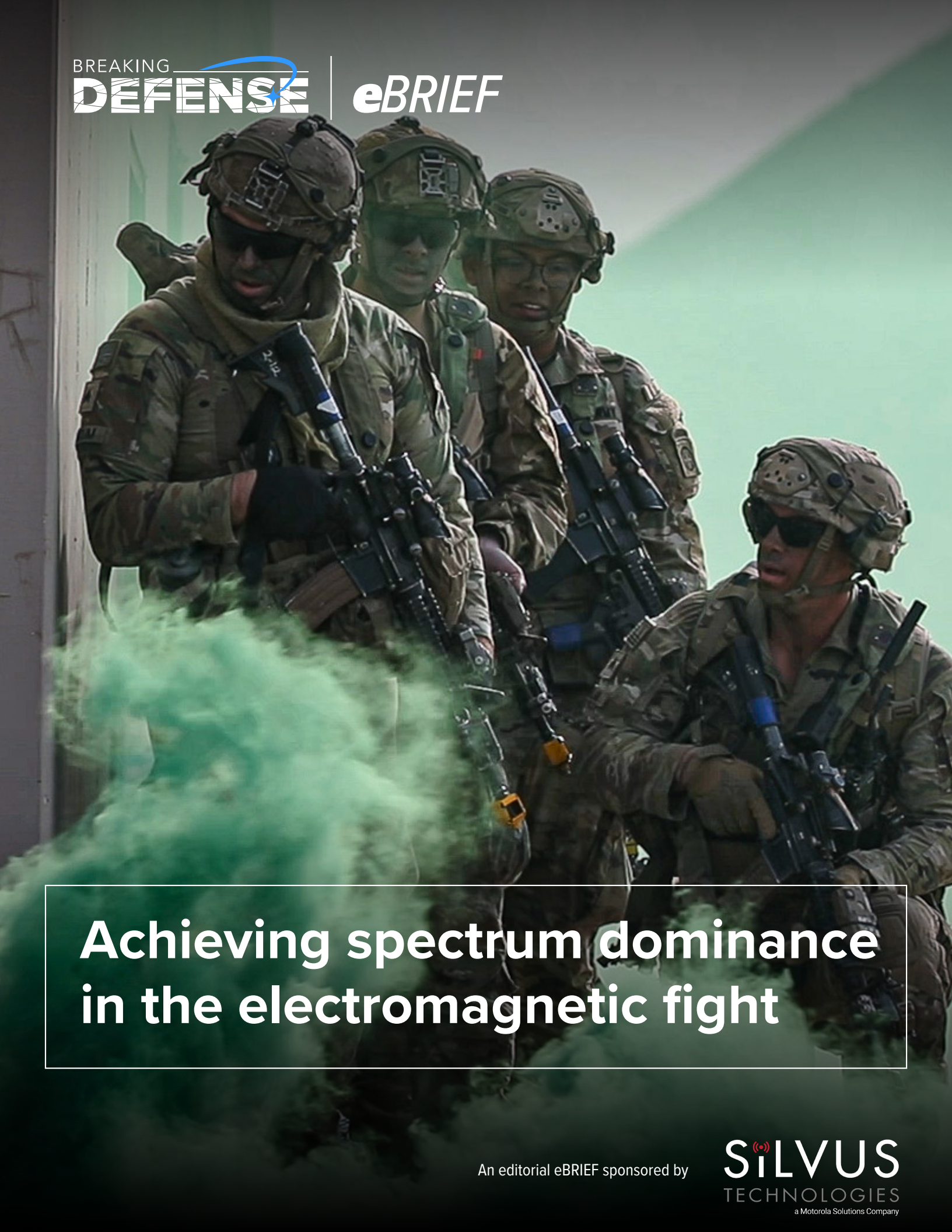
BREAKING DEFENSE | eBRIEF



Achieving spectrum dominance in the electromagnetic fight

An editorial eBRIEF sponsored by

SILVUS TECHNOLOGIES
a Motorola Solutions Company

SITREP

Near-peer competitors are moving to challenge US dominance in the electromagnetic spectrum, and nowhere is that more apparent than in the fight over secure communications. With advanced electronic warfare (EW) capabilities, adversaries are intent on disrupting command and control, sowing confusion, and undermining decision-making across the battlespace. To counter that threat, the Pentagon is doubling down on resiliency through Anti-Jam and Low Probability of Detection Systems engineered to keep comms transmitting and receiving in contested battlespace.

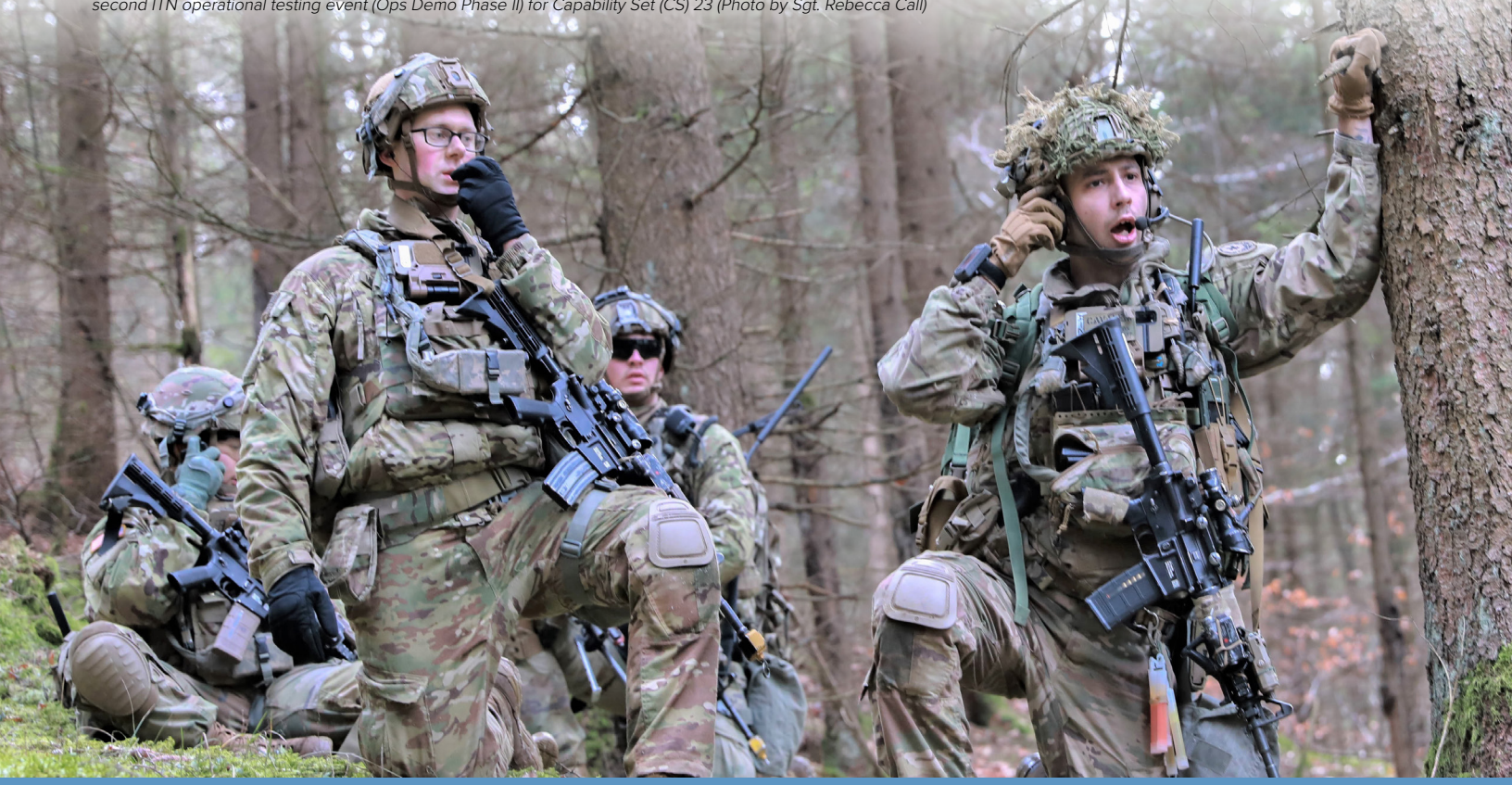
One area central to that effort is Naval Information Warfare System Command (NIWC) Atlantic's Resiliency Innovation & Vulnerability Assessment Lab (RIVAL), a joint initiative with the Joint Tactical Networking Center (JTNC). The lab serves as a proving ground for military and commercial systems, exposing them to contested electromagnetic environments to identify vulnerabilities and test performance under stress. The results help shape acquisition requirements, guide system development, and ensure warfighters get capabilities they can trust in the field.

The state of U.S. Anti-Jam and Low Probability of Intercept/ Low Probability of Detection (LPI/LPD) technologies is advancing, but experts stress that speed is critical. Many of the most promising innovations remain in early stages and require sustained investment, rapid fielding, and tight collaboration between government, industry, and academia. Demand signals are clear: warfighters need resilient, interoperable, and scalable communications to enable multi-domain and coalition operations.

As adversaries refine and expand their EW capabilities, the Pentagon's challenge is to stay one step ahead by ensuring secure communications remain a cornerstone of operations through a variety of Anti-Jam techniques. This Breaking Defense editorial eBRIEF explores how that's being done.

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

Soldiers with the 2nd Cavalry Regiment conduct dismounted operations during Dragoon Ready 2023 using the Integrated Tactical Network (ITN) capabilities, which include 2-channel Leader and Manpack radios, single channel radios, and Nett Warrior end-user devices for communications with personnel in the Strykers and command post. The event served as the second ITN operational testing event (Ops Demo Phase II) for Capability Set (CS) 23 (Photo by Sgt. Rebecca Call)



ON THE COVER: U.S. Army Paratroopers, assigned to Bravo Company, 2nd Battalion, 508th Parachute Infantry Regiment, 2nd Brigade Combat Team, 82nd Airborne Division, move under concealment through a Military Operations on Urban Terrain village leveraging a U.S. Army Small Multipurpose Equipment Transport during a human machine integration experiment as part of Project Convergence - Capstone 4, Fort Irwin, Calif., March 11, 2024. (U.S. Army photo by Spc. Marquis McCants)

DoD labs are stress-testing Anti-Jam systems to ensure warfighter C2 in the face of EW threats

Breaking Defense asked NIWC Atlantic and the JTNC to respond to a series of questions on how the Pentagon is tackling EW threats to communications. Their written responses were provided jointly by:

- **Brett Bendt:** NIWC Atlantic, Software Defined Radio Solutions (SDRS), Integrated Product Team (IPT) Technical Lead, RIVAL Lab Test Director;
- **Lt. Cmdr. Christopher "Neo" Leslie,** JTNC, Deputy Directorate Lead, Technical Analysis and Engineering Services (TA&ES);
- **Steven Boyd:** NIWC Atlantic, Lead System Engineer, SDRS IPT;
- **Immanuel "Manny" Johnson:** JTNC, Strategic Communications Support.

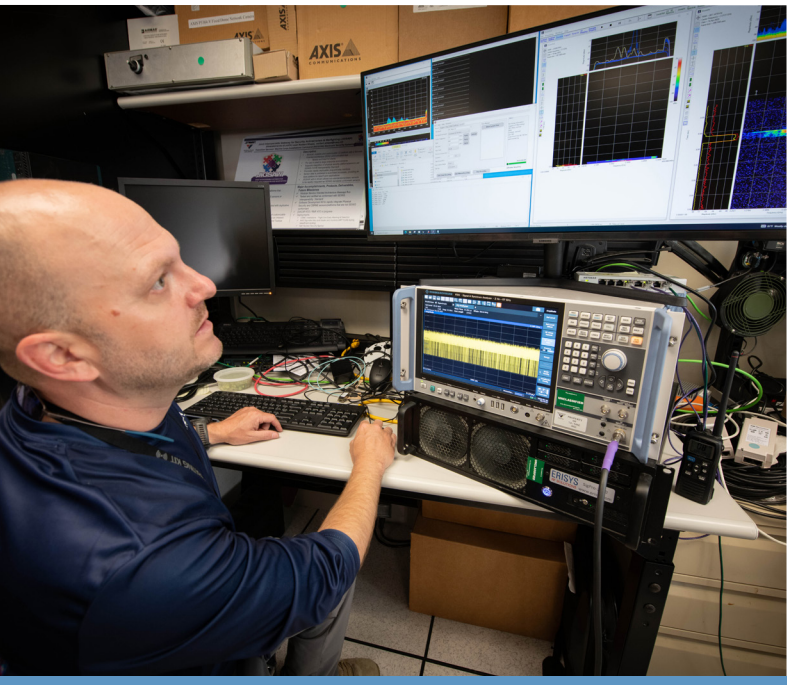
Breaking Defense: How would you describe the pace at which near-peer adversaries are advancing their EW capabilities?

Advancements in electronic warfare by both allies and adversaries are progressing rapidly and deliberately, fueled by substantial investments in offensive and defensive communications technologies. Similar to the commercial sector's focus on IT innovation, defense industries are leveraging cutting-edge wireless technologies to strengthen their communications and EW capabilities. These wireless innovations are continuously evolving to address the growing demands for capacity, connectivity, and reliability in congested electromagnetic environments.

DoD resiliency facilities (engineering and T&E), like NIWC Atlantic's RIVAL Lab, are identifying, testing, adapting and looking to transition commercial advancements to countermeasure adversarial advancements to disrupt, degrade, and deny warfighter communications in the EW battlefield.

What capabilities of ours are adversaries looking to degrade?

Adversaries are focused on degrading or denying our capabilities across the board including command and control (C2) capabilities, making communications a critical attack vector. By targeting communication capabilities, adversaries aim to disrupt the flow of information, sow confusion, and undermine decision-making processes. NIWC Atlantic and JTNC established the RIVAL Lab to characterize communication technologies against detection, degradation and interception techniques. This characterization enables the identification of possible vulnerabilities and capability improvements.



Sullivan's Island, SC (April 16, 2025), Naval Information Warfare Center (NIWC) Atlantic and Naval Surface Warfare Center, Crane Division (NSWC Crane) completed a week of intensive research and communications testing called "Southern Lightning" involving unmanned autonomous systems off the coast of Sullivan's Island in partnership with U.S. Fleet Forces Command. (U.S. Navy photo by Joe Bullinger/Released)

DoD resiliency facilities (engineering and T&E), like NIWC Atlantic's RIVAL Lab, are identifying, testing, adapting and looking to transition commercial advancements to countermeasure adversarial advancements to disrupt, degrade, and deny warfighter communications in the EW battlefield.

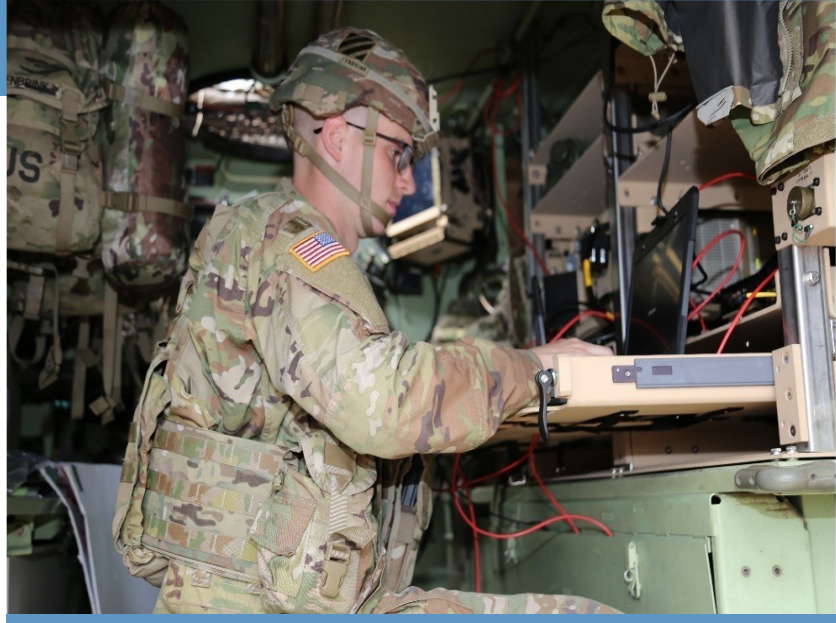
What does the military need to do to stay ahead of these threats?

The DoD must continue prioritizing and investing in a multi-faceted approach for identifying, evaluating and integrating resilient communication innovations that sustain effective communications under congested, constrained and contested environments. Similar to the investments made by NIWC Atlantic and JTNC for the RIVAL Lab, DoD investments should continue collaborating with industry and academia to leverage emerging commercial technologies such as Low Probability of Anything (LPx), artificial intelligence (AI), machine learning (ML), RF agility techniques to enhance electromagnetic spectrum operations (EMSO). The RIVAL Lab is one

example of a Department of the Navy capital investment for characterizing evolving TRANSEC features for operational maturity.

What's the state of our Anti-Jam and LPD capabilities?

The state of our Anti-Jam and LPD capabilities is promising, but continued investment in R&D and rapid fielding is essential to ensure these technologies are warfighter ready. In recent years, the defense industry has witnessed significant advancements in resilient communication technologies that incorporate robust transmission security (TRANSEC) features, including Anti-Jam and Low Probability of Detection (LPD) protections. While many of these capabilities are still in early Technology Readiness Levels or derived from commercial technologies, efforts are underway to mature and transition them to operational use for the warfighter as quickly as possible. By prioritizing collaboration between the DoD Programs of Record, industry, and research institutions; we can accelerate the critical capabilities to maintain operational superiority in the contested environments (EW battlefield).



Spc. Elijah Tenbrink, an Army intelligence analyst Soldier assigned to the Mustang Squadron, 6th Squadron, 8th Calvary Regiment, 2nd Armored Brigade Combat Team, 3rd Infantry Division, leverages the upper tactical internet to conduct mission command and network communications during the Army's three-week Armored Formation On-The-Move Network Pilot at Fort Stewart, GA, Feb. 7, 2022. (U.S. Army photo by Amy Walker, Project Manager Tactical Network, PEO C3T Public Affairs)

What are the various methods used by the DoD to address EW like frequency hopping and spread-spectrum?

Like commercial industries, the DoD employs several technologies to enhance communication capacity, performance, reliability and survivability. The DoD EMS strategy aims to enhance TRANSEC by reducing the likelihood of RF energy detection and impacts of interference using techniques like frequency hopping, spread spectrum, multiplexing, adaptive modulation, and dynamic spectrum access.

Similar to the Services tasking their respective research laboratories to investigate technology advancements, JTNC tasks the RIVAL Lab to characterize COTS and NDI innovations that often combine TRANSEC techniques to increase robustness or obfuscate detection. Recent RIVAL Lab investments have focused on enhancing emulated RF environments and expanding RF measurement technologies to better characterize advanced signal processing and software defined radio technologies without restricting the System Under Test's (SUT) capabilities to support the T&E infrastructure.

What are your thoughts on present-day Anti-Jam/LPD techniques? How have some of those techniques like spread spectrum become compromised over time, such as in a reduction in data rates?

Resiliency features like anti-jam and LPD for communications are continuously evolving and require creativity, innovation and adaptation to survive the EW battlefield. While significant communication advancements have been made, the increasing sophistication of adversaries, coupled with the legacy technology limitations (frequency hopping and spread spectrum techniques were introduced 50+ years ago) and understanding the system performance tradeoffs with employing TRANSEC techniques, effective resilient communications will face ongoing challenges. Identifying these challenges and understanding how they impact CONOPS with current and future communications is crucial for maintaining a competitive advantage.

DoD Working Groups, like JTNC's Resiliency Sub-Working Group (RSWG), work with warfighters, intelligence communities, industry partners, and DoD T&E facilities (like the RIVAL Lab) to better analyze communication resilience based on threats and operationally relevant environments to ensure real-world effectiveness.

By prioritizing collaboration between the DoD Programs of Record, industry, and research institutions; we can accelerate the critical capabilities to maintain operational superiority in the contested environments (EW battlefield).

Operational effectiveness requires more than specifications; it requires understanding the realities of performance tradeoffs associated with employing TRANSEC techniques and exercising these capabilities to validate end user needs are met. TRANSEC can impact data throughput and range, requiring a balance between stealth, operational effectiveness and survivability.

Where do LPD systems fit in within this conversation?

Detectability comes in many forms such as visual, acoustic, infrared (thermal) and electromagnetic. Since the RIVAL Lab is a radio T&E facility, LPD characterization primarily revolves around characterizing electromagnetic detectability.

Depending on the phase of war, LPD features can be central to ensuring resilient and secure communications in contested environments. Minimizing the RF signatures against energy, structure and imperfection detectors reduces the adversary's ability to target communications to disrupt C2. Think of it this way: LPD can be the first line of defense in a signals-based kill chain. Detection is the critical first step before the other sides can geolocate, intercept, identify/classify, or jam. Breaking the adversary kill chain as early as possible using TRANSEC enabled mitigations while maintaining effective (reliable) communications is critical in preventing detection, geolocation and targeted jamming in the EW battlefield.

LPD is more than a TRANSEC feature; it's a fundamental requirement for maintaining operational superiority. Characterizing the systems through rigorous testing is essential for determining limitations and strengths of different LPD approaches and providing independent analysis to enable informed decision-making about system acquisition and deployment. The RIVAL Lab is set up to characterize detectability across a range of SDRs and sensors.

What are your thoughts on current acquisition requirements around Anti-Jam and LPD capabilities for military communications systems? Are they reflective of the current need, and what do they typically look like?

Requirement development for system acquisition is evolving, and it is critical that it addresses performance as well as aspects such as Size, Weight, and Power (SWaP), security, and interoperability. As for resiliency related specifications, this topic has been at the forefront for the efforts of the JTNC's Resiliency Sub Working Group (RSWG) under the DoD CIO and Joint Staff J6 chartered Communications Technology and Waveform Working Group (CTWWG).

JTNC's RSWG works across various communities, including acquisition offices, industry, warfighter groups, and intelligence centers to better understand emerging technologies and desired capabilities in support of defining testable requirements. Acquisition requirements for AJ and LPD capabilities are evolving to reflect the growing complexity of EW threats. These requirements emphasize resilience, adaptability, and interoperability.

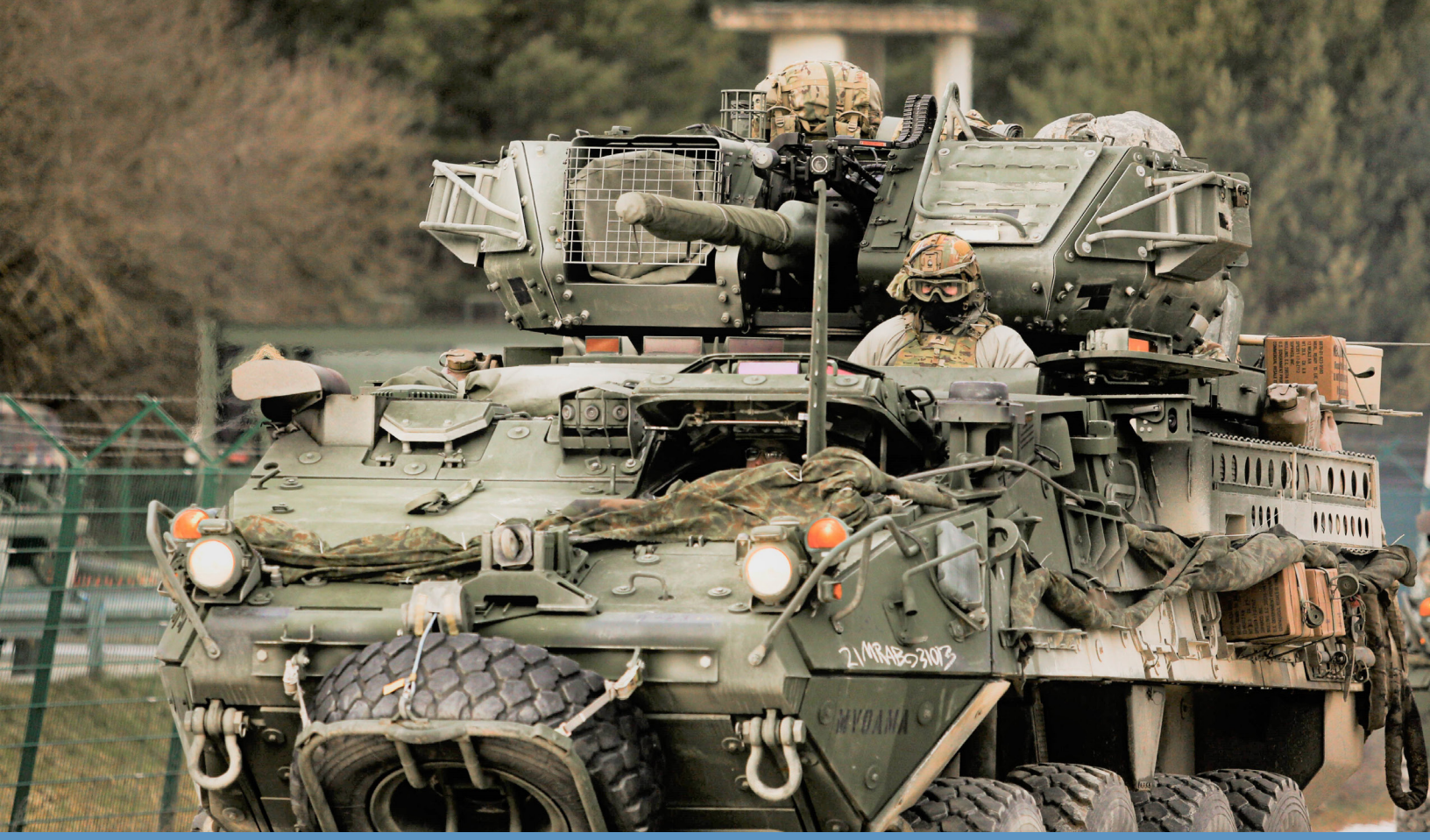
However, resiliency needs and definitions are different for each tactical domain (sea, ground, air, space) and also unique based on the environment (urban, mountain, desert, foliage). Characterizing a system's resiliency performance is highly influenced by context and tradecraft. Resiliency analysis from a ground-based line-of-sight (LoS) T&E facility will not completely align with results from maritime beyond LoS T&E facility. Context matters!

Tell us about the work you are doing on testing comms systems that can mitigate EW threats. How do you go about doing this work?

In partnership with JTNC, NIWC Atlantic's Resiliency Innovation & Vulnerability Assessment for LPx (RIVAL) lab represents a crucial investment in enhancing the DoD's ability to characterize resilient communication systems. The lab delivers results that enable better informed acquisition decisions and requirements development. This lab offers a platform and system-agnostic approach vital for evaluating a broad spectrum of military communication systems.

The RIVAL Lab aligns with JTNC's RSWG Assessment, Analysis, Test & Evaluation model to ensure a consistent approach to capability characterizations, EW resiliency T&E, and threat-informed EW T&E. The RIVAL Lab emphasizes deriving meaningful resiliency criteria based on use case, technology, and operational relevance. As a result, the lab provides actionable intelligence for data-driven decision-making and improved capabilities necessary for success in contested environments.

JTNC's Capability Characterization initiative focuses on characterizing innovative solutions from commercial vendors and NDI vendors who can provide operational impacts to the warfighter. Candidate products can range in Technology Readiness Level from prototype to field ready system. Through JTNC's sponsorship, the characterization events are free to product owners; but the final reports are posted to JTNC's Joint Communication Marketplace for use by a broad swath of US military agencies. Capability vendors and developers are encouraged to participate as much as possible and they are provided with the final reports as well.



The 2nd Cavalry Regiment (2CR) recently completed its annual Dragoon Ready exercise at the Joint Multinational Readiness Center in Hohenfels, Germany, designed to ensure combat readiness for the unit. The exercise also served as the second Integrated Tactical Network operational testing event (Ops Demo Phase II) for Capability Set (CS) 23, which demonstrated the latest version of networked communications between the command post, Strykers and dismounted troops. (U.S. Army Photo/Spc. Micah Wilson)

What is top of mind right now in this work?

What is at the top of our mind is getting the right capabilities to our joint warfighters so they are prepared and protected against our near peer adversaries.

What are the demand signals you are now getting on what you should be working on?

The demand signals we're seeing are being shaped by the accelerating shift toward Joint All-Domain Command and Control (JADC2), the need for resilient, interoperable communications in contested environments, and the growing emphasis on coalition interoperability.

Stakeholders, from the Combatant Commands COCOMs to Program Executive Offices (PEOs) and industry partners, are driving requirements for secure, software-defined, standards-compliant networking capabilities that can scale across services and mission profiles.

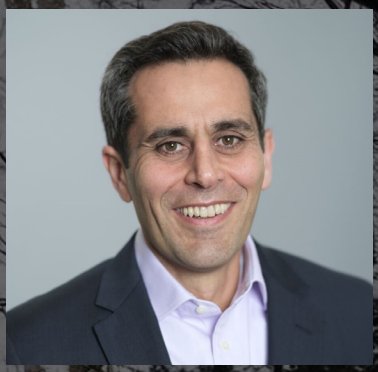
How are the results of your work shared with the DoD and industry?

Through partnership with JTNC, the RIVAL Lab conducts evaluations on resilient comms products developed by industry. This gives us the opportunity to directly engage with vendors. The RIVAL Lab posts the reports for US Government military and civilian access, which include DoD stakeholders, including program managers, system developers, and operational units.

The RIVAL Lab makes diligent efforts to have vendors participate throughout their product's evaluation event, including a post event sit-down to discuss results and findings. Additionally, the RIVAL Lab periodically briefs industry during JTNC RSWG Industry Technical Exchange Meeting (TEM). This allows the RIVAL team to present resiliency evaluation techniques and results to key industry stakeholders at the appropriate classification level.

VIEWPOINT FROM SILVUS TECHNOLOGIES

ADVANCING EW-RESILIENT COMMUNICATIONS THROUGH PARTNERSHIP AND INNOVATION



Silvus Technologies CEO and founder, Babak Daneshrad.

Across today's contested electromagnetic battlespace, maintaining assured connectivity is a shared priority for the Department of Defense, its research laboratories, and industry partners. Companies such as Silvus Technologies continue to collaborate closely with DoD organizations such as NIWC Atlantic, JTNC, and other warfighting labs to accelerate development and fielding of resilient tactical communications technology that incorporate next-generation EW defenses. These joint efforts are helping shape measurable, threat-informed resiliency standards and performance metrics to ensure mission-critical C2 systems can thrive – not just survive – in contested environments.

As adversarial EW threats grow in sophistication, today's operational environments demand advanced, multi-layered adaptive approaches capable of rapidly detecting, avoiding and mitigating jamming threats – without compromising data throughput or network performance.

Silvus Technologies has developed Spectrum Dominance – an expansive suite of Low Probability of Intercept/Low Probability of Detection (LPI/LPD), Anti-Jam (AJ) and Advanced Threat Protection (ATP) capabilities designed to deliver robust protection against EW threats.

Through the use of neural networks, these capabilities can sense their operational environment, adapt in real-time and deploy the optimal mix of EW defense techniques – dynamically and automatically. Future enhancements will further strengthen these capabilities through deeper integration of AI and machine learning for intelligent spectrum sensing and real-time adaptation.

Breaking Defense spoke with Silvus Technologies CEO and Founder Babak Daneshrad about the urgent need for tactical communication systems to integrate a diverse array of advanced LPI/LPD and Anti-Jam capabilities, and how Silvus is empowering the warfighter to maintain critical connectivity and achieve decision overmatch across the most contested domains.

Breaking Defense: How does Silvus view the Pentagon's efforts to strengthen resilient communications against modern electronic warfare threats?

Daneshrad: The DoD's recent progress through NIWC Atlantic's RIVAL Lab and JTNC's Resiliency Sub-Working Group represents a major step toward characterizing EW resilience – but ensuring that progress translates into acquisition standards is the next critical frontier. Silvus is proud to be part of this shared effort – working side-by-side with DoD stakeholders to evaluate, mature, and operationalize the next generation of Anti-Jam and LPI/LPD capabilities.

Our mission is to deliver next generation communications technology to the warfighter – empowering them to achieve RF spectrum overmatch. By integrating feedback from DoD testing environments together with direct feedback from operational users on the frontlines, we're continuously refining our technologies to ensure they meet mission demands – extending connectivity across complex terrain, ensuring C2 interoperability across joint and coalition networks, and enabling resilient communications solutions that that enable the warfighter to achieve their mission objectives even under electronic attack.

What do you see as the keys to maintaining a technological edge in the electromagnetic spectrum?

As near-peer adversaries continue to advance their EW capabilities, it's imperative to outpace that evolving threat – setting an innovation pace that adversaries cannot match. The key is proactive innovation that moves beyond reacting to new threats and instead anticipates them – leveraging data from field exercises, laboratory evaluations, and live operations to inform future capabilities.

At Silvus, we align our R&D roadmap closely with DoD priorities, scaling to meet emerging and predictive threat intelligence while investing in cognitive communications technology that can autonomously counter new EW

challenges. Congress can help bridge this final gap to ensure the U.S. maintains spectrum superiority not just in the lab, but on the battlefield.

What specific technical capabilities or approaches does Silvus have to provide better protection against EW effects compared to current solutions in the market?

Traditional techniques such as frequency-hopped-spread-spectrum (FHSS) have limitations in that they force a drastic reduction in data rate in order to withstand jamming, which in many cases could lead to mission failure. Silvus takes a different approach. We view LPI/LPD and Anti-Jam resilience as a multi-tiered problem – one that demands different tools, applied dynamically based on the threat environment. In response, we developed 'Spectrum Dominance' – an-ever expanding suite of LPI/LPD, Anti-Jam, and Advanced Threat Protection capabilities that provide a layered, adaptive defense against advanced EW threats.

What truly sets Silvus apart is that Spectrum Dominance delivers these advanced EW resiliency capabilities without sacrificing range, throughput or network robustness – even in highly congested and contested environments.

The first layers are dedicated to LPI and LPD covertness through dynamically adaptive techniques that conceal or reduce StreamCaster MANET radios RF signature – increasing tactical survivability by avoiding adversarial detection.

If an adversary attempts to interfere or jam communications, StreamCaster MANET radios leverage their built-in spectrum analyzer to perform real-time interference monitoring across the network both in frequency and geography. Upon detection of interference, MANET Interference Avoidance (MAN-IA) automatically moves the entire network to the cleanest frequency, without user intervention – maintaining network connectivity.

MANET Interference Cancellation (MAN-IC) takes a different approach. This capability samples the offending signal, characterizes its spatial profile and applies a null in the digital domain – effectively cancelling the jamming signal while preserving communications continuity.

How is Silvus Technologies responding to the evolving EW threat challenge?

At Silvus, we never stop innovating communications technology for the tactical edge. Through sustained internal research and development, we continuously advance our communications technologies to deliver class-leading performance to our customers. Our engineering teams are relentless in pushing the boundaries of what's possible, while our support teams ensure that our customers and end-users can operationalize these capabilities to meet their evolving mission demands.

Today's modern battlespace is more distributed, mobile and interconnected than ever before – with tactical networks fusing forces, sensors and decision makers at mission speed. This increased C2 interconnectivity enhances situational awareness and combat effectiveness, but also introduces new vulnerabilities that adversaries will actively seek to exploit through SIGINT and jamming attacks.

That's why we're working to stay out in front of the emerging EW threat landscape now and for the future. Today, Silvus' Spectrum Dominance suite of advanced LPI/LPD, Anti-Jam and Advanced Threat Protection capabilities utilize neural networks that analyze spectrum conditions and dynamically apply defensive countermeasures. These aren't lab experiments – they're deployed, operationally proven technologies that deliver real-world survivability against modern EW threats. For the future, we're moving toward fully cognitive radios that utilize AI and machine learning to continuously learn, predict and neutralize evolving threats autonomously – ensuring a decisive advantage in tomorrow's electromagnetic fight.

The threat is here, the technology is ready and with Spectrum Dominance, Silvus is delivering next-gen EW defenses built for the evolving battlespace.

SILVUS TECHNOLOGIES
a Motorola Solutions Company

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