 'Sovereign Internet Law,'" *German Council on Foreign Relations*, January 2020. https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law, 6.
90. Epifanova, "Deciphering Russia's "Sovereign Internet Law," 8.
91. Al Jazeera, "Shunned by the West, Russia's IT Sector Goes on the Defensive," November 21, 2022. https://www.aljazeera.com/news/2022/11/21/russias-it-sector-facing-ctrl-alt-delete-moment-in-midst-of-war.
92. Al Jazeera, "Shunned by the West, Russia's IT Sector Goes on the Defensive"
93. Chernova, Yuliya. "Departure of Tech Workers Weighs on Russian Economy." *WSJ*, November 13, 2022. https://www.wsj.com/articles/departure-of-tech-workers-weighs-on-russian-economy-11668172429.
94. Milmo, Dan. "Russia Blocks Access to Facebook and Twitter." *The Guardian*, March 4, 2022, sec. World news. https://www.theguardian.com/world/2022/mar/04/russia-completely-blocks-access-to-facebook-and-twitter.
95. Government of Russia, Federal Service for Supervision of Communications, Information Technology, and Mass Media, News of Roskomnadzor, "Retaliatory measures have been taken to restrict access to Russian media," March 4, 2022. https://rkn.gov.ru/news/rsoc/news74156.htm. Translated by Google.
96. Al Jazeera, "Shunned by the West, Russia's IT Sector Goes on the Defensive."
97. Van Noorden, Richard, "Data Hint at Russia's Shifting Science Collaborations after Year of War." *Nature* 615, no. 7951 (February 24, 2023): 199–200. https://doi.org/10.1038/d41586-023-00552-w.
98. Metz and Satariano. "Russian Tech Industry Faces 'Brain Drain' as Workers Flee." *The New York Times*, (New York), April 13, 2022, sec. Technology. https://www.nytimes.com/2022/04/13/technology/russia-tech-workers.html..
99. Champion, Marc, and Helena Bedwell. "Russia's Brain Drain Is Officially Underway." *Bloomberg.Com*, July 6, 2022. https://www.bloomberg.com/news/features/2022-07-06/russian-refugee-tech-workers-make-georgia-a-stepping-stone-for-global-career.

Communities, Agency, and Resilience: A Perspective Addressing Tragedy of the Cyber Commons

Dr. Samir Jarjoui
Dr. Renita Murimi
Robert Murimi

ABSTRACT

Cybersecurity suffers from a "tragedy of the commons" problem, where people and institutions have adopted lax security practices due to a tendency to weigh the perceived costs of adopting sound cybersecurity practices as higher than their expected benefits. For example, despite advancements in cybersecurity measures and extensive investments in tools and strategies to counter cyberattacks, foundational best practices have faltered leading to global cybersecurity challenges. Part of the dilemma stems from the fact that cybersecurity continues to be approached with a limited mindset, which creates a significant threshold of social cohesiveness for combating cyber threats. In the meantime, the cyber threat landscape continues to proliferate and exploit the fragile networks that we all inhabit. This paper provides a community-centered framework for cyber resilience that offers a starting point for addressing the tragedy of the commons problem in cybersecurity.

INTRODUCTION

Who is responsible for cybersecurity? From a proactive stance, people have assumed that the responsibility of cybersecurity lies under the purview of "others," a loose category encompassing the information technology teams, services teams, cloud providers, administrators, vendors, clients,

Samir Jarjoui is the Director of IT at Herb Pharm. He has 15 years of experience in IT management, cybersecurity, internal audit, and risk management. His work focuses on business and IT alignment to optimize organizational capabilities. He holds several professional certifications in the field of cybersecurity and a DBA with a focus on cybersecurity from the University of Dallas. He is also an adjunct professor of business at Warner Pacific University.

and a plethora of other stakeholders. From a reactive stance, as in the aftermath of a cybersecurity incident, we have resorted to shifting the onus of responsibility onto "others," assuming that someone else should have done better and prevented the cybersecurity incident from happening in the first place. This is similar to the problems surrounding climate change, where people all over the world have consumed natural resources without regard for consumption's wider effects, leading to poor environmental conditions for all of us. This situation was termed the "tragedy of the commons" by ecologist Garrett Hardin in his 1968 article referring to the adverse effects of overconsumption of scarce common resources.[1] In the context of environmental stewardship, the tragedy of commons (ToC) problem refers to finite environmental resources that risk being driven to empty when faced with users who over-consume them. Thus, a finite resource faces over-usage by individual actors who discount the impact of their usage patterns on the sustainability of the finite resource for the rest of the actors and for future generations.

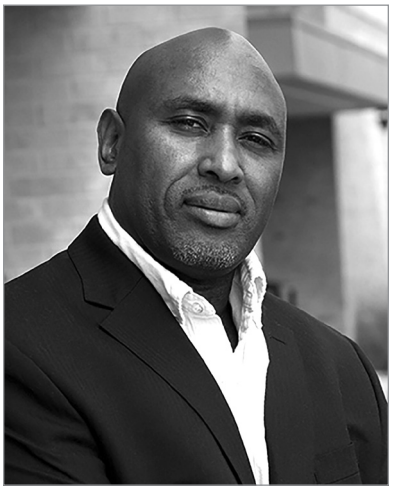
In the context of cybersecurity, however, we suggest that there is no single finite resource that is being driven to extinction. Cybersecurity is not a finite environmental resource like clean water or air. However, the resources to create, maintain, and sustain the security of our networks and data are finite. There are four kinds of resources used in cybersecurity that are closely interdependent. First, monetary resources that govern the investments made in cybersecurity infrastructure are limited, due to the finite nature of budgets where the return on investment for cybersecurity expenses is not easily quantified. Second, the hardware and software tools required to secure networks (whether cloud-based or physical infrastructure) are constrained by various factors related to the spatial needs of organizations and the associated monetary constraints. Third, the field of cybersecurity expands rapidly due to continuously emerging threats

Renita Murimi (IEEE SM'21) received her PhD and MS in Electrical Engineering from New Jersey Institute of Technology, and a Bachelor of Engineering in Electronics and Communications from Manipal Institute of Technology in India. She is an Associate Professor of Cybersecurity at the University of Dallas. Her current research interests are in the areas of cybersecurity and network science.

from a multitude of attackers with varying levels of resources. The continuous learning involved in staying abreast of recent challenges and developments of countermeasures pose significant temporal and cognitive constraints on the ability to defend our networks and make them resilient when attacked. Finally, the field of cybersecurity is characterized by substantial constraints in recruiting a qualified workforce. The talent shortage in cybersecurity has created a supply-demand gap in the cybersecurity workforce that leaves positions vacant as threats continue to proliferate. The commons of cybersecurity, thus, are the resources required to protect cyberspace from adversaries.

Much has been written about whether the Internet or cyberspace constitute commons at all. Digital commons have been analyzed in the context of cyberspace freedoms,[2] the electromagnetic spectrum,[3] and in the context of the generation of data, information, culture, and knowledge.[4-6] The ToC problem was also studied in the context of online consumer communities, where user tendencies to free ride instead of contributing were identified as a challenge to the sustainability of the commons.[7] Other forms of the digital commons have been conceptualized, including social media commons,[8] open-source software commons,[9] bandwidth and information commons,[10,11] and the commons of public trust that users place in cyberspace.[12] Simultaneously, previous research has refuted the notion of the Internet as commons by arguing that the Internet is neither "exclusionary nor rivalrous," and hence does not qualify as a commons.[13] Dan Hunter proposed that the Internet is a digital anti-commons, wherein private ownership of different kinds of online resources (licenses, permissions, and copyrights) prevents others from optimally using the resource.[14]

Over the years, the unrelenting pace of cyber incidents is a stern reminder of the inadequacies of current cybersecurity solutions. Furthermore, in technologically advanced societies, cyber threats are often



Robert Murimi received his MS in Computer Engineering from New Jersey Institute of Technology and a BS in Computer Science from New Jersey City University. Currently, he is pursuing a DBA with a focus in cybersecurity from the University of Dallas. He has over fifteen years of experience in software development, and is currently a software engineer at McKesson.

magnified by additional challenges such as antiquated, strained, and complex critical infrastructure systems, further complicated by the vast interconnectivity of many global communication systems.[15] We argue that it is time for a new approach to address the root causes of ToC in cybersecurity, one that can be tailored to building cyber-resilient communities to deal with evolving threats. People are quick to dismiss their role in protecting their networks and data, often relying on ignorance, or a tendency to underestimate the impact of their inadequate efforts, or a dependence on "others" to play their part in cyber security. The often-used aphorism of "it is not a question of whether, but when we will be hacked" points to a reluctant acceptance of the notion that nothing can be done to protect oneself in the cybersecurity war. Thus, a different ToC has unfolded in our digital environments, one where the impact of one's actions is not fully understood, and so the operational attitude is to resign to the occurrence of the inevitable breach or wait for "others" to do something to contain the fallout. ToC, thus, is a driving factor in the challenges to cyber defense that confront our fragile networks, where threat actors can advance their strategic and geo-political interests by furthering information warfare.

We see hope in a radical solution for ToC, of the kind that Elinor Ostrom proposed when she suggested that regulation was not the only way to proceed when it came to climate change.[16] Her work, eventually leading to the 2009 Nobel Prize in Economics, studied how small, stable communities under certain conditions manage their local common resources without falling victim to the ToC tragedy. A similar mindset could be utilized to adapt Ostrom's approach to ToC in cybersecurity. Ostrom's approach to addressing the ToC problem helped shift the focus away from top-down governance and regulatory approaches as the only mechanism to address the ToC problem. Her grassroots, bottom-up approach was proposed as a

supplement to regulation, and not a superior approach to regulation. Thus, her approach for cooperative institutions that were organized and run by the users of the resources brought a new approach to the field of commons management as a whole. Ostrom's approach has led to the formation of design principles that were influential in the management of common pool resources, from which sound inferences about commons and their management for diverse applications can be made.

In this article, we propose a systems approach[17] to develop cyber-resiliency for transcending the ToC problem in cybersecurity. Our solution framework outlines three dimensions—innovative learning, awareness, and adaptability—as the essential foundation for cyber-resilient communities who can effectively anticipate risk, mitigate deficiencies, and recover from inevitable cyberattacks. We believe our framework can help accelerate the emergence and sustainability of cyber-resilient communities, which in turn can influence the development of new communities to reach a magnitude and intensity that overcomes the problem of ToC in cybersecurity. In the next section, we outline the need not just for cybersecurity, but for a broader goal of cyber resilient commons.

The Need for Resilient Commons

Resilient cyber communities go hand in hand with resilient cyber commons. Resilience requires a rapid restoration of resources and proactive efforts that begin with acknowledging the inherent risks to the resources. Cyber attacks are characterized chiefly by an asymmetric distribution of information. This asymmetry extends to various facets of cybersecurity. When cybersecurity countermeasures that are deployed to thwart attacks work efficiently, the defenders have the upper hand. Conversely, when these measures fail, the attackers have the upper hand. The sophistication of the attacks points to an asymmetric distribution of resources and accountability for attackers. This is because for attackers it is enough to launch a successful attack only once, but defenders have to be on guard all the time.

The lack of standardization in cybersecurity defenses also leads to a variety of cybersecurity postures adopted by individuals and organizations. This asymmetry in cybersecurity postures makes it easier for attackers to go after organizations with weaker deterrence initiatives. Further, there is asymmetry involved in the accountability assigned to attackers and defenders. In certain kinds of cyber attacks such as denial-of-service attacks, when an individual's or an organization's network is attacked, the response to the attack involves network redesign or network repair, both of which are resource-intensive efforts without any immediate payback for the attacker. In other kinds of attacks such as ransomware attacks, if the victim does not pay the ransom, the attacker does not receive the ransom but still has access to the exfiltrated data from the ransom attack. For example, when a hacker group breaches a network or an individual account, the victims are not able to hold the attackers responsible or launch counterattacks to deter them. Thus, intrusions can't be matched with counter-intrusion, unless external forces such as governments and political institutions intervene. Typically, such

interventions are reserved only for highly disruptive attacks motivated by overt geo-political tensions. This asymmetry of attacker resources, attack vectors, and attack outcomes creates a disjointed cybersecurity landscape, where individuals and organizations find it more convenient to resort to the ToC mode of operations rather than explore multidimensional solutions that go beyond technological countermeasures. The past few decades have shown us that an effective cybersecurity strategy is a proactive one that allows for continuity and restoration of operations when faced with an attack, creating resilience in our digital infrastructure.

In general, resilience refers to the ability to adapt in a positive manner despite experiencing adversity.[18,19] Resilient systems can transcend changes and disturbances while retaining the same essential structure and capacity.[20] Existing literature on cyber resilience has risen out of the experiences and challenges of implementing cyber resilience within specific application domains. Cyber resilience lies at the intersection of several interconnected business and technology processes, such as supply chain,[21-23] critical infrastructure,[24-26] cyber-physical systems,[27-29] and the financial sector.[30] As cyber resilience continues to gain prominence, organizations such as MITRE and NIST have developed extensive frameworks to design, execute, and assess cyber resilience within organizations.[31] Other significant frameworks and metrics include the World Economic Forum (WEF)'s cyber resilience framework, the Department of Homeland Security (DHS)'s Cyber Resilience Review, and the Software Engineering Institute's Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) and CERT-Resilience Management Model (RMM) frameworks.

Our article is the first to suggest that cybersecurity suffers from the ToC problem, whose solution lies not just in technological but socio-technical approaches to understanding the impact of our actions in our networks. Below, we outline a community-centered framework for cultivating cyber resilience which includes the attributes of innovative learning, awareness, and adaptability to address the root causes of ToC in cybersecurity holistically. The next section describes our motivation for a community-centered framework for developing cyber resilience.

THE MOTIVATION FOR A COMMUNITY-CENTERED FRAMEWORK IN CYBER RESILIENCE

ToC, at its core, is a problem that affects entire communities – here, we use the term "community" rather loosely. As such, solutions that address ToC – whether in environmental stewardship or in cybersecurity – are best designed with an emphasis on communities. In this context of cybersecurity commons, a community could refer to a group of individuals or organizations that use a certain portion of cyberspace or an online network. This description of a community affords flexibility of scale, since networks and subnetworks could be differentiated into various levels of hierarchical online communities. Thus, a community could be the groups of Computer Science students at a college who receive university communications through a learning management system, residents of a town who receive water and trash utilities, employees of an organization's online social network groups, or any other configuration

of online networks and their users. An analysis of the root causes of ToC in cybersecurity points to the following three main themes that inhibit effective cyber resilience – i) superficial cyber resilience approaches ii) failure to reach a tipping point, and iii) lax cybersecurity efforts, as described next.

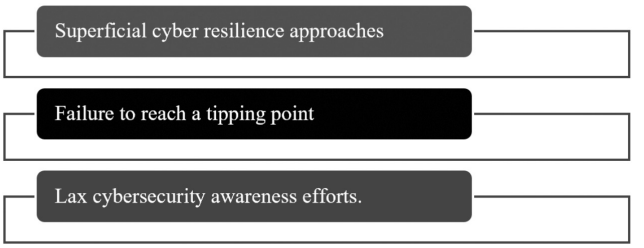


Fig. 1. Categories of challenges to cyber resilience

Superficial Cyber Resilience Approaches

An examination of well-established cyber resilience publications shows that cyber resilience initiatives have been primarily conveyed as a derivative of traditional cyber risk management and incident response strategies. For example, mainstream and prominent cybersecurity advocates, which includes organizations such as MITRE, the National Institute of Standards and Technology (NIST), and the International Organization for Standardization (ISO), continue to leverage a commonly used set of principles for cybersecurity risk management and cyber resilience artifacts, which typically include the general categories of assessment, detection, response, and recovery.[32,33] In addition, the overlap between cybersecurity and cyber resilience approaches has not been well defined and it is not clear how the two fields complement one another to optimize outcomes.

Further, while cybersecurity has benefited from existing and traditional risk management methodologies, social and cultural considerations continue to be a missing component in most existing strategies for combating cyber threats.[34,35] Without such multi-dimensional considerations, cybersecurity investments and efforts fail to generate the level of engagement needed to influence citizens on a global scale, thereby failing to solve the cybersecurity ToC problem.

Failure to Reach a Tipping Point

Cybersecurity investments continue to increase exponentially at the organizational and governmental levels, but cyber behavior lags behind despite best practices and threat intelligence warnings.[36,37] The actions of individuals can have profound implications, as demonstrated by the case of phishing attacks that require a few or even one compromised account to serve as an entry point for malware. Thus, despite existing efforts and the emergence of cyber resilience as a top priority for cybersecurity practitioners,[38] cybersecurity efforts have so far failed to reach a "tipping point" that enables transformation in cyber behavior at the global level.[39] Individual users' weak cybersecurity practices coupled with network security flaws are two critical areas that offer areas of improvement for reaching a "tipping point" in the security of the cyber commons.

Tipping points occur when a series of small changes become significant enough to propel a system beyond a certain threshold into a new state.[40] Malcolm Gladwell describes various examples, such as fashion trends and social behavior, where small initial changes started a runaway process causing significant transitions.[41] This is the kind of runaway process we are advocating in this research: the ability to generate sufficient and sustainable collective momentum to reach a tipping point for responsible and mindful cybersecurity behavior. The failure to reach a tipping point also derives from the fact that cybersecurity efforts continue to be a top-down approach – initiated, organized, pushed, and managed by governments and institutional bodies with little to no engagement from individual users and communities.

Lax Cybersecurity Awareness Efforts

Due to the rapid evolution of information systems and interconnected communication devices, the Internet has become a significant part of individuals' lives. It is, therefore, imperative to cultivate a sense of awareness as a foundation to address the evolving cyber threat landscape. Such awareness is crucial to developing and maintaining cyber resilience, which entails the ability to transcend destructive cyberattacks and involves a certain level of security mindfulness to stay on course.[42]

Current cybersecurity approaches continue primarily to emphasize action-based efforts as information systems-centric measures, and do not frame awareness as a fundamental principle for combating cyber threats. In addition, many cybersecurity awareness training programs continue to fall short due to their misaligned objectives and foci.[43] While the importance of security awareness training has been widely recognized, awareness training programs need to evolve past being merely a "check-the-box" exercise. Awareness efforts need to transform into an emphasis on security mindfulness – changing the "DNA" of communities to produce responsible and security-conscious citizens. The dimensions of the proposed framework's cyber resilience are discussed in the next section.

OUR PROPOSED FRAMEWORK

A community-centric approach to cybersecurity differs from the many traditional approaches to cybersecurity. On one end of the spectrum, a traditional top-down approach neglects to consider the perspectives of stakeholders and communities that are impacted by the choice of cybersecurity policies and tools. A traditional ad hoc approach lies on the other end of the spectrum, where the cybersecurity initiatives that are adopted are mostly reactive, creating a patchwork of solutions that are redundant in some areas and leave coverage holes in other areas. The connectivity of our networks creates fertile conditions for attacks to spread laterally and vertically, mimicking the spread of diseases and epidemics through populations. However, while approaches such as herd immunity offer notable benefits to communities, our digital networks cannot be protected based on herd immunity. In a network of "n" devices where "n-1" devices are protected by strong countermeasures and the

remaining device is unprotected or weakly protected, that one unprotected or weakly protected device poses a significant threat to the security of the network. This single device is merely an example, and can be replaced by any of the following without loss of relevance: a weak link, poorly configured software, open port, lax firewall rule, successful phishing attempt, weak password, expired antivirus software, backdoor, or any of the countless ways that attackers exploit networks. The aforementioned list is only a list of flaws in the technologies, and does not even account for disruptions in the socio-technical, economic, geo-political, and environmental realms.

A community-centric approach to cyber resilience is built on a foundation of trust.[44] In the context of a community approach to the security of the cyber commons, trust is an outcome of the shared sense of community responsibility. Such an approach requires that individual and organizational stakeholders work to elevate the cybersecurity posture of all entities, even at the cost of potential short-term gains. For example, in 2016 the Dutch government adopted a policy that increased the encryption capabilities available to users.[45] Such an approach meant that the Dutch government would potentially face situations where they might need access to some information that was encrypted, but would be locked out of access to that information. The Dutch government's commitment to upholding encrypted communication for confidentiality and integrity is evident in their funding of OpenSSL which is an open-source implementation of the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols. Their motivation for supporting encrypted communication is in the interests of "fundamental rights and freedoms as well as security interests and economic interests." Another example of a trust-based approach to cybersecurity is that of organizations that reveal zero-day vulnerabilities and report all discovered bugs. It might be costly to engage in such efforts, especially when the secret hoarding of flaws might result in future leverage against competing organizations or nation-states. However, such myopic activities are detrimental to building cooperation and ensuring the maintenance of trust among stakeholders, keys to the community-centric approach.

One approach to a community-centric approach to cybersecurity is the National Cybersecurity Strategy released by the White House in March 2023. This strategy is based on five pillars: defend critical infrastructure, disrupt and dismantle threat actors, shape market forces to drive security and resilience, invest in a resilient future, and forge international partnerships to pursue shared goals. A common theme across these five pillars is the need for "stakeholder communities" in each of these pillars to collaborate in defending cyberspace. A different example of a community-centric approach to cybersecurity is the Japanese Cybersecurity Strategy passed by the National Center for Incident Readiness and Strategy for Cybersecurity (NISC).[46] Among other notable aspects, this strategy specified that all stakeholders (individual, civic, government, and companies) were responsible for the security of cyberspace and pointed to participation in information sharing as a prerequisite for a holistic cybersecurity strategy. Additionally, cooperative efforts and alliance building, both international and domestic,

were highlighted as key to building confidence and trust in strengthening Japan's own cybersecurity posture while also strengthening that of its partners. The cross-community collaboration programs, the strengthening of local communities and small and midsize enterprises (SMEs), and adopting this approach in multiple layers starting with the local community and leading up to the international community all characterize the community-based nature of the NISC's approach to the cybersecurity of the digital commons.

Our proposed framework is based on a community-centered, systems-thinking approach with a bottom-up methodology to change the current state of cyber-aloofness. This bottom-up approach is fueled by the concept of resilient communities and is based on the three foundational principles of innovative learning, awareness and adaptability, as pointed out earlier and as outlined in Fig. 2.

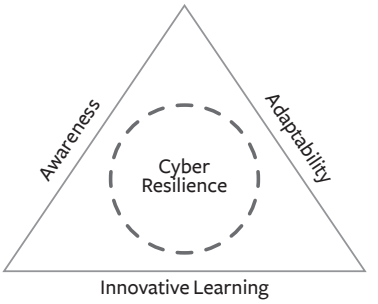


Fig. 2. A framework for cyber resilience.

Innovative Learning

The realization that digital grids around the world are a "commonly shared resource" would shift the task of cybersecurity from being someone else's responsibility to each and every individual user. Prior research has touted the power of change that is created "within" at the community level, where social, economic, cultural, and historic backgrounds are contextualized in the response to adverse events.[47,48] Leveraging innovative learning to create and sustain resilient communities is based on the premise that governments and institutional bodies are not the sole drivers of cyber resilience, although they can be an instrumental coordinator and sponsor. Therefore, a community-level focus on resilience promotes local engagement, accountability and flexibility in building cyber resilience.

In addition, a bottom-up approach would typically integrate social and structural aspects of cybersecurity, which are often overlooked, to drive change and investigate the root cause of cybersecurity risks at a deeper level. Further, a bottom-up community-based approach enables groups to acquire relevant institutional memory.[49,50] This localized knowledge can be leveraged by communities around the world, in accordance with their unique modes of learning and social attributes, to create a runaway process and momentum towards a tipping point in cyber resilience. Additionally, strengthening the capacity of community resilience can help build cyber resilience at the national or international levels, instead of fostering institutional or governmental dependencies.

Awareness

Despite the availability of sophisticated digital controls, technological countermeasures alone remain insufficient to protect users from online threats. Cyber controls can be rendered ineffective by the click of a button. The end-users are responsible for embracing privacy controls, using complex passwords, and adhering to cybersecurity policies and best

practices. A widely known cliché in cybersecurity is that "humans are the weakest link."[51] Lately, this cliché has met some pushback, with articles suggesting that humans are doing the best they can in the complex networked environments that they inhabit. Proponents of both these lines of contradicting thought agree that awareness is a key part of defense in the war against cybercrime.

In cybersecurity, the concept of awareness tends to manifest itself in the form of awareness programs and campaigns designed to educate and inform users to reduce risks.[52] While awareness programs can help develop resilience through the acquisition of knowledge needed to anticipate and respond to events, there are limitations to current approaches. Prior scholars noted that the predominantly used rule-based cybersecurity awareness training methodologies may not be effective in fending off attacks in the long run.

Cybersecurity awareness, as it exists today, largely remains a "check-the-box" compliance exercise and does not promote and sustain a deeper sense of mindfulness to achieve higher levels of resilience. Recent research has outlined three primary limitations of traditional rule-based cybersecurity awareness efforts: a superficial sense of mastery, lack of sufficient defenses against new and complex attacks, and inadequate ability to cultivate cognitive faculties to defend against sophisticated attacks. Furthermore, researchers have noted that there are differences in the mental models of security experts and non-expert users, which may result in communication and training gaps for mitigating cybersecurity risks.[53]

We argue that cybersecurity mindfulness extends beyond the scope of an individual. It is a broader and deeper sense of traditional cybersecurity awareness, and can be leveraged as an important building block to develop a "human firewall" culture within resilient communities. The ability to leverage the practice of cybersecurity mindfulness to make conscious and informed decisions can mean the difference between success and failure in cyber space. However, mindfulness as a building block of resilience is limited if it does not extend beyond the scope of an individual: resilient communities are built on interconnected structures of innovative learning, awareness, and adaptability.

Adaptability

Cyber security threats continue to evolve at a staggering pace and scale affecting all kinds of online entities. The policies, procedures, and controls that are developed in response to a particular threat must be continuously revised to counter different kinds of attacks and threats in different domains. Adaptability is, therefore, a key component of cyber resilience, where the solution frameworks are most effective if they are tailored to organizations and their capabilities. One resource for studying adaptability in cyber resilience can be found in the field of complex adaptive systems (CAS). Prior scholars have demonstrated that CASs such as networks, behavior is instigated by the collective and parallel actions of agents within a system, and not by a single entity.[54] Likewise, in cyber resilience, individuals and

institutions need to be equipped to respond to their changing environments, create mental models for interpretation and analysis of threats, and work together to adapt and thus increase the resilience of their networks and systems.

COMMUNITY-CENTRIC APPROACHES TO CYBER RESILIENCE

A lot has been written about the opacity of cybersecurity information sharing. Attacks are often not reported either by individuals or organizations. Often, the reports of these incidents are intentionally vague or opaque about the attack vector.[55,56] While certain information is deemed unallowable to share based on national security or governance interests, other cybersecurity-related information that can be shared widely stands to benefit cyber resilience strategies in cross-sector and in-sector organizations.[57-59] Additional approaches for promoting cyber resilience through responsible use of the cyber commons involve composable governance[60] and equifinality.[61] Composable governance refers to customizable frameworks of governance for specific domains of application, whereas equifinality offers stakeholders the ability to adopt solution bundles that fit their needs for ensuring cyber resilience. Table 1 provides a summary of various mechanisms discussed in this paper for achieving cyber resilience. These mechanisms are broadly classified into three categories: technical, governance, and social. It must be noted that these categories are not exclusive: overlap among categories and the encompassing mechanisms is key to enabling stakeholders to achieve cyber resilience.

Community-centric mechanism for cyber resilience	Description
Technical	- Support encryption - Share vulnerabilities, threat information, and countermeasures - Enterprise risk management
Governance	- Local governance of digital commons - Composable governance60 - Equifinality
Social	- Holistic cybersecurity - Social learning - Cultivating a culture of cybersecurity (cybersecurity mindfulness, human firewalls, communities of trust)

Table 1. Community-centric approaches to cyber resilience

One example of information sharing for achieving cyber resilience is in the Common Vulnerabilities and Exposures (CVE) dictionary.[62] Developed with support from The MITRE Corporation and the Department of Homeland Security (DHS), the Common Vulnerabilities and Exposures (CVE) catalog has come to exemplify a community-led effort to share information about flaws, their severity, their scope, and associated countermeasures. Prior to the development of the CVE dictionary, vulnerabilities were classified, scored, and identified differently depending on the vendor, leading to impeded interoperability and information-sharing. The success of the CVE has spurred several derivative initiatives, such as MITRE's Common Weakness Enumeration (CWE) list of software weaknesses[63] and the CVE Change Logs tool[64] to track changes to the CVE list. Widespread support for the CVE has facilitated its de facto status, where cybersecurity vendors make their products compatible with the CVE

dictionary identifiers. Other examples of community initiatives in cybersecurity that are already showing promise are the National Science Foundation's (NSF) Cybersecurity Center of Excellence called Trusted CI,[65] Cybersecurity and Infrastructure Security Agency's (CISA) Connected Communities Initiative,[66] and its Joint Cyber Defense Collaborative (JCDC),[67] which are some of several public-private partnerships being developed for capacity-building efforts against cybercrime.

One particular success story is the 2021 Tokyo Olympic and Paralympic Games.[68] The organizers of the Tokyo Olympics incorporated cybersecurity in the Olympic infrastructure from the start, and utilized an international team of cybersecurity experts. Nippon Telegraph and Telephone (NTT) corporation, which was responsible for providing the network and communications support for the Tokyo Olympics, reported they had thwarted 450M cybersecurity attacks targeted toward the Tokyo Olympics. Training and awareness campaigns for staff prior to the Olympics, advanced communication networks, and specialized cybersecurity infrastructure including personnel support helped the organizer of the 2021 Olympic Games secure the physical and digital infrastructure from an unprecedented number of attacks (the number of attacks was reported to be 2.5 times that of the London Olympics).

DISCUSSION

The discussion in this paper so far has centered on the idea that cybersecurity, woven along with innovative learning, awareness, and adaptability, contributes to the theory and practice of cyber resilience. The community-centered cyber resilience framework proposed in this paper has several implications for cyber security; we highlight a few key implications below.

The Role of Agency

User perceptions and mental models of cybersecurity best practices vary, and this variance impacts the agency of individuals and organizations in creating cyber resilience. Here, agency refers to the abilities of end users regarding both the acquisition of information about cybersecurity best practices as well as their implementation. The acquisition of such information is challenging due to various factors: lack of requisite technical skills, conflicting guidance, lack of clear policies, and an inability to discern the appropriate information pertaining to specific threat scenarios. In contrast to learning or acquiring information from experience (or empirical learning), which is often fraught with challenges, learning from social observation is far more effective. Information about a cyberattack can provide valuable lead time and learning opportunities for others who can avoid becoming the next victim of the attack. Social learning offers agency to each individual and organization in their efforts to secure their digital networks and is critical to developing a culture of cybersecurity that eventually fosters innovations. In fact, social learning that relies heavily on cognitive innovations has been observed as a critical component of cultural transmission in both human and animal societies.[69, 70]

Agency also confers upon agents the valuable attribute of adaptability. Faced with complex environments like the digital commons, individuals and communities have shown that they are predisposed to a willingness to interpret and implement guidelines in ways that make the most sense for their own values.[71] Adaptability, therefore, is key to dealing with the dynamic nature of the digital commons. Conflicting guidance and implementation in cybersecurity were found to be a consequence of value conflicts, where varying values of stakeholders in the digital commons included fairness, economic costs, and prevention of harm to information and physical assets.[72] Further, individual traits and responses to secure behavior in the digital commons differ.[73,74] These examples suggest that countermeasures to address the ToC problem in cybersecurity should consider the role of agency in a community-centered approach. Such an approach relieves individuals and communities of the burden of coming up with global solutions, and addresses the "awareness" aspect of our proposed framework. Instead, local solutions to secure networks can be adopted as the first step to securing regional and then larger, global networks for promoting cyber resilience.

Beyond Regulation

The idea of cultivating resilient communities to reach a tipping point in cybersecurity aligns with Ostrom's solution framework, which calls for mechanisms beyond regulation to combat the ToC problem. While leveraging innovative learning to build resilient communities may take several forms, prior research[75] outlines four factors that can be considered for building resilience. These include embracing change and uncertainty, fostering diversity to reduce risks, optimizing knowledge and problem-solving abilities, and creating opportunities for self-organization while reinforcing the role of local engagement, thus addressing the "adaptability" component of our proposed framework for a community-centered approach to cyber resilience.

Resilience Assurances

Good cybersecurity practices, first and foremost, assure stability. This assurance has value not just when the cybersecurity countermeasures work as intended, but also when they fail and attackers have the upper hand. In the latter case, especially, the assurance of stability carries a greater value since it offers the attribute of resilience to the networks. Modern-day networks are engineered for confidentiality, integrity, and availability (CIA), and threat vectors are constantly seeking to disrupt one or more of these assurances. Incorporating cyber resilience as an additional assurance will have significant impact on the ability of networks to withstand attacks to CIA. However, such an approach for incorporating cyber resilience will only be effective if it is designed with a focus on communities. Communities and networks share many structural traits, and the impact of cyber resilience can be most effective when leveraged with a focus on communities and social cohesiveness.

CONCLUSION

Despite billions of dollars spent each year on cyber-defense initiatives, global cybersecurity cooperation continues to lag, without consolidating efforts to empower users and communities around the world. In this article, we analyzed the role that communities can play in improving the resilience of our online environments through the perspective of the tragedy of cyber commons. Unlike the tragedy of environmental commons where a single finite resource is driven to extinction, the cyber commons that we inhabit are comprised of resources required to create, maintain, and sustain these commons. This article presented a bottom-up approach supported by resilient communities that would be critical to fuel change from within our communities to combat the global problem of the tragedy of the cyber commons. Getting past the tragedy of commons in cybersecurity requires a certain level of collective resilience to sustain our shared digital environments. The proposed framework in this article is intended to serve as a blueprint for cultivating and promoting community-centered cyber resilience, while strengthening global cyber defense capabilities in the process.

NOTES

1. Garrett Hardin, "The tragedy of the commons," *Science* 162, no. 3859 (Dec. 1968) https://doi.org/10.1126/science.162.3859.1243.
2. Lawrence Lessig, "Code and the Commons," *Conference on Media Convergence*, Fordham Law School, New York, NY (1999).
3. William Lehr and Jon Crowcroft, "Managing shared access to a spectrum commons," in *Proceedings of the First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks* (2005), available at https://doi.org/10.1109/dyspan.2005.1542658.
4. Mélanie Dulong de Rosnay and Felix Stalder, "Digital commons," *Internet Policy Review,* Alexander von Humboldt Institute for Internet and Society 9, no. 4 (2020), https://doi.org/10.14763/2020.4.1530.
5. Daniel McFadden, "The tragedy of the commons," *Forbes*, https://www.forbes.com/asap/2001/0910/061_2.html.
6. Nicolas Curien, Emmanuelle Fauchart, Gilnert, G., and Franceau Moreau, "Online consumer communities: Escaping the tragedy of the digital commons, *Internet and Digital Economics* (2007) https://doi.org/10.1017/cbo9780511493201.006.
7. Eytan Adar and Bernardo Huberman, "Free riding on Gnutella," *First Monday* 5, no. 10 (2000), https://doi.org/10.5210/fm.v5i10.792.
8. Seva Gunitsky, "Corrupting the cyber-commons: Social media as a tool of autocratic stability," *Perspectives on Politics* 13, no. 1 (2005), https://doi.org/10.1017/s1537592714003120.
9. Charles Schweik, "Sustainability in open source software commons: lessons learned from an empirical study of Sourceforge projects," *Technology Innovation Management Review* 3, no. 1 (2013), https://doi.org/10.22215/timreview/645.
10. Gian Maria Greco and Luciano Floridi, "The tragedy of the digital commons," *Ethics and Information Technology* 6, no. 2 (2004), https://doi.org/10.1007/s10676-004-2895-2
11. Virgilio Almeida, Fernando Filgueiras, and Francisco Gaetani, "Digital governance and the tragedy of the commons," *IEEE Internet Computing* 24, no. 4 (2020), https://doi.org/10.1109/mic.2020.2979639.
12. Roger Hurwitz, "Depleted trust in the cyber commons," *Strategic Studies Quarterly* 6, no. 3, 20-45 (2012).
13. Mark Raymond, "Puncturing the myth of the Internet as a commons," *Georgetown Journal of International Affairs* (2005), available at https://www.jstor.org/stable/43134322.
14. Dan Hunter, "Cyberspace as Place and the Tragedy of the Digital Anticommons," In *Law and Society Approaches to Cyberspace*, Routledge (2005), https://doi.org/10.4324/9781351154161-3
15. Patricia Longstaff, Nicholas Armstrong, Keli Perrin, Whitney Parker, and Matthew Hidek, "Building resilient communities: A preliminary framework for assessment," *Homeland Security Affairs* 6, no. 3 (2010), https://securitypolicylaw.syr.edu/wp-content/uploads/2012/09/Building-Resilient-Communities.pdf.
16. Elinor Ostrom, "Tragedy of the comons,: in The New Palgrave Dictionary of Economics, S.N. Durlauf and L.E. Blune, Eds, 2nd ed. Palgrave Macmillan (2008), https://dlc.dlib.indiana.edu/dlc/bitstream/handle/10535/5887/tragedy%20of%20the%20commons%20_%20Th...pdf.
17. Donella H. Meadows, T*hinking in systems: A primer,* D.Wright, Ed., White River Junction, Vermont, USA: Chelsea Green Publishing (2008).
18. Jaye Wald, Steven Taylor, Gordon Asmundson, Kerry Jang, and Jennifer Stapleton, "Literature review of concepts," *Psychological Resiliency* 134, (2006).
19. Helen Herrman, Donna E. Stewart, Natalia Diaz-Granados, Elena L. Berger, Beth Jackson, and Tracy Yuen, "What is resilience?," Canadian Journal Of Psychiatry. *Revue canadienne de psychiatrie* 56, no. 5, (2011), https://doi.org/10.1177/070674371105600504.
20. Ron Ross, Victoria Pillitteri, Richard Graubart, Deborah Bodeau, and Rosalie McQuaid, "Developing cyber-resilient systems: A systems security engineering approach," *NIST SP 800-160* vol. 2 (2021), available at https://doi.org/10.6028/NIST.SP.800-160v2r1.
21. Omera Khan, Daniel A.S. Estay, "Supply chain cyber-resilience: Creating an agenda for future research," *Technology Innovation Management Review* 5, no. 4 (2015), http://doi.org/10.22215/timreview/885.
22. Adrian Davis, "Building cyber-resilience into supply chains," *Technology Innovation Management Review* 5, no. 4 (2015), http://doi.org/10.22215/timreview/887.

NOTES

23. Luca Urciuoli, "Cyber-resilience: a strategic approach for supply chain management," *Technology Innovation Management Review* 5, no. 4 (2015), available at https://doi.org//10.22215/timreview/886
24. Mohammad Ghiasi, Moslem Dehghani, Taher Niknam, and Abdollah Kavousi-Fard, "Investigating overall structure of cyber-attacks on smart-grid control systems to improve cyber resilience in power systems," *Network* 1, no. 1 (2020), https://www.academia.edu/42209946/Investigating_Overall_Structure_of_Cyber_Attacks_on_Smart_Grid_Control_Systems_to_Improve_Cyber_Resilience_in_Power_System.
25. Andrea Salvi, Paolo Spagnoletti, and Nadia S. Noori, "Cyber-resilience of critical cyber infrastructures: Integrating digital twins in the electric power ecosystem," *Computers & Security* 112 , no. 102507 (2022), https://doi.org/10.1016/j.cose.2021.102507.
26. Andrew D. Syrmakesis, Cristina Alcaraz, and Nikos D. Hatziargyriou, "Classifying resilience approaches for protecting smart grids against cyber threats," *International Journal of Information Security* 21 (2022), https://doi.org/10.1007/s10207-022-00594-7.
27. Mariana Segovia, Jose Rubio-Hernan, Ana R. Cavalli, and Joaquin Garcia-Alfaro, "Cyber-resilience evaluation of cyber-physical systems," in *2020 IEEE 19th International Symposium on Network Computing and Applications (NCA)* (2020), https://doi.org//10.1109/NCA51143.2020.9306741.
28. Md. Ariful Haque, Gael K. De Teyou, Sachin Shetty, and Bheshaj Krishnappa, "Cyber resilience framework for industrial control systems: concepts, metrics, and insights," in *Proceedings of the IEEE International Conference on Intelligence and Security Informatics* (ISI) (2018), https://doi.org//10.1109/ISI.2018.8587398.
29. Kathleen Tierney, and Michel Bruneau, "Conceptualizing and measuring resilience: A key to disaster loss reduction," *TR News*, no. 250 (2007), https://onlinepubs.trb.org/onlinepubs/trnews/trnews250_p14-17.pdf
30. Benoit Dupont, "The cyber-resilience of financial institutions: significance and applicability," *Journal of Cybersecurity* 5, no. 1 (2019), https://doi.org/10.1093/cybsec/tyz013.
31. Deborah Bodeau, Richard D. Graubart, Rosalie M. McQuaid, and John Woodill, "Cyber resiliency metrics, measures of effectiveness, and scoring," *MITRE Corp* (2018), https://www.mitre.org/sites/default/files/2021-11/prs-18-2579-cyber-resiliency-metrics-measures-of-effectiveness-and-scoring.pdf.
32. NIST, "Framework for improving critical infrastructure cybersecurity version 1.1: NIST Cybersecurity Framework," *NIST* (2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.
33. ISO, "Risk Management – Guidelines," *ISO 3100,* Geneva, Switzerland, 2018.
34. Abraham Althonayan and Alina Andronache, "Resiliency under strategic foresight: The effects of cybersecurity management and enterprise risk management alignment," in *International Conference on Cyber Situational Awareness, Data Analytics and Assessment* (2019), https://doi.org/10.1109/CyberSA.2019.8899445.
35. Samir Jarjoui and Renita Murimi, "A framework for enterprise cybersecurity risk management," in *Advances in Cybersecurity Management*, K. Daimi and C. Peoples, eds., Cham, Switzerland: Springer (2021), 139–161, https://doi.org/10.1007/978-3-030-71381-2_8.
36. Robert Ramirez and Nazli Choucri, "Improving interdisciplinary communication with standardised cyber security terminology: a literature review," *IEEE Access*, vol. 4, 2016, 2216–2243, https://doi.org/10.1109/ACCESS.2016.2544381.
37. Samir Jarjoui, Robert K. Murimi, and Renita Murimi, "Hold My Beer: A case study of how ransomware affected an Australian beverage company," in *Proceedings of the International Conference on Cyber Situational Awareness, Data Analytics and Assessment*, IEEE Xplore (2021), https://doi.org/10.1109/CyberSA52016.2021.9478239.
38. Cisco, "Achieving security resilience," Security Outcomes Report, vol. 3, 2022, https://www.cisco.com/c/en/us/products/security/security-outcomes-report.html.
39. Hans D. Bruijn and Marijn Janssen, "Building cybersecurity awareness: The need for evidence-based framing strategies," *Gov. Inf. Q.* (34), no.1 (2017), https://doi.org/10.1016/j.giq.2017.02.007.
40. Van Nes, Egbert H., Babak MS Arani, Arie Staal, Bregje van der Bolt, Bernardo M. Flores, Sebastian Bathiany, and Marten Scheffer, "What do you mean,'tipping point'?." *Trends in Ecology & Evolution* 31, no. 12 (2016), https://doi.org/10.1016/j.tree.2016.09.011.
41. Malcolm Gladwell, "*The Tipping Point: How Little Things Can Make a Big Difference*," New York: Little, Brown and Company (2000).

NOTES

42. Mahdi Roghanizad, Ellen Choi, Atefeh Mashatan, and Ozgur Turetken, "Mindfulness and cybersecurity behavior: A comparative analysis of rational and intuitive cybersecurity decisions," *AMCIS 2021 Proceedings* 13 (2021), available at https://aisel.aisnet.org/amcis2021/info_security/info_security/13
43. Leah Zhang-Kennedy and Sonia Chiasson, "A systematic review of multimedia tools for cybersecurity awareness and education," *ACM Computing Surveys* (CSUR) 54, no. 12 (2022), https://doi.org/10.1145/3427920.
44. Ben Buchanan, *The cybersecurity dilemma: Hacking, trust, and fear between nations*, Oxford University Press, 2016.
45. Glyn Moody, "Dutch government: encryption good, backdoors bad", Ars Technica, 6 January 2016.
46. Japan NISC, "Outline of the Cybersecurity Strategy" (2021), https://www.nisc.go.jp/eng/index.html.
47. Fran H. Norris, Susan P. Stevens, Betty Pfefferbaum, Karen F. Wyche, and Rose L. Pfefferbaum, "Community resilience as a metaphor, theory, set of capacities, and strategy for disaster readiness," *American Journal of Community Psychology* 41, no. 1-2 (2008), https://doi.org/10.1007/s10464-007-9156-6.
48. Marcus Collier, Zorica Nedović-Budić, Jeroen C. Aerts, Stuart Connop, Dermot Foley, Karen M. Foley, Darryl J. Newport, Siobhan Mcquaid, Alexander Slaev, and Peter H. Verburg, "Transitioning to resilience and sustainability in urban communities." *Cities* 32 (2013), https://doi.org//10.1016/J.CITIES.2013.03.010.
49. Cem Sen, Korhan Arun, and Olkay Okun, "Organizational memory: A qualitative research on a multi-cultural organization," *Kybernetes* (2021), https://doi.org/10.1108/K-08-2021-0783.
50. Robert L. Cross and Andrew Parker, *The Hidden Power Of Social Networks: Understanding How Work Really Gets Done In Organizations*, Harvard Business School Press, Boston (2004), https://www.bu.ac.th/knowledgecenter/epaper/jan_june2010/pdf/Page_155.pdf
51. Martina A. Sasse, Sacha Brostoff, and Dirk Weirich, "Transforming the 'Weakest Link'—a human/computer interaction approach to usable and effective security," *BT Technical Journal* 19 (2001), https://doi.org/10.1023/A:1011902718709.
52. Matthew L. Jensen, Michael Dinger, Ryan T. Wright, and Jason B. Thatcher, "Training to mitigate phishing attacks using mindfulness techniques," *Journal of Management Information Systems* 34, no. 2 (2017), https://doi.org/10.1080/07421222.2017.1334499.
53. Robert Murimi, Sandra Blanke, and Renita Murimi, "A decade of development of mental models in cybersecurity and lessons for the future," in *Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media: Cyber Science* (2022), https://doi.org/10.1007/978-981-19-6414-5_7.
54. Kevin J. Dooley, "A complex adaptive systems model of organization change," *Nonlinear Dynamics, Psychology, and Life Sciences* 1, no. 1 (1997), https://doi.org/10.1023/A:1022375910940.
55. Waleed Alkalabi, Leonie Simpson, and Hasmukh Morarji, "Barriers and incentives to cybersecurity threat information sharing in developing countries: a case study of Saudi Arabia," in *Proceedings of the Australasian Computer Science Week Multiconference* (2021), https://doi.org/10.1145/3437378.3437391.
56. Priscilla Koepke, "Cybersecurity information sharing incentives and barriers," in *Proceedings of the Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity*, MIT Sloan School of Management (2017), https://cams.mit.edu/wp-content/uploads/2017-13.pdf.
57. David Turetsky, Brian Nussbaum, Unal Tatar, "Success stories in cybersecurity information sharing," in Proceedings of the SUNY Albany Cybersecurity Conference (2018), https://www.albany.edu/sscis.
58. Derek Manky, "The hard truth and good news about the fight against cybercrime," Forbes (2021), https://www.forbes.com/sites/fortinet/2021/05/17/the-hard-truth-and-good-news-about-the-fight-against-cybercrime/?sh=3adc2dce19b5.
59. Michael Daniel, "How global information sharing can help stop cybercrime," *Harvard Business Review* (2023), https://hbr.org/2023/06/how-global-information-sharing-can-help-stop-cybercrime.
60. Renita Murimi, "Governance in DAOs: Lessons in Composability from Primate Societies and Modular Software," *MIT Computational Law Report* (2022), available at https://law.mit.edu/pub/governanceindaos
61. Brett J. L. Landry, Renita Murimi, and Greg Bell, "Building equifinality and improvisation into effective cyber operations,". In *Effective Cybersecurity Operations for Enterprise-Wide Systems,* F. Adedoyin and B. Christiansen (Eds.) IGI Global (2023), https://doi.org/10.4018/978-1-6684-9018-1.ch009.
62. Common Vulnerabilities and Exposures, https://cve.mitre.org/.
63. Common Weakness Enumeration (CWE), https://cwe.mitre.org/.

NOTES

64. History of the CVE, https://www.cve.org/About/History.
65. NSF Trusted CI,. https://www.trustedci.org/.
66. CISA Connected Communities, https://www.cisa.gov/topics/risk-management/connected-communities.
67. CISA Joint Cyber Defense Collaborative (JCDC), https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative.
68. Brian Gant, "The Tokyo Olympics are a cybersecurity success story," *Security Magazine* (2021), https://www.security-magazine.com/articles/95880-the-tokyo-olympics-are-a-cybersecurity-success-story.
69. Robin Dunbar, "*Grooming, Gossip, and the Evolution of Language,*" Harvard University Press (1996).
70. Amanda Seed and Michael Tomasello, "Primate cognition," *Topics in cognitive science* 2, no. 3, https://doi.org/10.1111/j.1756-8765.2010.01099.x
71. Ameya Hanamsagar, Simon Woo, Christopher Kanich, and Jelena Mirkovic, "How users choose and reuse passwords," *Information Sciences Institute* (2016).
72. Marcus Christen, Bert Gordijn, Karsten Weber, Ibo Van de Poel, and Emad Yaghmaei, "A review of value-conflicts in cybersecurity: an assessment based on quantitative and qualitative literature analysis," *The ORBIT Journal* 1, no. 1 (2017), https://doi.org/10.29297/orbit.v1i1.28.
73. Michael Fagan and Maifi Khan, "To follow or not to follow: a study of user motivations around cybersecurity advice," *IEEE Internet Computing* 22, no. 5 (2018), https://doi.org/10.1109/mic.2017.3301619.
74. Margaret Gratian, Sruthi Bandi, Michel Cukier, Josiah Dykstra, and Amy Ginther, "Correlating human traits and cyber security behavior intentions," *Computers and Security* 73 (2018), https://doi.org/10.1016/j.cose.2017.11.015.
75. Fikret Berkes, "Understanding uncertainty and reducing vulnerability: lessons from resilience thinking," *Nat Hazards* 41 (2007) available at https://doi.org/10.1007/s11069-006-9036-7.

THE CYBER DEFENSE REVIEW

CONTINUE THE CONVERSATION ONLINE

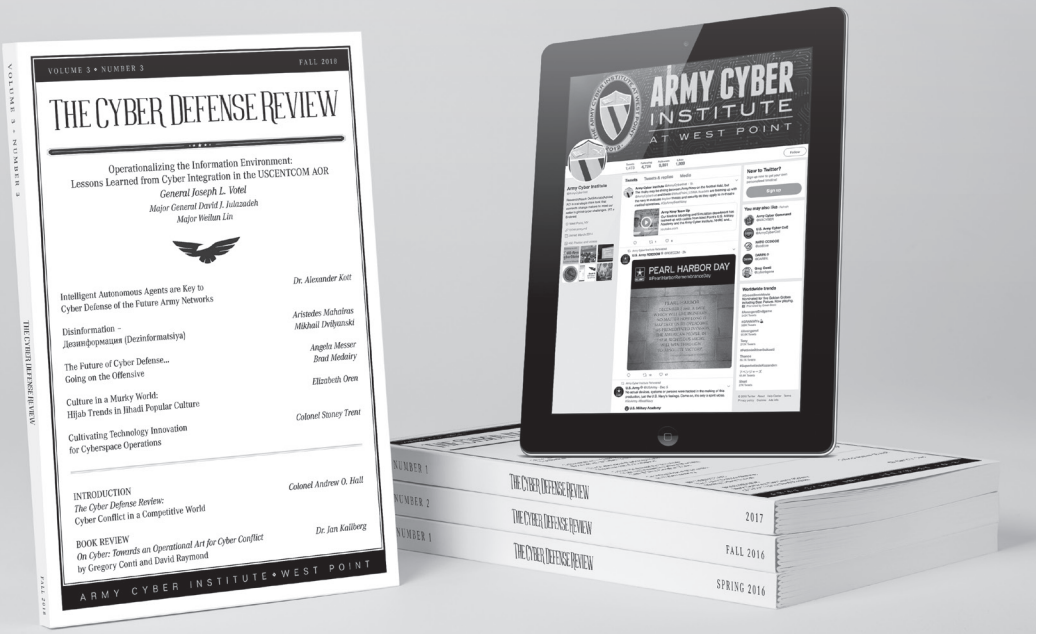
CyberDefenseReview.Army.mil

AND THROUGH SOCIAL MEDIA

Facebook @ArmyCyberInstitute

LinkedIn @LinkedInGroup

Twitter @ArmyCyberInst
@CyberDefReview



ARMY CYBER INSTITUTE ◆ WEST POINT 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.