BREAKING DEFENSE | eBRIEF

Trends driving offensive and defensive cyber warfare

An editorial eBRIEF sponsored by leidos

SITREP

Cyber warfare is shifting under the Pentagon's feet. The US military is no longer defending just data centers and networks, it is contending with adversaries who can infiltrate through the radio spectrum, hijack industrial controls, and disrupt weapon systems on the battlefield.

On the offensive side, Army scientists and engineers are pioneering "RF-enabled cyber," a blend of electronic warfare and hacking that uses the radio frequency spectrum to slip malicious payloads into adversary systems. By manipulating protocols at the bit level or interfering with processing cycles, these non-kinetic effects can blind sensors, disrupt decision-making, and give commanders new tools alongside kinetic firepower.

On defense, the Pentagon is moving quickly to institutionalize Zero Trust across its vast enterprise. Three architectures — the Navy's Flank Speed, DISA's Thunderdome, and Dell's Fort Zero — have cleared the bar for implementations by achieving all 152 Zero Trust goals set by the Defense Department CIO office.

Information technology networks are only part of the picture. Operational technology such as supervisory control and data acquisition (SCADA) systems and robots, and also frontline weapon systems like HIMARS, are vulnerable to cyber and electronic disruption. DoD leaders say securing the command-and-control pathways of these systems with Zero Trust principles is essential to ensuring US combat credibility in future conflicts.

We examine cyber warfare from both sides in this Breaking Defense eBRIEF.

– *Barry Rosenberg*
Technology & Special Projects Editor, Breaking Defense

ON THE COVER: Bravo Company (Bandits), 11th Cyber Battalion, culminated months of home station training with participation in National Training Center Rotation 25-03, January and February 2025. Expeditionary CEMA (Cyber and Electromagnetic Activities) Team 05 and ECT 06, B Co., 11CB, conducted electromagnetic reconnaissance, radio frequency enabled offensive cyber operations, and special purpose electromagnetic attacks to shape operations during the rotation for III Armor Corps, 1st Infantry Division, and 1st Battalion, 3rd Special Forces Group (Airborne). Photo by Steven Stover, 780th Military Intelligence Brigade (Cyber)

Convergence of offensive and defensive cyber is reshaping how DoD develops, fields, and integrates capabilities

Of all the tools the Department of Defense has at its disposal, few must evolve faster than those related to networks and information technology systems for both offensive and defensive cyber. Such conversations typically swirl around how defensive cybersecurity has to pace adversarial threats but the same goes for offense, too.

One of the latest developments in offensive cyber is a confluence of cyber and the radio frequency (RF) spectrum to create what's called RF-enabled cyber where offensive payloads ride on the RF spectrum to infiltrate and disrupt adversary networks.

"RF-enabled cyber takes it one step farther at the bit-byte level to achieve the desired effect," said Mark Farwell, CEMA (cyber electromagnetic) division chief in the C5ISR Center at US Army Combat Capabilities Development Command (DEVCOM). "We get down into the nitty gritty of protocols so that maybe we can flip bits over the air to cause a desired effect. It may be inherent to a protocol that we're taking advantage of or it could even be causing additional effects in the processing cycles of the system we're going after that has the desired intent."

Farwell noted that since US Cyber Command became fully operational with enhanced budget control authority, it now has strategic responsibility for what's called on-net or wire-type cyber operations. In response the C5ISR Center has shifted its offensive cyber science and technology focus to what the Army still has responsibility for, which is now more akin to offensive electronic warfare.

"Cyber RF-enabled effects capabilities play to the Army's inherent strengths," said Farwell. "We are a tactical force. We are that RF touch, that RF reach of the adversary [and] better suited to RF-enabled effects and non-kinetics in general to support Army maneuvers and our survivability. These more specialized electronic attack aspects help our tactical forces in the battlespace more so than in the past."

Such RF-enabled cyber actions help to create more offensive possibilities on the processing side of such operations, and the decision engines on the backend that may have a more lasting or a surgical-type effect that is better suited for what the commander is ultimately trying to achieve in the battlespace.

"The Army's great at kinetic effects when it comes to maneuver in order to take positions that they need to," said Shane Snyder, cyber effects branch chief in the DEVCOM C5ISR Center. "Some of the things we're looking at is how do you provide those similar non-kinetic effects to the commanders so they have that in their arsenal of things [if they] have this dilemma that they have to take care of."

Those offensive tools are typically geared toward individual areas of responsibility and their specific needs, but generally focus on countering an adversary's targeting capabilities against

U.S. Marines and Civilians with Marine Corps Cyberspace Warfare Group and Marine Corps Cyberspace Operations Battalion participate in Cyber Flag 23-2 at an undisclosed location, Aug. 7, 2023. The purpose of the exercise was to enhance readiness and cyber warfare capabilities. Each team was strategically positioned in an offensive or defensive role, engaging with various cyber-attack and defense scenarios. (U.S. Marine Corps photo by Cpl. Oneg Plisner)

friendly forces, including enemy intelligence, surveillance, and reconnaissance (ISR) sensors, as well as countering their decision cycles. Helping to make that possible are soldiers versed in software and code.

"Most everything we do today is evolving around software and that's how we're going to deliver these effects, whether it's good practices or just being able to get something into the soldier's hands where they're able to understand," said Steve Strickland, a computer scientist in DEVCOM's cyber effects branch. "One of things that's changed for the Army is that now we have soldiers that are capable of doing coding and development work. That goes hand in hand for us. Now we're able to work with them providing these capabilities and they're able to provide feedback to us so that we can continually evolve it to a product that they can use and understand without having to go through a lot of training to learn or having somebody else manage it because they don't understand the coding piece."

What also goes hand in hand is threat intelligence to inform offensive operations. That means a strong coupling with the Intelligence Community.

Said Snyder, "They do future trends analysis to see where things are going and have regional specific reports on things that we're looking at. All that drives our S&T to make sure we're informed. Without that tight relationship with the intel community, we wouldn't have that. It's those pieces, the reporting and intelligence pieces that they gather, [that allows us to] get more fidelity."

Cyber defense for IT, OT, and weapon systems

There is a tight coupling between offensive and defensive cyber, where offensive insights inform defensive capabilities, and vice

Sgt. James Hyman, Expeditionary Cyber-Electromagnetic Activities (CEMA) operator, 11th Cyber Battalion, gathers information from sensors to develop cyber effects, during an Operational Readiness Assessment for the battalion here, March 29, 2023. Photo by Steven Stover 780th Military Intelligence Brigade (Cyber)

versa. For example, after years of planning and development on how to introduce Zero Trust principles to military organizations, the DoD's CIO office has certified three ZT implementation programs that are now available for adoption by any other group within the Defense Department. They are the US Navy's Flank Speed (that also includes the Marine Corps), the Defense Information Systems Agency's Thunderdome, and Dell Technologies' Fort Zero.

All three gained approval by meeting 91 target-level and 61 advanced-level goals set by the DoD CIO office that must be achieved across the entirety of the DoD by the end of fiscal year 2027. According to the office, implementing all 152 goals should provide 100-percent cyber protection for information technology (IT) networks through capabilities like micro-segmentation and behavior monitoring that prevents intruders from breaching or moving laterally through networks in search of data and intellectual property.

None of those three architectures consist of a single system that executes Zero Trust but rather dozens of industry solutions tied together by a main systems integrator. For example, each of the approved implementations can include 30+ vendor systems with various cybersecurity capabilities. In the past, the DoD would have tried to integrate those systems together on its own, but the continuing onslaught and only partial success against cyberattacks and data loss illustrates the shortcomings of that approach. Now, the components of a complete and secure Zero Trust architecture can reside in a pair of computer cabinets integrated by a single organization.

With the protection of information technology networks proceeding apace, the DoD CIO office plans to apply its Zero Trust principals to one of the newest attack vectors – operational technology such as supervisory control and data acquisition (SCADA) systems, CNC machines, and robots. A commercial thermostat on the wall that controls temperature is also an OT attack vector if it's WiFi enabled and synced to an IT system.

The Stuxnet attack in 2010 on Iran's centrifuges that enriched uranium is an example of a cyberattack against OT. So was the Colonial Pipeline attack that shut down oil delivery to a large portion of the East Coast in 2021, creating a national security emergency. The critical energy, water and wastewater, and transportation infrastructures in the US are also vulnerable to OT infiltration through the many valves, switches, and sensors necessary for their operation.

"Colonial Pipeline is a perfect public example of what happened by essentially taking over the OT system of Colonial Pipeline for the purposes of ransomware," said Randy Resnick, director of the DoD CIO's Zero Trust Portfolio Management Office. "For a few days, it created minor panic in the population that thought they were going to run out of fuel. That's a national security issue. That's a homeland security issue. There is a large connection between the protection of the homeland and national security.

"Almost every attack on the US in some fashion becomes a point of concern within the Department of Defense and/or the Intelligence Community depending on the severity and [what] I'll call the blast radius of the attack. When it comes to OT systems, of course the Department of Defense needs to protect those systems ideally in a ZT way."

To address these vulnerabilities, the DoD CIO office is translating its ZT targets and advanced activities for IT and rewriting them to address OT. A fan chart for the path forward on ZT for OT is expected to be published in fourth-quarter 2025.

Another new vein of cyber defense to be mined is protection of weapon systems. When the US first agreed to send the longer-range High Mobility Artillery Rocket System (HIMARS) to Ukraine, for example, the consensus was that the weapon system would be a game changer to strike deeper into Russian territory. Soon, however, cyber and electronic attacks against the guidance of the launched rockets made them ineffectual in hitting their targets and ended their relevance on that particular battlefield.

The answer is not to address cybersecurity for the multi-million-dollar HIMARs artillery system as a whole but to add Zero Trust security protection to all the systems that make up the weapon.

"A fighter jet is a weapon system and it's integrated with hundreds of vendor products and solutions just like a ZT solution

Kenya Defence Forces service members and U.S. Air Force personnel collaborate during a cyber defense training course as part of exercise Justified Accord 2025 (JA25) at the Humanitarian Peace Support School (HPSS) in Nairobi, Kenya, Feb. 13, 2025. The course enhances participants' ability to conduct defensive cyberspace operations (DCO) and respond to emerging cyber threats in joint and multinational environments. Led by U.S. Army Southern European Task Force, Africa (SETAF-AF) and hosted by Kenya, Djibouti and Tanzania, JA25 integrates high-intensity training scenarios that sharpen warfighting skills, increase operational reach and enhance the ability to execute complex joint and multinational operations. The exercise runs from Feb. 10–21, 2025. Photo by SETAF Africa. U.S. Army Southern European Task Force, Africa

is," said Resnick. "You have Lockheed Martin or Northrop building fighter jets for the department. They are the ones doing the integration and the ones delivering the final product, and the government is buying X amount of final product. They're not doing the integrations.

"We're now thinking cybersecurity in the same sense. That's the model going forward. We're going to be buying integrations. The vendor is going to have to deliver an integrated solution for us that achieves a certain outcome. A fighter jet achieves a certain outcome and so that's a weapon system. A missile is another weapon system. A submarine is a weapon system. The torpedo in the submarine is a weapon system. You can see how granular you can get. We are not talking about achieving Zero Trust inside the weapon system or inside the multiple vendor products. What we are trying to do is achieve Zero Trust on the integration.

"What does that mean for a weapon system? For us at the moment, that means the command and control to the weapon system. If I could get inside the command and control, that's how I can defeat the weapon. From a Zero Trust perspective [for] weapon systems, our prime focus is to prevent adversary exploitation of the command and control of a weapon system.

"It turns out that command and control happens to ride IT systems. When we address IT systems to the target or advanced level, we are inheriting the protection of command and control. The way we're addressing weapon systems is by securing the IT piece of the weapon system that sits outside the weapon [and] that goes into the weapon as a command or control to describe what we want that weapon to do. I want you to launch, I want you to go to this GPS coordinate. That's what I mean by addressing ZT in weapon systems."

At the moment, target and advanced-level goals for weapon systems are yet to be determined, but Resnick said they will be forthcoming.

VIEWPOINT FROM LEIDOS

THE FUTURE OF CYBER WARFIGHTING

leidos

Matt Schumacher is Vice President of National Security Sector Cyber at Leidos.

The United States, along with its allies and partners, requires certainty to operate resilient networks, combat systems, and infrastructure that underpin our global warfighting capability. To actively defend these systems, while maintaining the capability to strike our adversaries when and where we choose, cyber warfighters must operate in a multi-domain cyber battlespace with superior, combined offensive and defensive capabilities driven by timely, relevant, and accurate threat intelligence.

Cyber warfare is the strategic high ground for peer and near-peer nation-state threat actors such as China and Russia, and as Great Power competition evolves, U.S. readiness and capabilities must outpace that of our adversaries in cyberspace, achieving a state of domain advantage across the competition continuum. The U.S. military can find itself simultaneously in all three stages of the competition continuum, engaging hostile actors and neutralizing threats in cyberspace – at speed and global scale.

This thought piece from Matt Schumacher, vice president, National Security Sector Cyber, Leidos, provides key insights into the future cyber battlespace, focusing on opportunities for warfighters to outmaneuver and defeat our adversaries. It specifically focuses on the cyber warfighter and their operational mission space, recognizing the need for a doctrinal continuum of conflict that integrates: (1) specialized, campaign-specific intelligence to underpin and drive cyber operations; (2) scaled offensive cyber capabilities; and (3) advanced cyber defense combat capabilities that are A.I. enhanced. This three-part article explores these warfighting mission sets and recommends how industry partners can provide support.

Scaling Mission-Grade Cyber Intelligence

Nation-state sponsored and affiliated cyber adversaries who represent and engage in the majority of Advanced Persistent Threat (APT) campaigns, are central to Great Power competition, primarily involving China, Russia, Iran, and North Korea. These actors are leveraging advances in artificial intelligence, quantum computing, and software development to scale their strategic cyber warfare capabilities in pursuit of tactical and operational-level advantages. Recent campaigns, such as the Volt Typhoon and Salt Typhoon attacks, demonstrate the ability to carry out sophisticated attacks and operate undetected within protected United States infrastructure. U.S. cyber forces must be trained and operationally focused on defending vital nodes and reciprocating these campaigns to deter our adversaries in cyberspace.

To address these threats, our threat intelligence must integrate seamlessly with offensive and defensive cyber operations, producing timely, relevant, and actionable high-quality intelligence on APTs with specific focus on the following areas:

1. **Regional-Specific APT Intelligence:** Assessing hard-target campaigns and target types in anti-access/area denial (A2AD) environments across physical and logical cyber terrains.
2. **Offensive-Focused All-Domain Intelligence:** Intelligence-driven products for targeting operations with expertise and data in areas such as supply chains, multi-domain combat systems, and red system component vulnerabilities, mobile systems, including deep knowledge of operating systems, protocols, and component functions
3. **Intelligence-Driven Cyber Tooling:** Develop and deploy military grade software through intelligence-driven DevSecOps collaboration among analysts, developers, and operators. Mission software that integrates adversary TTPs in development and testing will drive resiliency across the system environment.

We know that high-quality Cyber-Intelligence Preparation of the Operating Environment (C-IPOE) processes enable cyber warfighters to:

- Develop robust cyber defense plans for effective Hunt-Forward Operations, accelerating the intelligence-to-development-to-operations cycle.
- Create precise targeting plans for offensive operations, bolstered by actionable on-net data and specialized trusted A.I. tools to rapidly produce target mission packages.
- Maintain critical advantage across operational domains and develop leading edge cyberspace operations technologies.

With AI-Driven cyber defense, warfighters move beyond mere response; they anticipate, adapt, and act preemptively. This embodies the essence of advanced intelligence, transforming traditional cyber defense into a proactive, resilient, and adaptive strategy.

Offensive Operations – Delivering Lethality in Cyberspace

Offensive cyber operations will increase as strategic warfighting capabilities in low- and high-intensity global conflicts. These capabilities offer cost effective, scalable options as alternatives to kinetic warfare. As adversaries evolve, the U.S. must ensure ongoing effectiveness in operating within red-space (adversary) cyber terrain; diversity in payload delivery; and acceleration of the cyber kill chain, creating a full spectrum cyber operation with no way in. Future cyber warfare operations require the following capabilities, in pursuit of these goals:

- **Scalable Exploitation Development and Targeting:** Accelerate and automate the quality of target data through advanced reverse engineering, vulnerability research, and targeting for CNO operators to ensure payload precision. These capabilities will largely be driven by A.I. enabled special-purpose platforms to improve mission precision and velocity.
- **Invisible Payloads with Churnable Infrastructure:** Ensure payloads are undetectable, rapidly available, and commercially mature in relation to the target environment.
- **Enhanced Delivery Mechanisms:** Integrate air-gapped and RF-enabled payloads into Cyber-Electromagnetic Activities (CEMA) warfare systems.

The ability to scale cyber weapon production and deployment across domains — land, air, maritime, and space — is vital. Ethical considerations and strategic oversight must accompany these advancements to maintain credibility and deterrence.

Defensive Operations – Setting Up the Attack Surface Defense

Advanced cyber defense poses significant challenges in a multi-domain, integrated battlefield. Commanders and operators require continuous system availability during high-intensity combat operations. A resilient defense hinges on leveraging A.I., automation, data analytics, and an active threat-hunting operation. One of the most crucial metrics is driving down "mean time to action" across the operating environment. Key defensive strategies in cyber defense include:

1. **Multi-Domain and Multi-System (MDMS) Defense:** Securing physical weapon systems, operational technology (OT), and command-and-control platforms across all operating environment domains (air, land, sea, space, cyberspace).
2. **A.I.-Augmented Defense:** Smartly deploy trusted A.I. solutions to scale defensive capabilities across the MDMS attack surface and correlate with trusted threat indicators and offensive tradecraft. Enables security teams to scale their detect, defend, and counter threat operations more effectively.
3. **Counter Information Operations:** Minimize adversary influence campaigns within the information environment through information advantage capabilities.

An "assume breach" mindset empowers defenders to proactively hunt, clear, and remediate threats to high-value assets creating a Resilient by Design operational system. Partnerships with industry and adoption of innovative technologies are essential to achieving these goals.

Conclusion

The evolving cyber battlespace requires an aggressive frontline where innovation, intelligence, and decisive action converge. Where there are capability gaps, U.S. industry has solutions available, mission expertise, and the innovation budgets to put battle-tested, scalable technologies into the hands of cyber warfighters today. As the U.S. and its allies face increasingly sophisticated adversaries, collaboration between military cyber operators, government agencies, and industry partners is critical. By integrating cutting-edge intelligence, offensive capabilities, and adaptive defensive strategies, the cyber warfighter can maintain superiority in the cyber domain. Industry partners have a pivotal role in shaping this future — through advanced technologies, collaborative development, capability investment, and unwavering commitment to mission success.

Breaking Defense thanks Leidos for supporting this editorial eBRIEF. Sponsorship does not influence the editorial content of the eBRIEF.