Beyond Zero Trust: Reclaiming Blue Cyberspace with AI*

Scott A. Weed
United States Air Force

Abstract—**Given the rapidly evolving cyberspace threat landscape and current US military cyber capabilities, how can the DOD employ emergent technology to regain its competitive advantage? Industry best practices are necessary but insufficient to counter the threats undermining national security. They cede friendly and neutral cyberspace to adversaries and cannot serve as the desired end state. This article offers a literature review of evolving approaches, analyzes gaps within the DOD cyber strategy, and discusses one emergent capability to fill those gaps. This research contends that the military must field an AI-enabled domain-sensing capability to provide new strategic outcomes. This capability, only possible through modern network and computing resources, offers Internet-scale, machine-speed Deep Learning to defend DOD networks. The military could then observe, pursue, and counter threats and realize a more active defense posture to defend the nation against converging non-state and state malign cyber actors.**

I. Motivation

"*The status quo is a slow surrender of American power and responsibility.*" - US Cyberspace Solarium Commission [1]

The rapidly changing strategic landscape of cyber actors, capabilities, and threats becomes increasingly perplexing and entangled with Internet users measured in the billions, and networked devices estimated at three times the number of humans [2]. Cyberspace has already changed how people live, interact, and think, but its future holds far more potential for change. Its volatile trajectory has already begun to alter the character of warfare in existentially challenging ways. This becomes more evident as algorithms increasingly supplant human decision making. Additionally, state and non-state actors have effectively leveraged cyberspace to undermine American interests and way of life for two decades [1]. The increasingly shared realization of substantial national security risk has created a de facto consensus among national leaders; what John Kingdon coined a "focusing event" [3]. As a result, a window of opportunity emerges for concerted policy changes and strategic realignments necessary for the US military to adapt and regain its competitive advantage in cyberspace.

II. Impetus for Change

After decades of accumulated risk from the current approach, a rapidly growing body of national policy, strategic guidance, and departmental efforts seeks to drive modernization and innovation in cyber. Various US Presidents have issued executive orders and national security memoranda on improving the Federal government's cybersecurity, each recognizing the urgent need to modernize and secure Federal information technology (IT). This collective guidance has set aggressive timelines for Federal adoption of leading industry principles ranging from the use of least privilege to segmentation, secure configuration, supply chain protection, cloud solutions, multifactor authentication, and zero trust (ZT) architectures [4]. In addition, several US Congress National Defense Authorization Acts require more decisive Federal action on Artificial Intelligence (AI), including a White House National AI Initiative Office, a formalized Department of Defense (DOD) AI organizational structure, an expanded role for the National Institute of Standards and Technology (NIST), and other sweeping mandates [5]–[8].

The military's cyber activities surrounding its warfighting mission have advanced considerably in recent years. As a result, the DOD has multiple evolving strategies to integrate national policy and guidance that span cyber, AI, digital modernization, and data disciplines. These strategies highlight the need to employ emergent technology to maintain or improve the nation's competitive advantage and support the joint force across an increasingly contested cyber domain [9]–[12].

Two noteworthy aspects of the DOD Cyber Strategy articulate the military's most pressing strategic needs. First, the department "will defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict." Second, the department will aggressively seek machine-speed and large-scale analytical capabilities to defend against malign cyber activity [9]. Defending forward entails an ability to observe, pursue, and counter adversaries beyond friendly cyberspace to identify their tactics, disrupt their activities, and potentially impose costs [1], [13]. It represents a marked shift in strategic thinking after decades of failed deterrence and a newfound emphasis on persistent global engagement in cyberspace. When coupled with the new DOD strategy of integrated deterrence, where military capability underpins foreign policy, the power of defending forward and active engagement become more essential to national security [13]–[15]. However, it is essential to note that such a strategy of persistent cyber engagement draws some criticism as a contentious approach that risks escalation. Nevertheless, the concept is starting to engender broader international discussion [16]. While the strategy was developed

*Invited position paper. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Department of the Air Force or the U.S. Government.

in response to more provocative adversarial state behavior, it still encounters tension with the nascent state cyberspace norms that US diplomats shaped through the United Nations (UN) [17], [18]. Notably, the UN and North Atlantic Treaty Organization increasingly discuss the role of self-defense and collective accountability in cyberspace when confronted with the realities of geopolitics and the modern threat landscape [17]–[19]. Beyond these aspirational strategies, the military requires tangible building blocks to defend itself in the cyber domain.

The military, much like industry, relies upon interlocking suites of tools and software to protect their networks from intrusion and compromise. These have evolved as rule-based detection and alerting capabilities, for example tools like Security Information and Event Management (SIEM). These depend on real-time intelligence and often leverage the MITRE ATT&CK framework to provide context [20], [21]. These signature-based capabilities and detected indicators of compromise (IOCs) are akin to a black box recorder, which provides lagging forensics after a compromise occurs [22]. More modern approaches include User and Entity Behavioral Analytics (UEBA), Security Orchestration, Automation, and Response (SOAR), and the concept of Zero Trust (ZT). UEBA overlays user and network device activity against contextual details over time to establish individualized behavior baselines, looking for deviations from those baselines to detect insider threats [20], [22]. SOAR tools heavily leverage automation to distill vast quantities of data in order to transform information overload into meaningful analysis, incident response, and reporting [23]. In contrast, ZT represents less of a tool and more of a design approach. ZT strives to eliminate Internet design flaws inherent in the implicit trust that is often granted to network traffic, both broadly across the Internet and narrowly within a given network perimeter once a user has authenticated. Both of these design flaws are pervasive, and both have been exploited for decades.

ZT consists of three core approaches: presuming a breach has occurred and limiting internal movement, continuous granular authentication and authorization, and granting the least privileged access. It is data-centric and role-driven rather than perimeter-based, and strives to protect critical assets, data, and operations even when the environment has been compromised. A shift to Zero Trust architecture requires a complete network redesign and integration across endpoints, identities, applications, network devices, infrastructure, and data [24]–[26].

Overall, the technology enabling DOD's cybersecurity is a combination of cyber hygiene, traditional signature-based tools like SIEM, and AI-enabled UEBA, SOAR, and ZT to meet the department's cyberspace objectives [9]. The department also primarily employs a defense-in-depth approach, with enterprise SIEM and UEBA functionality fed by sensors and feeds across the DOD Information Network (DODIN) [27]. These narrow AI-enabled tools help provide greater insight across the environment and reduce blind spots between historically stove-piped networks across the DODIN [28]. Implementing ZT principles will provide a significant advantage for the department over the status quo, offering better prevention of lateral, escalatory, or persistent adversarial access [26]. It will also increasingly support hybrid or distributed remote access for a department moving towards commercially-hosted cloud services with a blurred demarcation between military and commercial networks [29]. Combined with network segmentation, ZT should also isolate risk domains between a ZT-capable business IT environment and ZT-incapable Operational Technology (OT) supporting critical infrastructure. This need for isolation becomes more pronounced as actors increasingly target Internet-of-Things and OT cyber terrain that sit beyond traditional business IT [25]. However, Federal and DOD cyber strategies still have significant blind spots and challenges in keeping pace with evolving threats.

While the department needs to further SIEM, SOAR, ZT, and UEBA capabilities, these remain an insufficient end state for protecting the military's cyberspace. If these industry approaches were sufficient, the past several years of increasingly impactful cyber events across some of the most capable global technology companies would not have occurred [30]–[33]. SIEM or UEBA, when protecting an enterprise from external or internal threats, may fail to detect knowledgeable users who understand how the tools develop alerts and baselines [34]. Moreover, ZT will be a challenging, resource-intensive, and unending endeavor. It is less about buying a turnkey solution and more about bringing on a methodology that must pervade acquisition, design, fielding, operations, and sustainment. Continual risks remain from misconfiguration, human fallibility, exempted users, and diminished budgets, which would undermine its true benefit. The National Security Agency acknowledged that a constant posture of a presumed breach might fatigue defenders [26]. Additionally, the department will experience challenges realizing ZT at scale across its diverse networks, often segregated into core IT and non-core mission enclaves via distinct funding and authorities. While ZT should ease the distinction between on-premises and remote work, access determinations will become increasingly complex [35].

One aspect not emphasized explicitly in recent guidance is the burgeoning need for the department to reduce technical debt and configuration drift across the DODIN. The department struggles with purging end-of-life and end-of-support legacy IT from its environment, often due to programmatic, proprietary vendor solutions, or niche mission requirements that hinder technical currency [25], [36], [37]. These represent sustainment challenges for any large enterprise but are underlying considerations that influence the risk of compromise and, in turn, strategic risk. Modernization investment across the DODIN, historically a challenge, becomes ever more critical to reducing the technical debt and variance that hampers ZT realization. Department leadership recognizes these challenges as well.

The Principal Deputy DOD Chief Information Officer (CIO) remarked that even ZT could not provide the full defensive capabilities required to protect the DODIN from emerging threats. The CIO noted that greater AI capabilities than those currently employed are essential to the department's future [38]. Moreover, adversaries anticipate the department moving toward ZT and actively design algorithms and attacks to counter it, with zero-day vulnerabilities remaining a threat. Cryptocurrency and blockchain-enabled escrow have monetized and intensified an anonymous and specialized hack-as-a-Service criminal ecosystem [21], [25], [39], [40]. Some estimates—solely from publicly available data—suggest several private actors may generate illicit revenue streams that "rival the budgets of nation-state [cyber] attack organizations" These resources then fuel development and deployment of vastly more sophisticated threats against leading best practices. This is evident in the accelerating use of consent phishing, machine learning (ML), automation, and an unparalleled ability to scale [25]. Given the aforementioned holistic security model and its gaps, the question remains: how might the military use emergent ML technology to regain its edge?

Ultimately, the existing paradigm lacks the DODIN-scale real-time detection and prediction capabilities required to observe and control the cyber domain effectively. It fails to achieve the domain sensing and awareness necessary to observe friendly cyberspace fully, especially for systems with interfaces beyond the DODIN, and it lacks machine-speed means to peer into adversarial cyberspace. Military cyber defenders have the riskier and unenviable task of close-quarters defense without better detection and response capabilities that could provide a degree of standoff. As a result, the military and broader Federal government continue to suffer from impactful cyber threats, including advanced persistent threats (APTs), ML-enabled malware, ransomware, botnets, software supply-chain attacks, phishing, insider threats, and distributed denial-of-service (DDoS) attacks. Recent years highlight that existing measures and tools may address legacy threats but fail to counter accelerating threat sophistication, especially with emergent ML techniques. Therefore, the department must find a means to advance its approach beyond this well-known playbook and look to emergent breakthrough ML-enabled capabilities.

III. The Rise of Machine Learning

AI and Machine Learning (ML) are evermore indispensable to American national security and military power. They increasingly amplify national capabilities and accelerate military decision speed while exposing the potential weaknesses of an adversary. The National Security Commission on AI report noted that "humans cannot be everywhere at once, but software can." However, as noted by the former CEO of Google and the former Deputy Secretary of Defense, "Americans have not yet grappled with just how profoundly the [AI] revolution will impact our economy, national security, and welfare" [41].

There are a growing variety of Adversarial ML (AML) applications, which NIST defines as "systems that develop methods to manipulate a target system and generate a specific outcome, often to defeat security or provide counter-algorithmic capabilities" [42]. Real-world vignettes include injecting image distortions that obscure a stop sign for sensors on a self-driving car, fooling a medical algorithm into misdiagnosing cancer, or creating dynamic malware capable of evading enterprise cybersecurity detection and tools [43]. To date, these examples often come about via researchers who manipulate variables under experimental conditions that may not exist in the wild. Yet the threat is not far off – this research is no less than a proof of concept that can be further advanced and developed [44]. States like China and Russia, and non-state actors aggressively invest in AI/ML with an aim for military, security, and asymmetric applications to contest the American status quo [1]. As a result, an algorithmic digital arms race has emerged in the quest for novel ways to defeat ML systems. The ability to guarantee resilience in the face of AML, especially with the advent of generative adversarial networks, will remain an area of intense research in the near term [20]. These once-theoretical challenges to friendly systems have ultimately become real.

While AI has developed significantly since Alan Turing's 1950 Imitation Game experiment, advanced computation and mathematics of the past decade unlocked a new age of Deep Learning (DL) capabilities under the broader AI umbrella [45]. DL goes beyond ML to leverage multilayered neural networks –modeled after the human brain – to derive powerful new learning and insight. A 2016 Defense Advanced Research Projects Agency (DARPA) Cyber Grand Challenge, the first all-machine hackathon, saw self-healing supercomputers patching their vulnerabilities at machine speed while compromising competitors [46]. AlphaZero and MuZero algorithms bested all human competitors in chess, Shogi, Go, Bridge, and classic video games. Additionally, an 'Artuμ' agent successfully controlled inflight U-2 mission systems for the first time, while a DARPA-sponsored agent bested a top United States Air Force (USAF) fighter pilot in simulated air-to-air combat [47]–[49]. Overall, algorithms will become a center of gravity for national power as they increasingly underpin and coalesce the processes that bind society and national instruments of power. Hence, AI/ML offers untold benefits to those who can harness it, including those charged with fighting and winning their nation's wars.

The Chief Digital and Artificial Intelligence Office (CDAO) is the primary execution arm for the DOD AI strategy and the primary proponent for aiding units in generating AI-ready data for operational applications. The DOD already collects vast amounts of logs, yet agencies across the department must standardize, curate, and share their data to make them exploitable and relevant [50]. Industry estimates are that preparing and curating data constitutes nearly 80% of the effort in adopting emergent AI/ML technology [51]. In addition, the acquisition community must ensure statutory requirements emphasize AI-ready data specifications as part of procurement and design phases, including data rights for future development. Finally, the commercial sector already demonstrates paths for pivoting to AI-ready data, and DOD units must follow the CDAO lead. While AI is not the solution to every problem, one successful example of this pathway is the joint USAF and MIT AI

Accelerator efforts that develop novel AI applications across combat and support mission areas. This AI-focused teaming has shifted the USAF AI ecosystem in record time towards more discrete and relevant problems for warfighters [52]. These achievements set the foundation for the introduction of a powerful DL capability with a strong potential to provide the DOD's missing cyber domain sensing and awareness.

IV. Deep Cyber Sensing

The DOD needs to integrate a novel cyber sensing capability into the DODIN as a critical element of its broader strategy to adapt to this new era. The essence of this concept is not new. A campaign for collective strategic resilience against cyber threats has been developing under several methodologies over the last four years, from the Cyber Operational Resilience Alliance (CORA) to Signals Synthesis [53]. Likewise, Observe-Pursue-Counter and Zero Botnets frameworks provide policy and technical principles behind practical options to respond to such threats [54]. Finally, the Cyber Phenomenology Exploitation and Reasoning (CyPhER) concept represents a feasible architecture to realize forward defense in cyberspace, repulsing adversaries closer to their point of origin [55]. Of note, the USAF is exploring this research space for implementation into the Air Force Information Network [56].

The author proposes that these aforementioned influences, gathered and synthesized under the notional nomenclature of Deep Cyber Sensing (DeCyS), form a novel concept for network reconnaissance, which once developed and implemented, could detect anomalous activity at a speed and scale beyond industry. In comparison to industry-leading Microsoft, leveraging ten thousand internal analysts and fifteen thousand external security partners to assess trillion signals daily, DeCyS would allow a much smaller DOD team to realize a similar scale using hybrid open-source technology [57]–[63]. Such a capability would represent a strategic inflection point for DOD cybersecurity and cyber defense, across DODIN Operations and Defensive Cyberspace Operations mission sets [64]. It could offer unparalleled discernment of threats emanating from the broader Internet beyond defended friendly cyberspace [55].

DeCyS offers three primary benefits to the DOD: machine-speed network observation with Internet-scale traffic volume, privacy-preserving analytics required by some allies and defense industrial partners, and detection of threats and potential identification of previously unknown adversarial infrastructure. DeCyS would allow the DOD to integrate research developments with hyper-sparse matrix mathematics, supercomputing, and novel processing to deliver previously unachievable storage and computational speed toward its strategic needs [54], [55], [59]–[63]. The military would gain unparalleled insight across the DODIN through the integration of this innovation at its nexus with the Internet, which it could export to cybersecurity systems across the military's cyberspace components and the Defense Industrial Base. Additionally, DeCyS offers the DOD privacy-aware and responsible cyber domain sensing and awareness with unique visibility beyond its defended perimeter at the speed needed for today's adversaries [65].

First, and most importantly, DeCyS achieves several orders-of-magnitude improvements in processing and storage over extant network observation methods that make Internet-scale analysis tenable [54]. The method focuses on the source and destination Internet Protocol addresses already present in the headers of Internet traffic and stores these data in hyper-sparse matrices, capitalizing on minimal data values to reduce storage and computation [54]. Linear algebra associated with matrices and developments in supercomputing and scalable processing provide two powerful results: more efficient big data analytics and data anonymization for privacy purposes. Furthermore, this approach offers a mathematically feasible solution for observing and assessing all the relationships among internal and external network addresses [55].

Next, traffic anonymization and avoidance of deep-packet inspection preserve the privacy associated with wide-aperture traffic ingestion unless explicitly approved for deeper anomaly analysis. DeCyS can exploit these filtered data streams to create traffic baselines, which analysts can selectively analyze for desired specificity based on the perceived threat, thus reducing data requirements by an order of magnitude [55]. In turn, DeCyS data would have relevance more broadly across Federal cybersecurity and intelligence organizations to enrich the interagency posture. DeCyS upholds individual privacy, which is core to US national and cultural values and liberal civil societies worldwide [54].

Third, DeCyS internally relies on unsupervised Deep Learning (DL) to accurately baseline both recurring and novel network traffic and thus identify anomalous behavior through nonlinear relationships of internal and external addresses [54]. The proper vantage point, such as the department's demarcation with the broader Internet, would allow the clustering of enterprise traffic flows that could identify command and control traffic of a supply-chain attack ahead of traditional detection methods [54]. The key to signature-less detection is the employment of DL against these hyper-sparse matrices to develop a highly accurate traffic baseline that will enable reliable identification of subsequent deviations [54]. The architecture relies upon the power-law probability distribution of network sources and destinations to train highly accurate baseline traffic models from anonymized matrices [54]. The capability capitalizes on wide-aperture traffic ingestion where volume and variety are richest. It can then detect the flow changes from an anomaly given its divergence from the baseline and assess known and unknown threats by activity [66]. This shifts system defense away from a reliance upon Indicators of Compromise or Attack (IOC/IOA) toward actual Indicators of Behavior (IOB) associated with target "complexes" comprising thousands of devices [21]. These IOBs would better characterize malicious reconnaissance or command and control traffic that otherwise might evade DOD detection below the noise floor and could thus serve as precursors to other malign activity.

Finally, DeCyS highlights anomalies independent of the attack vector or modality, whether botnet, malware, or actor. DeCyS would declutter the noise that Advanced Persistent Threats (APT) hide behind, and allow defenders the ability to detect their subtle activity despite masking by a Distributed Denial of Service (DDoS) or overt obfuscation attempt, and better discern cyber threat actors practicing “live off the land” tactics [22]. DeCyS, coupled with analysis from darkspace sensors, could also observe practice or test fire of adversarial activity into darkspace ahead of intended operational employment. Most notably, DeCyS clusters network addresses longitudinally over time to highlight convergence and discover previously unknown adversary infrastructure, spotlighting and deanonymizing sources over the horizon beyond friendly cyberspace. Thus, such a capability could meet national calls for action.

V. The Missing Keystone

All layers of the holistic cybersecurity model discussed here remain essential for the DOD, yet the military needs to field the Internet-scale, machine-speed, DL-empowered DeCyS capability to mitigate its strategic blind spots and risks in the existing domain approach. This key element promises to provide the domain sensing and awareness foundational to regaining the military’s competitive advantage in cyberspace. From a historical perspective, Great Britain faced a similar challenge in the late 1930s. The looming existential threat of the German Luftwaffe galvanized British political will and technical innovation to fashion the world’s first integrated air defense system, known as Chain Home. These meshed coastal radar stations provided the critical early warning necessary for the Royal Air Force to detect, respond, and defend against the Luftwaffe during the Battle of Britain [67]–[69]. Without this, German fighters and bombers would have continued to dominate Britain and denied the ability to mass American forces.

This ability to sense the domain, secure friendly airspace, and defend forward from its perimeter kept Great Britain viable in the war effort. Moreover, it preserved the Allied foothold in Western Europe, eventually resulting in the defeat of Nazi Germany. Likewise, during the Cold War, the United States developed a scaled-up Chain Home system, the Semi-Automatic Ground Environment (SAGE), to protect North America against the Soviet nuclear bomber threat [70]. Similar requirements to sense and gain awareness of the operating domain are also priority efforts in modern national maritime and space strategies, and the recurrent domain-agnostic dynamics between attack and defense carry well into cyberspace [64], [71], [72].

DeCyS could spotlight behavior independent of the vector, whether botnet, malware, or APT. Such a DL-powered capability would augment existing cybersecurity tools by correlating real-time insights within friendly space while discerning origins and unknown infrastructure over the horizon. DeCyS efficacy depends upon wide-aperture data ingestion from a well-positioned observation point [54]. The appropriate vantage point would allow DeCyS to detect, cluster, and correlate a supply chain compromise during its initial stages rather than months after infection [40].

The DOD Unified Platform (UP), as the emergent centerpiece for the broad military network architecture, provides the most impactful and enduring point to position DeCyS between the DODIN and the commercial Internet. The USAF originally created the UP as a cloud-based software development factory. US Cyber Command (USCYBERCOM) and its Joint Forces Headquarters-DODIN (JFHQ-DODIN) later adopted the UP as a big data platform to integrate sensors, operators, and capabilities for full-spectrum cyber operations [73], [74]. The department already feeds myriad sensors and taps into the UP, with continued investment and enhancement forecast as its primary big data platform. Furthermore, the DOD forecasts UP to eventually span all security classification enclaves, include connectivity with DHS, and grow to serve as the framework for the emergent Joint Cyber Warfighting Architecture concept. Additionally, the JFHQ-DODIN Commander executes Directive Authority for Cyberspace Operations on behalf of USCYBERCOM, with explicit authority to conduct department-wide defensive and cybersecurity activities [64]. In this capacity, JFHQ-DODIN could internally act on DeCyS-tipped indicators of behavior (IOBs) while exporting indications and signatures of malicious activity to inform legacy cyber activities across the broader Federal government. Early detection would allow defenders to modify access to the friendly cyber landscape to observe, delay, confound, or counter intruders [55]. The UP represents the optimal intersection of enterprise vantage and technology to integrate DeCyS to generate new strategic and operational options for decision-makers. However, the implications of such a capability go well beyond strictly technical benefits.

The primary benefit of a DeCyS capability is a next-generation ability for the military to make the invisible visible and provide defenders with actionable insight to counter threats before they reach friendly cyber terrain [55]. Additionally, the correlation and insight provided by DeCyS beyond the defended perimeter could provide new options for decision-makers to hold previously unknown adversarial infrastructure at risk, which is often the most costly and time-consuming real-world aspect of their campaign [25]. A precise and proportional response could then blind, degrade, or deter adversaries, forcing them to reposition, rebuild, and recommit.

DeCyS creates strategic outcomes broader than the cyberspace domain. It fulfills the intent of presidential mandates and departmental strategies to create the type of decision advantage pursued across the strategic military art. The military would gain more effective options through cyber or other domains from this new awareness. This is the essence of Sun Tzu’s The Art of War and Colonel John Boyd’s Observe-Orient-Decide-Act (OODA) Loop [75], [76]. Additionally, the DOD’s Homeland Defense (HD) responsibilities rely on active defenses. Early detection is key to engaging threats before they reach the homeland, suggesting that HD begins with multi-domain awareness [77]. Its innovation and speed also bring the military closer to the tenets underlying Joint All-Domain Operations and DARPA’s Mosaic Warfare, seeking to seize friendly opportunities rapidly while creating compounding dilemmas for adversaries in real-time [78], [79].

In an era where actors continuously engage the nation below the threshold of armed conflict, domain awareness is imperative to credible deterrence and response options to modern threats [55]. The Secretary of Defense has remarked that AI will enable faster, more rigorous decisions that ensure adversaries “know that we can respond not just in [one domain] but in many others” [15]. The primary threat facing American national interests emanates from states, and this versatility to respond across domains creates a more credible deterrent and de-escalation effect while returning the initiative to the US military [25]. Ultimately, this effort aligns departmental actions with national political objectives to shape the strategic environment in favor of the United States [80].

VI. Conclusion

The US military, and broader Federal government, have an opportunity with DeCyS to regain the competitive edge in the cyber domain. Current industry practices are necessary but insufficient to counter current and future threats to our national security, especially given decades of technical debt and configuration drift across the DODIN [13]. The current DOD cybersecurity paradigm leaves gaps that cede friendly cyberspace to adversaries and cannot serve as the end state. The DOD should continue pursuing its current strategy while aggressively fielding the DL-enabled domain sensing and awareness DeCyS capability. DeCyS presents the DOD with otherwise unreachable advancements in speed and scale, adversarial insight, and modernization. Further research should gauge implementation costs, develop higher fidelity heuristics on threat actors, and determine possible applicability beyond the DODIN, given the privately owned nature of cyberspace [55]. Ensuring DOD activities integrate effectively across the whole-of-government, state, local, tribal, and private sectors is essential to realizing whole-of-nation unity of effort. These steps are foundational to leveling the strategic playing field with our adversaries via credible deterrence and response, and should deterrence fail, to win the next war.

References

[1] C. S. Commission *et al.*, “Cyberspace solarium commission final report,” 2020.

[2] Cisco, “Cisco annual internet report (2018-2023),” 2023.

[3] J. W. Kingdon and E. Stano, *Agendas, alternatives, and public policies*, vol. 45. Little, Brown Boston, 1984.

[4] The White House, “Executive order on improving the nation’s cybersecurity,” 2021.

[5] Stanford Human-Centered Artificial Intelligence, “Summary of ai provisions from the national defense authorization act 2021,” 2021.

[6] The White House, “A strategic intent statement for the office of the national cyber director,” 2021.

[7] United States Congress, “H.r.3359 - cybersecurity and infrastructure security agency act of 2018,” 2018.

[8] United States Department of State, “Secretary antony j. blinken on the modernization of american diplomacy,” 2021.

[9] United States Department of Defense, “Dod cyber strategy 2018,” 2018.

[10] United States Department of Defense, “Summary of the 2018 dod artificial intelligence strategy,” 2018.

[11] United States Department of Defense, “Dod digital modernization strategy: Dod information resource management strategic plan fy19-23,” 2019.

[12] United States Department of Defense, “Dod data strategy,” 2020.

[13] C. C. Demchak and F. Spidalieri, “Tallying unlearned lessons from the first cybered conflict decade, 2010-2020,” *The Cyber Defense Review*, vol. 7, no. 1, pp. 15–20, 2022.

[14] E. O. Goldman, “Paradigm change requires persistence-a difficult lesson to learn,” *The Cyber Defense Review*, vol. 7, no. 1, pp. 113–120, 2022.

[15] Lloyd Austin III, “The pentagon must prepare for a much bigger theater of war,” 2021.

[16] M. Smeets, “Cyber command’s strategy risks friction with allies,” *Lawfare (blog)*, vol. 28, 2019.

[17] United Nations, “United nations repertory of practice of united nations organs,” 2021.

[18] United Nations, “Open-ended working group on information and technology,” 2021.

[19] North Atlantic Treaty Organization, “Cyber defence,” 2021.

[20] I. J. Faber, *Cyber Risk Management AI-Generated Warnings of Threats*. Stanford University, 2019.

[21] B. E. Strom, A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington, and C. B. Thomas, “Mitre att&ck: Design and philosophy,” in *Technical report*, The MITRE Corporation, 2018.

[22] CrowdStrike, “Ioa vs. ioc,” 2021.

[23] Palo Alto Networks, “What is soar?,” 2021.

[24] Microsoft, “Evolving zero trust: How real-world deployments and attacks are shaping the future of zero trust strategies,” 2021.

[25] Microsoft, “Digital defense report,” 2021.

[26] National Security Agency (NSA), “Embracing a zero trust security model,” 2021.

[27] Defense Information Systems Agency (DISA) Symposium, “Jfhq-dodin: Fight the dodin,” 2019.

[28] United States Department of Defense, “Department of defense information technology enterprise strategy and roadmap,” 2021.

[29] United States Air Force (USAF) Enterprise IT-as-a-Service (EITaaS) Integrated Program Office, “Usaf eitaas overview,” 2021.

[30] Mandiant, “Sunburst & unc2452: Solarwinds breach resource center,” 2021.

[31] Volexity, “Operation exchange marauder: Active exploitation of multiple zero-day microsoft exchange vulnerabilities,” 2021.

[32] United States Cybersecurity & Infrastructure Security Agency (CISA), “Alert (aa21-110a) exploitation of pulse connect secure vulnerabilities,” 2021.

[33] United States Cybersecurity & Infrastructure Security Agency (CISA), “Cisa, fbi, nsa and international partners issue advisory to mitigate apache log4j vulnerabilities,” 2021.

[34] M. A. Salitin and A. H. Zolait, “The role of user entity behavior analytics to detect network attacks in real time,” in *2018 international conference on innovation and intelligence for informatics, computing, and technologies (3ICT)*, pp. 1–5, IEEE, 2018.

[35] United States National Institute of Standards and Technology (NIST), “Special publication 800-207: Zero trust architecture,” 2020.

[36] United States Government Accountability Office (GAO), “Information technology: Agencies need to develop and implement modernization plans for critical legacy systems,” 2021.

[37] United States DOD Defense Innovation Board (DIB), “Ten commandments of software,” 2018.

[38] Kelly Fletcher, “Dod official discusses cybersecurity priorities at billington summit,” 2021.

[39] UN Office on Drugs and Crime, “Unodc report: darknet cybercrime is on the rise in southeast asia,” 2021.

[40] CrowdStrike, “Global threat report,” 2021.

[41] NSCAI, “National security commission on artificial intelligence (nscai) - final report,” 2021.

[42] United States National Institute of Standards and Technology (NIST), “Artificial intelligence: Adversarial machine learning,” 2024.

[43] Hyrum Anderson, “Evading next-gen AV using A.I.,” 2017.

[44] E. Alhajjar, P. Maxwell, and N. Bastian, “Adversarial machine learning in network intrusion detection systems,” *Expert Systems with Applications*, vol. 186, p. 115782, 2021.

[45] A. M. Turing, “Mind,” *Mind*, vol. 59, no. 236, pp. 433–460, 1950.

[46] United States Defense Advanced Research Projects Agency (DARPA), “Cyber grand challenge,” 2016.

[47] DeepMind, “Alphago history,” 2021.

[48] United States Defense Advanced Research Projects Agency (DARPA), “AlphaDogfight Trials Foreshadow Future of Human-Machine Symbiosis,” 2016.

[49] DefenseNews, "Artoo, take the wheel: U-2 spy plane flies for the first time with an AI co-pilot," 2020.

[50] United States Department of Defense, "Chief digital and artificial intelligence office (cdao)," 2024.

[51] Gil Press, "Cleaning big data: Most time-consuming, least enjoyable data science task, survey says," 2016.

[52] United States Air Force (USAF)-Massachusetts Institute of Technology (MIT) Artificial Intelligence (AI) Accelerator, "Ai accelerator challenges," 2014.

[53] C. C. Demchak, "China: Determined to dominate cyberspace and ai," *Bulletin of the Atomic Scientists*, vol. 75, no. 3, pp. 99–104, 2019.

[54] J. Kepner, J. Bernays, S. Buckley, K. Cho, C. Conrad, L. Daigle, K. Erhardt, V. Gadepally, B. Greene, M. Jones, R. Knake, B. Maggs, P. Michaleas, C. Meiners, A. Morris, A. Pentland, S. Pisharody, S. Powazek, A. Prout, P. Reiner, K. Suzuki, K. Takhashi, T. Tauber, L. Walker, and D. Stetson, "Zero botnets: An observe-pursue-counter approach." Belfer Center Reports, 6 2021.

[55] S. Pisharody, J. Bernays, V. Gadepally, M. Jones, J. Kepner, C. Meiners, P. Michaleas, A. Tse, and D. Stetson, "Realizing forward defense in the cyber domain," in *2021 IEEE High Performance Extreme Computing Conference (HPEC)*, pp. 1–7, IEEE, 2021.

[56] United States Air Force (USAF)-Massachusetts Institute of Technology (MIT) Artificial Intelligence (AI) Accelerator, "Ai accelerator research," 2014.

[57] Microsoft, "Digital defense report," 2023.

[58] J. Kepner, M. Jones, D. Andersen, A. Buluç, C. Byun, K. Claffy, T. Davis, W. Arcand, J. Bernays, D. Bestor, W. Bergeron, V. Gadepally, M. Houle, M. Hubbell, A. Klein, C. Meiners, L. Milechin, J. Mullen, S. Pisharody, A. Prout, A. Reuther, A. Rosa, S. Samsi, D. Stetson, A. Tse, C. Yee, and P. Michaleas, "Spatial temporal analysis of 40,000,000,000,000 internet darkspace packets," in *2021 IEEE High Performance Extreme Computing Conference (HPEC)*, pp. 1–8, 2021.

[59] J. Kepner, M. Jones, D. Andersen, A. Buluc, C. Byun, K. Claffy, T. Davis, W. Arcand, J. Bernays, D. Bestor, W. Bergeron, V. Gadepally, D. Grant, M. Houle, M. Hubbell, H. Jananthan, A. Klein, C. Meiners, L. Milechin, A. Morris, J. Mullen, S. Pisharody, A. Prout, A. Reuther, A. Rosa, S. Samsi, D. Stetson, C. Yee, and P. Michaleas, "Temporal correlation of internet observatories and outposts," in *2022 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW)*, pp. 247–254, 2022.

[60] I. Kawaminami, A. Estrada, Y. Elsakkary, H. Jananthan, A. Buluç, T. Davis, D. Grant, M. Jones, C. Meiners, A. Morris, S. Pisharody, and J. Kepner, "Large scale enrichment and statistical cyber characterization of network traffic," in *2022 IEEE High Performance Extreme Computing Conference (HPEC)*, pp. 1–7, 2022.

[61] H. Jananthan, J. Kepner, M. Jones, W. Arcand, D. Bestor, W. Bergeron, C. Byun, T. Davis, V. Gadepally, D. Grant, M. Houle, M. Hubbell, A. Klein, L. Milechin, G. Morales, A. Morris, J. Mullen, R. Patel, A. Pentl, S. Pisharody, A. Prout, A. Reuther, A. Rosa, S. Samsi, T. Trigg, G. Wachman, C. Yee, and P. Michaleas, "Mapping of internet "coastlines" via large scale anonymized network source correlations," in *2023 IEEE High Performance Extreme Computing Conference (HPEC)*, pp. 1–9, 2023.

[62] M. Jones, J. Kepner, A. Prout, T. Davis, W. Arcand, D. Bestor, W. Bergeron, C. Byun, V. Gadepally, M. Houle, M. Hubbell, H. Jananthan, A. Klein, L. Milechin, G. Morales, J. Mullen, R. Patel, S. Pisharody, A. Reuther, A. Rosa, S. Samsi, C. Yee, and P. Michaleas, "Deployment of real-time network traffic analysis using graphblas hypersparse matrices and d4m associative arrays," in *2023 IEEE High Performance Extreme Computing Conference (HPEC)*, pp. 1–8, 2023.

[63] M. Jones and et al, "Graphblas on the edge: Anonymized high performance streaming of network traffic," in *2022 IEEE High Performance Extreme Computing Conference (HPEC)*, pp. 1–8, 2022.

[64] Joint Chiefs of Staff - Joint Doctrine Publications, "Joint publication 3-12, cyberspace operations," 2018.

[65] CrowdStrike, "Global threat report," 2023.

[66] E. H. Do and V. N. Gadepally, "Classifying anomalies for network security," in *ICASSP 2020 - 2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 2907–2911, 2020.

[67] Black Camel Pictures, "Castles in the sky," 2014.

[68] B. T. Neale, "Ch — the first operational radar," *GEC journal of research*, vol. 3, pp. 73–83, 1985.

[69] United Kingdom Royal Air Force Radar Museum, "The birth of radar and the second world war," 2024.

[70] MIT Lincoln Laboratory, "Sage: Semi-automatic ground environment air defense system," 2024.

[71] The White House, "National maritime cybersecurity plan to the national strategy for maritime security," 2020.

[72] The White House, "National cislunar science & technology strategy," 2022.

[73] United States Air Force, "Platform one," 2021.

[74] United States Department of Defense, "Dod directive 5101.21e, dod executive agent for unified platform and joint cyber command and control (jcc2)," 2020.

[75] S. B. Griffith, *Sun Tzu: The art of war*, vol. 39. Oxford University Press London, 1963.

[76] S. E. McIntosh, "The wingman-philosopher of mig alley: John boyd and the ooda loop," *Air Power History*, vol. 58, no. 4, pp. 24–33, 2011.

[77] Joint Chiefs of Staff - Joint Doctrine Publications, "Joint publication 3-27: Homeland defense," 2018.

[78] United States Air Force, "Air force doctrine note 1-20, usaf role in joint all-domain operations," 2020.

[79] United States Defense Advanced Research Projects Agency (DARPA), "Darpa tiles together a vision of mosaic warfare," 2021.

[80] Joint Chiefs of Staff - Joint Doctrine Publications, "Joint publication 5-0, joint planning," 2020.