

Resilient Dependencies: Preparing to Fight Through Cyber Disruption

Lt. Gen. Maria B. Barrett

U.S. Army Cyber Command, Fort Gordon, GA, USA

In a volatile threat environment, the Army's readiness and ability to execute missions at home and abroad increasingly hinge on digital dependencies spanning commercial software, IT/OT infrastructure, utilities, and the organic industrial base. This opener frames a cohesive approach to mission thread resilience across the Unified Network, emphasizing three imperatives: partner early and often with program managers, vendors, contractors, and local utilities to rehearse crisis response and establish shared understanding; procure secure by design capabilities with transparent vulnerability disclosure and rapid patching; and make data informed, commander owned risk decisions that enable formations to "fight through" disruption. Drawing lessons from the Army Cyber Institute's Jack Voltaic workshops and the inaugural Army Defensive Cyberspace Operations Optimization Conference, the article illustrates how civil military interdependencies can cascade and how rehearsals reveal hidden assumptions. A "fort to port" vignette, where a cyber compromise of national rail switching triggers operational delays, shows the value of synchronized public-private response, near real-time operational data, and flexible branches and sequels. The piece calls for acquisition leaders to weigh vendor track records on zero days and patch latency, signals the need to report and coordinate through ARCYBER's Information Warfare Operations Center and NETCOM's Global Cyber Center, and argues for a whole-of-nation model akin to the Civil Reserve Air Fleet to surge cyber resilience. Ultimately, it celebrates the tenacity of signal and cyber professionals and invites continued thought leadership that prevents strategic surprise in cyberspace while transforming how the Army teams, trains, and fights in and through a contested homeland.

Keywords: cyber resilience, DevSecOps, critical infrastructure, operational technology, mission risk

Disclaimer: *The views expressed in this work are those of the author(s) and do not reflect the official policy or position of their employer(s), the U.S. Military Academy, the Department of War, the U.S. Government, or any subdivisions thereof. 2025. This is a work of the U.S. Government and is not subject to copyright protection in the United States. Foreign copyrights may apply.*



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

OPENING

The volatility of today's world requires unceasing diligence in assessing risk to our Army organizations, units, and their missions. Threats in the cyber domain targeting our digital dependencies will always challenge the Army's combat readiness and ability to fulfill peace and wartime missions. Cyber events like the Colonial Pipeline disruption, and physical events like Hurricane Helene require shared trust and collaboration with commercial and municipal infrastructure partners that underpin the core functionality of our Army installations and nation. I strongly applaud the Army Cyber Institute at West Point (ACI) for its success in the Jack Voltaic® series of workshops, which have brought much-needed awareness and focus to the complexity of civil-military interdependencies. I also commend ACI's other invaluable contributions to the Army and operational force, as exhibited by products that make us think critically about how we team and train to tackle our Nation's cyber challenges. Continued thought leadership is a command imperative if we are to optimize support to the Army's operational force in areas like mission thread defense and national policy analysis. Here, ACI stands at the frontier, on mission to prevent strategic surprise in cyberspace.

OPERATIONALIZING SUPPORT FOR CAPABILITY DEPENDENCIES

This past January, the Army Cyber Command (ARCYBER) hosted the first Army Defensive Cyberspace Operations Optimization Conference (ADCyOC). The event spanned the gamut, leveraging robust academics to baseline Army command stakeholders' knowledge of mission thread analysis and information technology (IT) and operational technology (OT) dependencies on critical missions. Every intrusion the ARCYBER team analyzes, whether DoD or commercial domain, confirms a core tenet that the Army's cybersecurity and mission resilience is increasingly dependent on other entities and service providers in ways few understand well enough to sufficiently advise commanders on risk to mission. Our cyber

force must acknowledge this understanding gap and evaluate the risk of these dependencies in order to buttress Commanders' decision-making.

I offer three thoughts below on addressing our mission thread resiliency:

1) Partner for External IT/OT Dependency Support for Critical Operations

Program Managers, service providers, contractors, and infrastructure owners must understand the critical Army mission their technology (e.g., software) or infrastructure (e.g., municipal water, internet service circuit) is supporting. Start a healthy conversation between your Army organization and those organizations on which you depend. Ask how you can rehearse crisis response and continuously reinforce trust and shared understanding of impact "left of crisis". As ARCYBER operates and defends the Army's Unified Network, we engage with contractors and industry liaisons who provide network and data capabilities. Events like CrowdStrike in 2024 highlight that even advanced, well-resourced global conglomerates are susceptible to commercial software and IT infrastructure providers. That event did not disrupt Army networks, but it focused us on where a company's "first-call" should go in the future. Vendors often report to Army program or contracting offices costing valuable time for synchronizing an effective response. Time is ammunition in cyber operations. They should report critical cybersecurity information directly to ARCYBER's Information Warfare Operations Center (IWOC)—the command responsible for assessing risk and developing remediation plans, or to NETCOM's Global Cyber Center, the nexus of the Army's Unified Network. Bottom line: this issue is operational, not contractual.

Today, we constantly remind software and hardware vendors that their support, transparency, and leadership are vital to our Army missions; they are an extension of our network security. While imperfect, collaboratively thinking through 'likely' and 'most dangerous' cyber scenarios in advance has paid off with our commercial partners who value candor in their teaming with us.

IT and its dependencies are not the only concern for network owners and mission commanders. OT and the physical infrastructure it supports (for example, water and energy utilities) also impact Army missions. As with technology vendors, garrison leaders and senior mission commanders should continuously connect and collaborate with local agencies and utility providers to build relationships that optimize a shared understanding of capabilities, initial response actions, and most likely and/or threatening scenarios that could adversely impact services. ACI's Jack Voltaic workshops demonstrate the value in communities that openly discuss concerns, coordination points, and mutual support capabilities so that we avoid cascading failures caused by unvalidated assumptions.

The Army's on-premises OT within the organic industrial base (OIB) is a similar cause of concern. The Army manages critical missions that support global force projection and logistics

for the Joint Force. We should better understand our OIB dependencies on vendors, utility providers, and other critical infrastructure and key resources (CIKR) such as transportation and chemical ecosystems. Commanders overseeing these OIB missions should understand the dependencies fully within their control, and those that require special partnership, coordination and/or rehearsal to optimally mitigate service disruption.

2) Secure By Design | Expedient and Transparent Vulnerability Disclosure

We must start making purchasing and contracting decisions based on risk. A key first step is for our industry partners to better understand our risk profile and methodology. When deployed, I would never send a Soldier outside the berm with faulty body armor. Nor would I accept this risk on our network perimeter, within our mission command or business systems, or in other critical functions. We must stop acquiring technology and capabilities from vendors that are not developing products that are secure by design. Vendors' DevSecOps processes must include responsive and transparent vulnerability disclosure, matched by expedient patch delivery or effective risk mitigation. Software development in unsecured environments invites unseen long-term risk that is unacceptable in our critical warfighting systems. Accepting the risk of such software must be a decision of last resort.

While some acquisition programs are mandated to procure technology that meets high security standards, we are at an inflection point where everything we connect to the Unified Network is a potential avenue of approach for adversaries, exposing our critical missions and giving them the opportunity to hold our data at risk. Leaders with acquisition authority must be armed with the right questions, intelligence, and framework to analyze product risk. We should seldom, if ever, acquire a product from a vendor with a history of zero-day vulnerabilities that took months to patch. Our technology requirements will continuously grow as the Army increasingly employs artificial intelligence (AI) capabilities. Those advances must be informed by both our real-time understanding of the threat and the vendor's track record and reputation.

3) Data-Informed Decisions and Fighting Through Disruption

Army and Joint leaders understand that we likely will never have enough cyber defense capacity to fully defend all mission and terrain against a dedicated adversary. They also know we may need to "fight through" a disruption. Consider the following "fort to port" scenario:

INDOPACOM tensions cause an Army division to mobilize to its Seaport of Debarkation (SPOD). Troops load their equipment onto trains at their installation railhead and depart on the several hundred-mile trip to the SPOD. Halfway to the SPOD, the Cybersecurity & Infrastructure Security Agency (CISA) alerts the Army that U.S. rail infrastructure has been compromised by a malicious cyber actor, and as a precautionary measure, rail operations have been halted nation-wide pending further assessment.

What does the Division Commander do next?

The Division Commander could request available cyber forces to expedite restoring rail operations. USCYBERCOM and DHS are likely already working to assess and resolve the situation. However, with elevated global tensions, Army cyber forces may already be committed against other existing cyber mission priorities.

Assume the rail operators determine they must physically inspect the functionality of hundreds of automated switching devices along the track and projects requiring at least fourteen days to restore rail operations. The division G4 projects that a ground movement to the SPOD will take at least nine days.

There are several ways to tackle this hypothetical scenario. A cyber response team may either be unavailable or otherwise not aligned with the commander's optimal scheme of maneuver. However, our cyber forces in overwatch can be just as effective without 'boots on the ground.' Advances in technology now allow commanders and staffs to access more data in near real-time, with which to see options and make more timely decisions. Less complexity allows them to focus on the fight to their front. S6/G6 teams provide vital assessments to the commander on risks to data, platforms, and networks. This is key given our interdependence on commercial capabilities. Commanders still own the risk to their mission as well as the options they have to mitigate that risk. Fostering optimal operational transparency with commercial partners on which the commander's mission depends is crucial.

CYBER OPERATIONS MAY NOT BE SILVER-BULLET REMEDIES TO DISRUPTION

Having routinely participated in U.S. Forces Command's (FORSCOM) Rehearsal of Concept (ROC) Drill for a mass deployment and mobilization of U.S. Forces in support of a combatant command, "fight through" was the crux of my pitch describing to commanders the cyber realities of operating in, through, and from a contested homeland. Leaders who anticipate likely branches and sequels, triggered by technological disruption that are designed to disrupt movements and operations, are more likely to decide on successful alternative paths and are more resilient than those who don't.

A COHESIVE APPROACH TO CYBER DEFENSE

Every day, I'm encouraged by the tenacity of our Army signal and cyber professionals who operate and defend the Army's Unified Network. This is the backbone of Army data-centric operations. Still, I harbor a healthy respect for the malice and capabilities of our most formidable adversaries. Dominating cyberspace will require continuous investment and vigilance. While ARCYBER continues to adapt to meet the challenges of a domain evolving at warp-speed, we must align with national programs that partner industry and the DoD to confront them head on. I eagerly welcome collaboration among public and private sectors to establish trustworthy mechanisms that more effectively allow us to engage experts in troubleshooting

and responding to cyber emergencies. Programs like the Civil Reserve Air Fleet demonstrate the power and willingness of American industry to support national security endeavors and achieve a “whole-of-nation” approach to national defense.

This year marks the Army’s 250th anniversary—our cyber forces continue to demonstrate the tenacity, innovation, and perseverance that have been our hallmarks since 1775. I’m honored and proud to be a part of our continued transformation. Please enjoy this volume of The Cyber Defense Review. I thank each of you for serving as a catalyst in making our cyber force the best it can be.

Respectfully,
mbb