THE CYBER DEFENSE REVIEW
2025, VOL. 10, NO. 2, 81-97
https://doi.org/10.55682/cdr/p4kg-88cm

RESEARCH ARTICLE

Pulling the Thread: A Campaign Approach to Mission Thread Defense of Force Projection

David L. McNatt[1], Eunseok (Sam) Yoo[2], Joshua J. Welte[3], Pete Sinclair[1]

[1]U.S. Army Cyber Command, Fort Gordon, GA, USA
[2]Defense Logistics Agency Energy Middle East, Naval Support Activity, Bahrain
[3]U.S. Transportation Command, Scott Air Force Base, IL, USA

The U.S. military's ability to rapidly project power around the globe is a cornerstone of American defense strategy, and adversaries leverage denial strategies across domains to disrupt this capability. Recent cyberspace exploitation campaigns have infiltrated U.S. critical infrastructure, raising concerns about the military's ability to project decisive force during crises. Increasing cyber resilience for force projection requires transitioning from an asset-focused approach to a more proactive, mission-driven approach for defensive cyberspace operations (DCO). U.S. Army Cyber Command (ARCYBER) is implementing a campaign approach to address the cross-organizational challenge of increasing cyber resilience by leveraging partnerships to facilitate collaboration, leading the process of identifying critical systems, and producing plans to align requirements with resources. ARCYBER works closely with the Total Army (Active, Guard, and Reserve) and Joint and Interagency partners to promote effective collaboration, providing a common framework to translate organizational missions into cyberspace defense priorities. ARCYBER defends the Army's mission threads by maneuvering forces and hardening networks. Beyond proactive mitigation, the logistics enterprise must be prepared to "fight through" or bypass disruptions that penetrate defenses, ensuring mission success even in contested environments.

Keywords: cyber resilience, force projection, logistics, critical infrastructure, mission thread analysis, defensive cyberspace operations, risk mitigation

INTRODUCTION

> "In any kind of operation, there are two things you must get right…you have got to have your command and control in place, and you have got to have a robust, reliable logistics system." - LTG (R) Paul Mikolashek [1]

In the summer of 2017, chaos erupted at the Copenhagen headquarters of Maersk, the multinational shipping giant, as employees scrambled across open-plan offices to unplug computers, watching in horror as more screens flickered to black. A Russian cyber actor deployed malicious software (malware) known as *NotPetya* against Ukraine, which spread far beyond the country's borders. The cyberattack exploited a vulnerability in the Windows update mechanism to irreversibly encrypt an infected computer's master boot record, preventing it from finding its own operating system. The infected systems and the data residing inside them were effectively destroyed. Maersk's operations, which accounted for a fifth of global shipping capacity across 76 ports and nearly 800 ships, came to a standstill, suffering over $300 million in damages. The disruption exposed the vulnerability of modern commerce's interconnected systems to cyberattacks (McQuade 2018). This scenario highlights the potential for similar disruptions to defense critical infrastructure (DCI) and the joint logistics enterprise (JLEnt) during a major contingency operation.

As America's rivals grow more adept at cyberspace exploitation, there is an ongoing debate about how the United States can best secure itself in this domain. Recently, multiple cyber exploitation campaigns have infiltrated U.S. critical infrastructure, raising concerns about the U.S. military's ability to respond in a crisis. Proposed responses to these threats include new regulations, adjustments to roles and responsibilities across the national security enterprise, expanding the cyber workforce, and placing greater emphasis on "defending forward" and imposing costs on rivals (Segal 2025). U.S. Army Cyber Command (ARCYBER), as the Army's service cyberspace component, is responsible for operating and defending the Army's portion of the Department of Defense Information Network (DODIN), and when directed, other DODIN and non-DODIN networks (HQDA 2017). How can ARCYBER contribute to these emerging solutions and proactively mitigate threats to U.S. military force projection? Addressing this requires understanding both the nature of cyber risks and ARCYBER's unique advantages.

The complexity of cyber threats and limited resources often creates a default organizational preference for relegating cyber risk to technical commands and staff directorates. This status quo approach relies on asset- and compliance-based cyberspace security measures, which are necessary but not sufficient for establishing cyber resilience. The intangible nature of the cyberspace domain and the lack of institutional cyber knowledge often exacerbate this incentive, making operational planners hesitant to integrate cyber considerations into their operations. Furthermore, the technical cyber workforce may not always be familiar with

1. Quoted in Klug (2023)

operational staff priorities and may struggle to communicate technical cyber information in a way that is useful to operational staff. This often results in a lack of shared cyber risk understanding across organizations. This separation creates a disconnect between operational mission requirements and technical asset dependencies, hindering the Army's ability to optimize its cyberspace defense posture in a contested environment.

The ability to project power across transoceanic distances is increasingly challenged by rivals working to disrupt this capability across domains. Increasing cyber resilience in Army force projection requires transitioning from an asset-based approach to a more proactive, mission-based approach for defensive cyberspace operations (DCO). ARCYBER's campaign approach involves partnering with key stakeholders, identifying defense requirements, and developing plans that align requirements with resources. Effective collaboration across organizations requires a shared understanding of the strategic environment, cyber threats, and the challenges inherent to the cyberspace domain. To achieve this, ARCYBER works closely with the Total Army (Active, Guard, and Reserve) and Joint and Interagency partners. Through this collaborative effort, ARCYBER leads the process to enable supporting commands to analyze their mission threads, identify critical systems, and submit defense requirements. Finally, ARCYBER develops plans that synchronize cyberspace defense requirements and resources to mitigate threats to Army missions proactively. Through this approach, ARCYBER aims to empower commanders to make risk-informed decisions and improve overall operational resilience. Ultimately, this approach enhances the Army's ability to project power in a contested cyberspace environment.

This article is organized into four main sections. The first section provides a foundational understanding of the strategic cyber threat to the JLEnt. The second section highlights the unique challenges associated with cyber resilience. The third section details ARCYBER's approach to enhancing cyber resilience through partnerships, process, and plans. The fourth section looks beyond cyber resilience in logistics to highlight other critical functions and discuss logistics concepts that aim to improve overall operational resilience in a contested environment.

UNDERSTANDING THE LANDSCAPE

The Cyber Strategic Environment

According to *cyber persistence theory* by Harknett, Fischerkeller, and Goldman (2023), cyber actors continuously pursue initiative persistence to shape the contemporary cyber strategic environment. This pursuit of initiative persistence is driven by the underlying structure of cyberspace—a set of ever-changing digital conditions that incentivize state actors to continuously engage in cyber operations against other states to set security conditions to their advantage. Unlike nuclear or conventional models, which rely on coercion, these cyberspace

operations occur within a framework of persistent engagement, allowing rivals to continuously exploit vulnerabilities in pursuit of strategic advantage. Consequently, cyberspace engagements are best seen as continuous bouts of constant competition between rivals seeking cumulative outcomes through, primarily, cyber *faits accomplis*, which are efforts to seize and exploit digital terrain before an adversary can react.

Since the early 2010s, the strategic cyberspace competition for initiative persistence has evolved as part of the intensifying security competition between U.S. alliance networks and an increasingly cooperative Eurasian entente comprising China, Russia, Iran, and North Korea. The U.S. military's ability to project power rapidly across the globe is the foundation for American defense policy in this dynamic security environment (Busler 2022). Force projection, or "the ability to [deploy and sustain] the military instrument of national power from the United States or another theater in response to requirements for military operations," relies on the JLEnt through DCI (Joint Chiefs of Staff 2022b, GL-10). Logistics is "planning and executing the movement and support of forces" (Joint Chiefs of Staff 2023b, GL-5), and DCI is the "Department of Defense and non-Department of Defense networked assets and facilities essential to project, support, and sustain military forces and operations worldwide" (Joint Chiefs of Staff 2023a, GL-5). Cyber persistence theory, along with the observed evidence, strongly suggests that the contemporary cyber strategic environment poses significant risks to the U.S. military's power projection. Prudent planning, therefore, demands that U.S. military planners anticipate that potential adversaries will not wait for a crisis to contest America's ability to generate, project, and sustain its forces. Instead, rivals will continuously seek to pre-position on DCI to enable denial-by-disruption strategies calibrated to degrade U.S. force projection (van Ovost 2022). In short, rivals will use cyber *faits accomplis* to shape security conditions to their advantage.

By contesting logistics and force projection, adversary denial strategies could significantly hinder operational effectiveness and strategic decision-making. A denial strategy is a military approach aimed at undermining an adversary's ability to achieve their objectives, particularly in territory or political goals, by making the costs of pursuit prohibitively high, thereby forcing them to reconsider or concede (Pape 1996; Borghard and Lonergan 2017). With respect to military strategy, "logistics remains a means, circumscribes the potential ways, and plays a vital role in determining the time horizon necessary to achieve the desired ends depending on the level of risk" (Klug and Leonard 2025, 2). By contesting U.S. military force projection, adversaries can impact strategic decision-making by reducing options, delaying responses, and increasing risk. This disruption extends to the operational level of warfare, where commanders and staff "use operational art through campaign design and planning to sequence and sustain battles" (Benson 2025, 100). Therefore, the U.S. military must increase its operational resilience, with cyber resilience as a critical component, to counter these adversary denial strategies and maintain its strategic edge.

The *2022 National Defense Strategy* (NDS) acknowledged that today's contested environment poses a threat to U.S. strategic coherence. To counter this, the NDS prioritized resilience as a cornerstone of America's ability to deter attacks and prevail in armed conflict. Defining resilience as "the ability to withstand, fight through, and recover quickly from disruption," the NDS emphasized the importance of cyber resilience in mitigating cyber risk across "a growing surface of vital networks and critical infrastructure" (DoD 2022, 8). Cyber risk involves the potential for damage caused by the exploitation of vulnerabilities in information systems, considering both the likelihood of an attack and the impact if it occurs (Jabbour and Poisson 2016). Cyber risk has a reciprocal relationship with cyber resilience, in which risk informs resilience, and resilience in turn mitigates risk. Cyber resilience involves anticipating, withstanding, recovering from, and adapting to disruptions to systems that utilize or depend on cyber resources (NIST 2021). Cyber resilience is essential for maintaining operational resilience. With military operations increasingly reliant on digital technology, cyber risks amplify overall operational risks (Thomas 2024). Mitigating these threats is an increasingly complex challenge, driven by the rapid proliferation of information systems and the growing sophistication of exploits from both rival nation states and cybercriminals.

Cyber Threats

The information technology (IT) and operational technology (OT) systems underpinning U.S. critical infrastructure and the JLEnt have become increasingly automated and interconnected. IT encompasses devices such as laptops, software, and networking tools for communication and productivity. OT encompasses systems such as industrial control systems (ICS), supervisory control and data acquisition (SCADA), and programmable logic controllers (PLC). These cyber-physical connections enable remote monitoring and control of dispersed equipment (Parfomak and Jaikaran 2021), but their interconnectivity introduces greater cyber risks.

In IT and OT systems, disconnects are often revealed between the desired functionality and the actual behavior of the implemented code. These discrepancies create vulnerabilities in the digital landscape which offensive and defensive cyberspace operations teams continuously vie over for advantage. The effectiveness of cyberspace operations depends on identifying these underlying weaknesses. Detecting weaknesses in a target system requires a skilled team of specialists; this team includes operators who gain and maintain access, analysts who identify vulnerabilities, and developers who create exploits for operators to deploy. Exploitation efforts must start long before a crisis arises because operational effectiveness demands deep system knowledge. Moreover, once an exploit is used, its discovery, followed by patching or system hardening, limits its effectiveness for future use (Libicki 2012; Lin 2010; Smeets 2022).

The ongoing struggle over exploiting and protecting vulnerabilities has led to the emergence of various types of offensive cyberspace operations (OCO), each with distinct objectives and

methods. To better understand how threats gain an advantage in cyberspace, it is essential to grasp the types of effects OCO can produce and the mechanisms used to achieve those effects. Unlike actions in the conventional strategic environment, vis-à-vis the application of land, sea, or air power, OCO cannot substitute force for exploitation. This is a consequence of the clandestine character of cyberspace exploitation, as actors must obscure their intentions and activities to prevent defenders from rapidly closing off vulnerable avenues of approach and to avoid escalation. Additionally, since OCO relies on subverting system vulnerabilities clandestinely, political scientist Lennart Maschmeyer (2021) argues that an operational trilemma constrains the effectiveness of cyberspace operations: the *speed* with which vulnerabilities can be identified and exploited; the *intensity* of the effects generated; and the degree of *control* over a system and the effects delivered. Achieving optimal results simultaneously in all three areas is not possible.

OCO consists of cyberspace exploitation and cyberspace attack activities. Cyberspace exploitation involves access creation; intelligence, surveillance, and reconnaissance (ISR) activities; and preparation for effects delivery (Joint Chiefs of Staff 2022a). One example of this activity is Volt Typhoon, a Chinese state-sponsored cyber actor that compromised the IT networks of multiple U.S. critical infrastructure sectors across the continental United States and territories such as Guam. In addition to ISR in cyberspace, Volt Typhoon's actions appear to be aimed at pre-positioning themselves within networks for potential lateral movement to OT assets, with the intent to disrupt critical functions during a moment of crisis or military conflict (Jaikaran 2024; CISA 2024). Cyberspace attacks deliver effects. U.S. military doctrine distinguishes between system *denial* effects—which reduce a system's functional capacity (*degrade*), temporarily deny access (*disrupt*), or irreparably deny access (*destroy*)—and system *manipulation* that creates physical effects (Joint Chiefs of Staff 2022a).

According to international relations scholar Max Smeets (2022), cyber effects are primarily generated through three mechanisms: Distributed Denial of Service (DDoS), data manipulation, and system manipulation. First, DDoS attacks overwhelm a target system with a flood of data packets from multiple compromised sources. DDoS attacks are among the simplest and cheapest to execute, typically affecting only publicly accessible websites. Though temporary, their impact can be significant (Borghard and Lonergan 2017). A notable example is the 2012-2013 DDoS attacks by Iranian cyber actors against nearly 50 U.S. financial institutions, which disrupted access to public websites and incurred substantial mitigation costs (Warner 2020).

The second mechanism is data manipulation, where an attacker with the necessary access can modify, delete, or encrypt data (Smeets 2022). This action destroys value and renders digital resources unusable. Depending on the nature of the data targeted, entire systems may be rendered non-functional, as seen in the *NotPetya* attacks on Maersk. A similar example is the May 2021 Colonial Pipeline cyberattack, in which the DarkSide ransomware group

encrypted the company's IT billing systems. While there was no evidence that the company's OT systems were compromised, they were also shut down as a precaution. This attack crippled the operation of the largest fuel pipeline in the United States, halting the flow of gasoline, diesel, and jet fuel along the East Coast. The resulting disruption led to widespread fuel shortages, price hikes, and panic buying, causing significant economic and logistical challenges. Ultimately, Colonial Pipeline paid a ransom to regain access to its systems, citing the critical importance of its infrastructure and its responsibility to the nation (Nakashima, Torbati, and Englund 2021; Bogage 2021).

The third mechanism is system manipulation, which is typically achieved through OT systems (Smeets 2022). Manipulating a system can cause it to perform a regular function at a time or in a way that is not desired. In 2000, a disgruntled former employee of Maroochy Water Services in Queensland, Australia, exploited vulnerabilities in the sewage control system, releasing over 750,000 gallons of raw sewage into public waterways over several weeks. In extreme cases, system manipulation can alter a system's processes in ways that result in physical destruction. For example, in 2007, researchers conducted the Aurora Generator Test at Idaho National Labs to demonstrate how a cyberattack could physically damage the electric grid. Using malware to manipulate a diesel generator's circuit breakers produced abnormal torques, ultimately causing its destruction. Perhaps most notably, in 2009, a cyber actor exploited the PLCs controlling the centrifuges at Iran's nuclear enrichment facility in Natanz. The malware modified the centrifuges' operation, causing physical damage to between 1,000 and 2,000 of the devices (Zetter 2014).

While cyber effects cannot entirely halt U.S. military force projection, these effects can introduce Clausewitz's "fog, friction, and chance" into critical nodes of the logistics enterprise, causing cascading disruptions across operations. Military cyberspace operations weaponize friction in the contest between opposing military systems (Rovner 2020). The intensity of cyber effects against DCI will, however, be constrained by Maschmeyer's trilemma. At the outset of a conflict, adversaries will have a finite number of exploits available. As these effects are delivered and mitigated, adversaries will need time to identify new vulnerabilities and develop additional exploits. They must choose whether to concentrate their effects early in the conflict or to sequence them for sustained disruption.

These cyber resource constraints make targeting vulnerabilities in military logistics particularly appealing. Logistics operations often rely on information sharing and partnerships with commercial entities that may have inconsistent cybersecurity measures. These inconsistencies can create exploitable conditions that offer adversaries high potential payoffs. Gaining insight into logistics operations early in a conflict through cyberspace exploitation offers invaluable intelligence on U.S. intentions. DDoS attacks on public-facing websites can hinder cooperation with commercial partners, while altering or destroying data can introduce inefficiencies and necessitate duplicative efforts. Logical and physical destruction effects require costly and

time-consuming mitigation efforts. These disruptions reverberate through tightly coordinated logistical operations, causing delays in the logistics chain and creating narrative vulnerabilities regarding U.S. capability and commitment (Dougherty 2023).

CROSS-ORGANIZATIONAL CHALLENGES FOR DEFENSIVE CYBERSPACE OPERATIONS

Enhancing cyber resilience for critical missions in the face of increasingly sophisticated cyber threats is a significant challenge for defense planning that requires extensive collaboration. In theory, the malleability of cyberspace should favor the defender, but in practice, the scale and complexity of modern information systems leave ample opportunity for exploitation (Libicki 2012). Adversaries seek to disrupt force projection by targeting dependencies within mission threads, where a cyber effect can create cascading delays, miscoordination, and mission failures. Mission threads are "operationally driven, technically supported descriptions of the end-to-end set of activities required to execute a mission or mission task" (CJCS 2022, A-5–A-6). Cyber resilience is a critical component of *mission assurance*, a doctrinal process that seeks to ensure that everything needed to carry out essential functions—including people, equipment, facilities, networks, and supply chains—remains operational and resilient, no matter the environment or situation (DoD 2018). The challenge of mitigating cyber risk lies in the requirement for "analysis beyond a specific portion of cyberspace, geographic area, or organizational responsibility," and the need for units to "apply systems thinking to understand the processes, components, dependencies, and interactions from both a technical and organizational perspective" (HQDA 2024, 1–2).

The traditional approach to managing cyber risk often focuses on network operations for functionality and security. However, this approach places too much reliance on the technical workforce to mitigate cyber risk. This tendency stems from the organizational and technical complexity of network analysis and risk communication. Operational planners often overlook cyber considerations due to the intangible nature of cyberspace and a general lack of institutional cyber knowledge. At the same time, technical personnel are often unfamiliar with operational priorities and struggle to communicate technical information in a way that is useful to operational planners. As a result, cyber risk is frequently relegated to specialized organizations such as the G-6/J-6 staff directorate or a cyberspace operations headquarters. The disconnect between operational and technical planners creates a gap in understanding between operational mission requirements and technical asset dependencies (Corbari et al. 2024).

The involvement of multiple stakeholders with varying roles and authorities further compounds the complexity of mitigating cyber risk to force projection. This challenge is particularly pronounced when Mission Relevant Terrain-Cyber (MRT-C) systems, such as logistics networks owned by private sector entities, reside outside of the DODIN. The authority to

address active threats on a network is fragmented, depending on whether the threat occurs on a private or public sector network and whether the nation is engaged in armed conflict. Consequently, responsibility for countering threats to Army networks is spread across Federal Law Enforcement, Homeland Security, and Homeland Defense activities. This fragmentation of authority impacts both preparedness and response times in peacetime and wartime, complicating the ability to address emerging threats swiftly.

ARCYBER has identified these challenges and adapted its approach to solving them over time. In 2020, a Homeland Defense planning effort in support of Headquarters, Department of the Army (HQDA) initially highlighted the complexities of determining and acting upon Army cyber protection interests in the homeland. This effort ultimately led to the Army Force Projection (AFP) planning effort. Utilizing Mission Thread Analysis (MTA), the AFP effort revealed the need for a broader Army-wide initiative to address these issues. This requirement, in turn, led to the development of the DCO-Optimization effort and the Army Defensive Cyberspace Optimization Conference (ADCyOC). These complementary planning efforts aim to define and document the Army's cyberspace defense requirements more accurately, empowering ARCYBER to direct forces and harden networks more effectively. Moreover, these efforts help identify dependencies where the Army requires Interagency support. While national cyber policy continues to evolve, the Army must be prepared to advocate for its interests with Interagency partners effectively.

ADOPTING A CAMPAIGN APPROACH TO INCREASE CYBER RESILIENCE

To address emerging challenges in cyberspace, ARCYBER has refined its partnerships, processes, and planning to mitigate cyber risk and de-conflict overlapping efforts. In response to increasingly sophisticated cyber threats, ARCYBER has refined the MTA process to better employ defensive cyberspace forces and close the gaps in cyberspace defense that traditional asset-based, compliance-driven, and reactive security measures leave unaddressed. By decomposing mission threads into operational and technical requirements, MTA enables proactive risk mitigation through the identification of MRT-C. MRT-C includes the components of the cyber terrain such as devices, links, applications, and protocols that are essential to the operation of a critical asset or the successful completion of a mission. Mapping MRT-C allows defensive cyberspace forces to maneuver more effectively and harden networks in support of mission owners (HQDA 2024; Corbari et al. 2024). DCO seeks to "defeat the threat of a specific adversary and/or to return a compromised network to a secure and functional state" (Joint Chiefs of Staff 2022a, II–4). Defensive cyberspace forces need a deep understanding of network architecture, cross-organizational mission dependencies, and prioritized directives to proactively mitigate risk and respond swiftly to incidents.

Leveraging Partnerships

The cross-organizational challenge of cyber resilience in force projection requires partnerships across the Department of War (DoW), the Total Army, and the Interagency. The unique knowledge, relationships, and authorities of these partners complement ARCYBER's capabilities. Building relationships with these partners before a crisis is crucial to their effectiveness in times of need. While Interagency partners and Total Army defensive cyberspace forces may not be ideal for emergency response, they are well-suited for cyberspace defense requirements that involve long-term collaboration with MRT-C owner and operators, both on and off the DODIN. Army Reserve and National Guard defensive cyberspace forces have developed capabilities leveraging their long-term relationships with MRT-C owners throughout the United States, as well as their experience with commercial technology partners.

Force projection requires a collaborative approach between service and joint stakeholders in cyberspace operations, homeland defense, logistics, and mobilization. While HQDA provides institutional oversight and coordination, key stakeholders span various operational functions. In cyberspace, this includes U.S. Cyber Command (USCYBERCOM), DoD Cyber Defense Command (DCDC), and ARCYBER. Homeland defense relies on the collaboration of U.S. Northern Command (USNORTHCOM) and U.S. Army North (ARNORTH). Logistics success hinges on the combined efforts of U.S. Transportation Command (USTRANSCOM), the Defense Logistics Agency (DLA), Army Materiel Command (AMC), U.S. Army Transportation Command (ARTRANS), and other service transportation components. Finally, effective mobilization necessitates seamless integration between Forces Command (FORSCOM), the Office of the Chief of Army Reserve (OCAR), the National Guard Bureau (NGB), and First Army. This intricate *system-of-systems* underscores the criticality of collaboration in protecting DCI and ensuring successful mobilization and force projection.

Cyber effects pose a significant threat to DCI; yet, without adequate support for collaboration, Interagency partners may lack the awareness and preparedness necessary to effectively mitigate these attacks, thereby increasing cyber risk. These partners include the Department of Homeland Security (DHS), which encompasses Homeland Security Investigations (HSI), the Federal Emergency Management Agency (FEMA), and the Cybersecurity and Infrastructure Security Agency (CISA); the Department of Justice (DOJ); and various state, local, and tribal governments, including their law enforcement components. Experience has shown that the Interagency is sometimes unaware of DoW and Army requirements, leaving them unprepared to respond to cyberattacks on DCI vital to DoW missions. This knowledge gap is a policy issue stemming from the unclear division of responsibilities between Homeland Security and Homeland Defense mission sets and authorities.

To address these coordination issues, engaging with interagency partners before a crisis is essential. By sharing off-DODIN DCI protection requirements with Interagency partners

while campaigning in competition, the Army can give them ample time to prepare and take proactive measures. This preparation can include collaborating with the private sector and developing legal strategies to counter malicious cyber actors (MCA) when necessary. Building relationships between the interagency and MRT-C owners and operators during this phase can also facilitate a more effective response to MCAs targeting MRT-C. This approach is analogous to how a local fire department works with businesses to identify potential fire hazards and develop tailored response plans, ensuring they are better equipped to respond in an emergency. Taking a proactive and collaborative approach strengthens collective defenses and improves the ability to respond to cyber threats.

Leading the Process

ARCYBER has adopted a campaign approach to optimize Army DCO and proactively mitigate risk to critical missions such as force projection. This approach is an iterative process of continuous improvement that requires collaboration across stakeholders to identify MRT-C and defend the Army's vital missions. This process is structured around the annual ADCyOC to facilitate a shared understanding across the Army enterprise, and bi-weekly working groups, which provide regular touchpoints with stakeholders. This structured process enables ARCYBER to collaborate with stakeholders across the Army, providing a common framework to translate Army missions into actionable cyberspace defense priorities. It enables stakeholders to advocate for their priorities, allowing ARCYBER to engage with units and gather the technical information needed to plan and execute DCO effectively.

MTA supports this campaign approach by providing a framework for organizations responsible for planning major operations, contingencies, or institutional functions to collaborate with ARCYBER. Through this analysis, organizations can translate their missions into mission threads, MRT-C, and actionable cyberspace defense requirements. This approach shifts the focus from individual assets to a more holistic understanding of mission vulnerabilities, encompassing those that extend beyond organizational boundaries. By clearly mapping MRT-C, MTA enables commanders to make better-informed decisions regarding resource allocation of defensive cyberspace forces and risk mitigation to support a mission (HQDA 2024).

To achieve this comprehensive understanding, operational planners and technical professionals must collaborate to identify and analyze mission threads. Operational planners from the G-3 and G-5 staff directorates work with technical signal and cyber professionals to decompose their mission essential tasks. MTA involves identifying, defining, and depicting mission process threads (MPT), which outline the conceptual flow of the task, and mission engineering threads (MEngT), which capture the technical components required to execute each step. Mission owners use the MPTs to "depict the process of a mission as a series of steps or actions required to achieve successful accomplishment" (Corbari et al. 2024, 42). The MEngT includes the components, both physical and digital, necessary to execute each

step in the MPT successfully. When analyzing the MEngT, planners must carefully scope the requirements to prevent over-analysis and avoid wasted effort. Common models for MEngT analysis include the cyberspace layer model (persona, logical, physical) and network layer models, such as the Open Systems Interconnection (OSI) Model. Critically, staff must also identify any external dependencies, such as electrical power and satellite connectivity (HQDA 2024; Corbari et al. 2024).

Effective MTA results in a clear depiction and understanding of the organization's MRT-C, highlighting the cross-organizational dependencies between mission owners and asset owners (Corbari et al. 2024). This information is captured within the Mission Assurance Risk Management System (MARMS) through the Mission Assurance Decision Support System (MADSS) and Strategic Mission Assurance Data System (SMADS) (CJCS 2023). Identifying and depicting this cyber terrain creates situational awareness of dependencies, uncovers vulnerabilities, and supports resource allocation decisions for maintaining operational continuity.

This comprehensive understanding of MRT-C, achieved through MTA, allows commanders to make informed risk assessments and operational decisions. With a clearer understanding of the cyber risks to their mission threads, commanders can more effectively decide whether to avoid, mitigate, or accept risk. Actions to address these risks "may include changing how the capability is employed, mitigating the risk throughout the mission thread, reengineering portions of the mission thread, or preparing to operate with diminished capabilities [or falling back on analog processes]" (HQDA 2024, 3). Commanders may also elevate the risk to a higher echelon for further action (HQDA 2024).

Furthermore, identifying MRT-C through MTA informs other critical processes such as determining defense requirements, positioning forces, informing task critical asset (TCA) nominations, and identifying DCI. A TCA is "an asset that is of such extraordinary importance that its incapacitation or destruction would have a serious, debilitating effect on the ability of one or more DoD or OSD Components to execute the capability or mission-essential task it supports" (DoD 2018, 19). In addition to TCA and DCI identification, MTA provides a more comprehensive understanding of the vulnerabilities tied to those resources. When cyberspace defense requirements are based on a detailed knowledge of MRT-C, intelligence collection efforts are more focused and defensive cyberspace forces can deploy sensors on the network more effectively, resulting in a more agile and responsive defense that enables defensive cyberspace forces to address incidents swiftly.

Beyond the tangible actions taken, fostering a psychological "perception of control" is crucial for cyber resilience. When effective staff collaboration empowers leaders to project a sense of control while they "fight through" a cyber disruption, it sustains trust and cohesion within their organizations, reducing the risk of cascading disruptions across their functions (Thomas 2024).

Producing Plans

ARCYBER increases cyber resilience across the Army enterprise by developing plans that align requirements and resources. First, ARCYBER advocates for resources by consolidating Defense Requirements Statements (DRS) from across the Army enterprise and facilitates their inclusion in USCYBERCOM's mission alignment process. The DRS uses a straightforward format, enabling mission owners to describe their cybersecurity needs clearly. This standardized approach facilitates a better understanding of individual requirements and guides mission owners in providing essential information for DCO planning and prioritization. USCYBERCOM's mission alignment process, in turn, leverages these DRS submissions to inform their decisions regarding mission prioritization and the alignment of cyber mission forces across military services and Joint Force Headquarters-Cyber (JFHQ-C) (Corbari et al. 2024). Finally, USCYBERCOM's Combatant Command Campaign Plan (CCP) and annual orders process operationalize these forces across the cyber enterprise.

Second, ARCYBER operationalizes near-term requirements to proactively mitigate cyber risk across the Army through its own annual orders process. When Army organizations identify their MRT-C and cyberspace defense requirements, they often lack the organic resources and expertise to fully defend their mission threads. Collaboration with supporting Army commands allows ARCYBER to capture defense requirements in its annual orders and align forces to missions. ARCYBER defends the Army's mission threads by maneuvering forces and hardening networks. These forces include cyber protection teams (CPTs), which can deploy mission elements forward to hunt and clear threats from networks and harden them against future compromise. CPTs can also monitor MRT-C on an ongoing basis. In addition to CPTs, Network Enterprise Technology Command's (NETCOM) Regional Cyber Centers (RCC) work with ARCYBER's G-36 and the Cyber Protection Brigade (CPB) to leverage enterprise-wide analytics in support of identified cyberspace defense requirements (Barrett 2024). ARCYBER also utilizes cyber red teams and cyber readiness inspection activity (CRIA) teams to identify vulnerabilities and enable defense of MRT-C. Requirements that exceed ARCYBER's capacity can be referred to the Cyber National Mission Force and Interagency partners (Corbari et al. 2024).

Lastly, ARCYBER captures long-term planning requirements to increase cyber resilience across the Army through its campaign support plan (CSP) and contingency planning. ARCYBER's CSP aligns with USCYBERCOM's CCP and HQDA's Army Campaign Plan (ACP). Through these processes, ARCYBER collaborates on longer-term operational and institutional initiatives to strengthen cyber resilience in critical Army missions such as force projection. These initiatives may include operational partnerships, network modernization, force structure adjustments, and the fielding of new capabilities. This planning is most effective when informed by MRT-C and cyberspace defense requirements from across the Army enterprise. ARCYBER also incorporates these requirements into its contingency plans, enabling a more

rapid response in a crisis to support operation plans (OPLANs). Effective collaboration across the Army enterprise facilitates planning that bolsters cyber resilience in both campaigning and contingency response efforts.

PREPARING TO "FIGHT THROUGH" DISRUPTIONS

Achieving broader operational resilience requires mission thread defense of other critical functions and more wholistic concepts for operational risk mitigation across the logistics enterprise. MTA allows other critical functions, such as multinational operations, ISR, long-range precision fires, command and control, and integrated air and missile defense (IAMD), to shift focus from individual assets toward a broader understanding of mission vulnerabilities.

While proactive mitigation of cyber risk enhances overall operational resilience, the logistics enterprise must be prepared to "fight through" disruptions caused by cyber effects that bypass efforts to protect and defend MRT-C. The logistics community recognizes the challenges of the current contested environment and is developing concepts to strengthen operational resilience in the face of denial effects across domains. Integrating logistics planners earlier in the planning process can improve operational resilience by ensuring that courses of action are more aligned with logistics capacity, rather than accepting risks to sustain operations that were conceived without proactive logistics input (Hughes 2024).

Chris Dougherty (2023), a researcher at the Center for a New American Security (CNAS), developed a framework for responding to the contested logistics environment through an adaptive logistics approach. Central to the framework is the persistent challenge that "reinforcements take too long to arrive from the United States or other theaters to defend allies and partners or counterattack from a position of strength" (11). To enable forward forces to persist and build combat power, Dougherty proposes an adaptive logistics strategy that can transition from efficient methods to more resilient ones, based on threats, operational needs, and the status of infrastructure.

Dougherty's (2023) adaptive logistics strategy has forward, theater, and enterprise components. He offers three elements in enhancing resiliency in forward logistics. First, forward forces should moderate their operational tempo to minimize attrition by doing less and avoiding destruction. Second, the U.S. military should preposition forces and materials in dispersed, secure locations to reduce reliance on resupply from rear areas. Third, Army forces should prepare to "live off the land" by sourcing fuel and other essential materials locally, thereby reducing their dependence on uninterrupted resupply. At the theater level, intermediate basing operations could further strengthen theater logistics by supporting multiple defensible lines of communication. At the enterprise level, accurate and timely information enables a responsive and efficient "pull" model where logistics meets operational demand "just-in-time." In a contested environment where information is degraded, logistics must shift to a robust

and sufficient "push" model, which relies on anticipating needs and moving resources during windows of opportunity. With a risk-informed understanding of the cyber threat, commanders are better equipped to "fight through" disruptions by combining cyber and operational mitigation activities.

CONCLUSION

As the Army navigates today's contested cyber environment and evolving fiscal realities, leaders must not lose sight of the fact that sustained investment in cyber resilience will remain a strategic necessity. The ability to project force and sustain operations will hinge on the Army's ability to mount effective cyber defenses that can anticipate, withstand, and recover from persistent threat activity. ARCYBER's campaign approach provides a starting point, but its success will depend upon a long-term commitment from military leaders, planners, and technical experts. By prioritizing proactive cyberspace defense measures, integrating cyber resilience into force planning, and fostering collaboration, the Army can ensure that its logistics enterprise remains resilient in the face of ever-changing threats. The alternative—waiting until a crisis to react—risks ceding the initiative to adversaries already operating in a persistent state of cyber engagement. The Army's ability to fight and win in a cyber-contested battlespace is precisely what hangs in the balance.

ABOUT THE AUTHORS

Colonel David L. McNatt is an Army Strategist serving at U.S. Army Cyber Command as the G-5 Director for Strategy, Plans, and Policy. He ensures ARCYBER's near-term efforts support future objectives. He is a graduate of Boston University as well as the Naval War College where he also studied as a Cyber & Innovation Policy Institute (CIPI) Gravely student.

Lieutenant Colonel Eunseok (Sam) Yoo is an Army Logistician currently commanding the Defense Logistics Agency Energy Middle East. Previously, he served as the Strategic Operations Division Chief (G-5) at U.S. Army Cyber Command, focusing on Global Force Management, Security Cooperation, and implications of Defensive Cyberspace Operations for the Army enterprise. He holds an M.S. in Logistics Management from Florida Institute of Technology and is a graduate from the School of Advanced Military Studies (SAMS), the Joint Cyberspace Operational Planners Course, and the College of Naval Command and Staff at the Naval War College.

Major Joshua J. Welte is an Army Strategist at U.S. Transportation Command. While contributing to this article, he served as a strategic planner at U.S. Army Cyber Command. At ARCYBER, he led initiatives in areas such as Indo-Pacific plans, Army cyber posture, expeditionary cyberspace operations, cyberspace security cooperation, and defensive cyberspace operations. MAJ Welte holds an M.A. in Security Studies from Kansas State University and a Certificate in Social Influence from Augusta University. He is a graduate of the School of Advanced Military Studies (SAMS), the Joint Cyberspace Operational Planners Course, and the Joint Logistics Planners Course.

Mr. Pete Sinclair is currently employed by Peraton as a Cyberspace Operations Planner in support of the U.S. Army Cyber Command G-5. He retired from the Army after serving in three different branches over 21 years and six deployments. He is a graduate of Northern Michigan University and the School of Advanced Military Studies (SAMS). 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. This is his second contribution to *The Cyber Defense Review*.

REFERENCES

Barrett, Maria B. 2024. "Operational Perspectives from the Field – ARCYBER in the Cyberspace Domain." *The Cyber Defense Review* 9 (1): 19–30. https://www.jstor.org/stable/48770661.

Benson, Kevin. 2025. "The Operational Level of War and Logistics." In *Professionals Talk Logistics: Sustaining Strategy and Operations,* edited by John Klug and Steve Leonard, 100–115. Havant, UK: Howgate Publishing.

Bogage, Jacob. 2021. *Colonial Pipeline CEO Says Paying $4.4 Million Ransom Was 'the Right Thing to Do for the Country'.* The Washington Post, May 19, 2021. https://www.washingtonpost.com/business/2021/05/19/colonial-pipeline-ransom-joseph-blunt/.

Borghard, Erica D., and Shawn W. Lonergan. 2017. "The Logic of Coercion in Cyberspace." *Security Studies* 26 (3): 275–305. https://doi.org/10.1080/09636412.2017.1306396.

Busler, Bruce. 2022. "Strategic Mobility in the Context of U.S. National Defense Strategies." *Joint Force Quarterly* 107 (4th Quarter): 75–84. https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3197251/strategic-mobility-in-the-context-of-us-national-defense-strategies/.

CISA (Cybersecurity and Infrastructure Security Agency). 2024. *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure.* Technical report. February 7, 2024. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

CJCS (Chairman of the Joint Chiefs of Staff). 2022. *Universal Joint Task List Program.* Technical report CJCSI 3500.02C. Washington, DC: U.S. Department of Defense. https://www.jcs.mil/Portals/36/Documents/Doctrine/training/cjcsi_3500_02c.pdf.

CJCS (Chairman of the Joint Chiefs of Staff). 2023. *Mission Assurance Construct Implementation.* Technical report CJCSI 3209.01A. Washington, DC: U.S. Department of Defense. https://www.jcs.mil/Portals/36/Documents/Library/Instructions/CJCSI%203209.01A%20(JS-221219-T8WP)%20VDJS%20Signed.pdf.

Corbari, George, Neil Khatod, John Popiak, and Pete Sinclair. 2024. "Mission Thread Analysis: Establishing a Common Framework in a Multi-discipline Domain to Enhance Defensive Cyberspace Operations." *The Cyber Defense Review* 9 (1): 42–50. https://www.jstor.org/stable/48770663.

DoD (U.S. Department of Defense). 2018. *Mission Assurance (MA),* DoD Directive 3020.40. U.S. Department of Defense, Washington, DC. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302040p.pdf.

DoD (U.S. Department of Defense). 2022. *National Defense Strategy.* U.S. Department of Defense, Washington, DC. https://apps.dtic.mil/sti/trecms/pdf/AD1183514.pdf.

Dougherty, Chris. 2023. *Buying Time: Logistics for a New American Way of War.* Technical report. Washington, DC: Center for a New American Security. https://www.cnas.org/publications/reports/buying-time.

Harknett, Richard J., Michael P. Fischerkeller, and Emily O. Goldman. 2023. *Cyber Persistence Theory: Redefining National Security in Cyberspace.* Oxford: Oxford University Press.

HQDA (Headquarters, Department of the Army). 2017. *Army Commands, Army Service Component Commands, and Direct Reporting Units.* Technical report Army Regulation 10-87. Washington, DC.

HQDA (Headquarters, Department of the Army). 2024. *Mission Thread Defense.* Technical report Training Circular 3-12.2.90. Washington, DC.

Hughes, Zachary. 2024. "Giving Our 'Paper Tiger' Real Teeth: Fixing the U.S. Military's Plans for Contested Logistics Against China." *Joint Force Quarterly* 115 (4th Quarter): 38–47. https://digitalcommons.ndu.edu/joint-force-quarterly/vol115/iss3/20/.

Jabbour, Kamal, and Jenny Poisson. 2016. "Cyber Risk Assessment in Distributed Information Systems." *The Cyber Defense Review* 1 (1): 91–102. https://www.jstor.org/stable/26267301.

Jaikaran, Chris. 2024. *Salt Typhoon Hacks of Telecommunications Companies and Federal Response Implications.* Technical report. Congressional Research Service, November. https://crsreports.congress.gov/product/pdf/IF/IF12798.

Joint Chiefs of Staff. 2022a. *Cyberspace Operations.* JP 3-12. Washington, DC: Joint Chiefs of Staff.

Joint Chiefs of Staff. 2022b. *Joint Campaigns and Operations.* JP 3-0. Washington, DC: Joint Chiefs of Staff.

Joint Chiefs of Staff. 2023a. *Joint Homeland Defense.* JP 3-27. Washington, DC: Joint Chiefs of Staff.

Joint Chiefs of Staff. 2023b. *Joint Logistics.* JP 4-0. Washington, DC: Joint Chiefs of Staff.

Klug, John, and Steve Leonard. 2025. "Introduction." In *Professionals Talk Logistics: Sustaining Strategy and Operations,* edited by John Klug and Steve Leonard, 1–10. Havant, UK: Howgate Publishing.

Klug, Jon. 2023. "Establishing the Realm of the Possible: Logistics and Military Strategy." *Military Strategy Magazine* 9 (1). https://www.militarystrategymagazine.com/article/establishing-the-realm-of-the-possible-logistics-and-military-strategy/.

Libicki, Martin C. 2012. "Cyberspace Is Not a Warfighting Domain." *I/S: A Journal of Law and Policy for the Information Society* 8 (2): 321–36.

Lin, Herbert S. 2010. "Offensive Cyber Operations and the Use of Force." *Journal of National Security Law & Policy* 4 (1): 63–86. https://nationalsecurity.law.georgetown.edu/wp-content/uploads/2010/08/06_Lin.pdf.

Maschmeyer, Lennart. 2021. "The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations." *International Security* 46 (2): 63–90. https://doi.org/10.1162/isec_a_00418.

McQuade, Mike. 2018. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," August 22, 2018. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Nakashima, Ellen, Yeganeh Torbati, and Will Englund. 2021. "Ransomware Attack Leads to Shutdown of Major U.S. Pipeline System." *The Washington Post* (May 8, 2021). https://www.washingtonpost.com/business/2021/05/08/cyber-attack-colonial-pipeline/.

NIST (Standards, National Institute of, and Technology). 2021. *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach.* NIST Special Publication 800-160, Volume 2, Revision 1. Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-160v2r1.

Pape, Robert. 1996. *Bombing to Win: Air Power and Coercion in War.* Ithaca, NY: Cornell University Press.

Parfomak, Paul W., and Chris Jaikaran. 2021. *Pipeline Cybersecurity: Federal Programs.* Technical report. Congressional Research Service, September 9, 2021. https://crsreports.congress.gov/product/pdf/R/R46903.

Rovner, Joshua. 2020. "Cyberspace and Warfighting." In *Ten Years In: Implementing Strategic Approaches to Cyberspace,* edited by Jacquelyn G. Schneider, Emily O. Goldman, and Michael Warner, 85–104. Newport, RI: Naval War College Press.

Segal, Adam. 2025. "China Has Raised the Cyber Stakes: The 'Salt Typhoon' Hack Revealed America's Profound Vulnerability," January 21, 2025. https://www.foreignaffairs.com/united-states/china-has-raised-cyber-stakes.

Smeets, Max. 2022. *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force.* London: C. Hurst & Co. Ltd.

Thomas, Ria. 2024. "Redefining Cyber Resilience: Through the Risk Register Lens." *Journal of Business Continuity & Emergency Planning* 18 (1): 75–83.

van Ovost, Jacqueline D. 2022. "Statement of General Jacqueline D. Van Ovost, United States Air Force Commander, United States Transportation Command Before the Senate Armed Services Committee On the State of the Command," March 29, 2022. https://www.armed-services.senate.gov/download/van-ovost-statement-03/29/2022.

Warner, Michael. 2020. "A Brief History of Cyber Conflict." In *Ten Years In: Implementing Strategic Approaches to Cyberspace,* edited by Jacquelyn G. Schneider, Emily O. Goldman, and Michael Warner, 21–38. Newport, RI: Naval War College Press.

Zetter, Kim. 2014. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon.* New York: Broadway Books.

Received 14 March 2025; Revised 29 October 2025; Accepted 7 November 2025