TechNet Augusta

August 17–20, 2026 | Augusta Marriott at the Convention Center | Augusta, GA

2026 SOLUTIONS SHOWCASE

AFCEA TechNet Augusta 2026 Solutions Review

The theme of this year's TechNet Augusta conference is "command and control (C2)/counter-C2 in support of Army and joint warfighting." This three-day event provides a forum for government, military and academia leaders and industry experts to discuss issues related to cyber electromagnetic activities and unified land operations. This year, speakers will focus conversations on the enhancement of warfighting outcomes by accelerating the delivery of innovative and interoperable systems. Advanced C2 and counter-C2 capabilities are critical in joint operational environments where decisive action is needed.

To seek out solutions to the U.S. Army's emerging and existing challenges presented by the ever-changing threat landscape, The Army Cyber Center of Excellence presented 10 problem statements for companies to address. This Solutions Review Compendium features industry experts' innovative solutions to problems like synthetic access breaches, cryptographic threats and operating in disconnected, low-bandwidth environments. The top solutions will be presented in the engagement theater at TechNet Augusta.

This year's conference will deepen the military and private-sector partnerships required to deliver innovative capabilities with unprecedented speed and efficiency.

The content within this compendium offers a diverse range of perspectives and technological solutions, inspiring future Army innovation.

Best wishes,

Lt. Gen. Bruce Crawford, USA (Ret.)
President and CEO
AFCEA International

Problem Statements

Problem Statement 1: How can quantum-accelerated optimization be integrated into electromagnetic warfare (EW) and combat systems for real-time threat analysis in GPS-denied environments?

Problem Statement 2: How can we unify fragmented networks, platforms and radio systems into a single cohesive infrastructure that preserves individual functionalities while delivering automated PACE routing, dynamic mesh management, intelligent QoS and centralized boundary security?

Problem Statement 3: How can we develop validated, resilient machine-to-machine (M2M) security protocols to prevent "synthetic access" breaches driven by autonomous agentic AI?

Problem Statement 4: How can we deliver resilient, agile systems that seamlessly unify electronic protection, support and attack capabilities to dominate the electromagnetic operational environment (EMOE) across all domains?

Problem Statement 5: How can we harden existing command and control networks against next-generation cryptographic and algorithmic threats, including advanced digital signature forgery?

Problem Statement 6: How can we provide high-performance algorithmic execution and tactical database replication at the edge within a ruggedized form factor capable of surviving disconnected, low-bandwidth operations?

Problem Statement 7: What are the best techniques for real-time optimization in logistics, resource allocation and autonomous swarm management across contested networks?

Problem Statement 8: How can we deliver intuitive, error-resilient user interfaces that minimize operator cognitive load through automated combat workflows and streamlined UX/UI, allowing tactical teams to focus on high-level combat reasoning rather than menu navigation?

Problem Statement 9: How can a singular combat network integrate disparate command structures and sensors while minimizing cognitive burden and maximizing network observability through smart flow management and CMOSS/SOSA compliance?

Problem Statement 10 – Information Advantage: How can we integrate visual imagery, virtual reality (VR) and spatial imagery tools into command post C2 workflows to enhance situational understanding, operational visualization and collaborative decision-making?

Problem Statement 10 – DCO: What technology exists, or is in development, that the U.S. Army has not yet experimented with, that could be a “game changer” for assured voice and data communications at echelon?

Table of Contents

Submissions

Quantifying Zero Trust Readiness: A Risk-Based Model for Accelerating Federal Adoption

William Johnson, Chief of Software Product Delivery, Tensley Consulting Inc. •
will.johnson@tensleyconsulting.com

ABSTRACT

Federal agencies and military organizations face an unprecedented challenge: achieving full zero trust (ZT) adoption by the fiscal year 2027 end-of-year mandate while maintaining mission availability, operational continuity and security at scale. Traditional checklist-driven approaches have proven insufficient for environments where strict access controls can disrupt critical operations, modernization budgets are constrained and workforce capacity is already stretched thin. These challenges are amplified in operational technology (OT) environments, where legacy systems, safety-critical processes and limited downtime windows make zero-trust implementation uniquely complex.

This presentation introduces the Zero Trust Risk Based Objective Assessment Methodology (ZT ROAM), a quantitative solution designed to help agencies prioritize investments, measure ZT readiness and validate progress through outcomes rather than compliance artifacts. By integrating mission impact, risk exposure, architectural maturity and operational constraints into a unified scoring model, this automated assessment process enables leaders to make quick, defensible, data-driven decisions about where to focus limited resources. It also provides a structured path for aligning IT and OT zero-trust efforts, reducing implementation friction and accelerating transformation without compromising availability.

BIO: William Johnson is a seasoned cybersecurity executive and decorated military veteran with more than two decades of experience securing national interests and pioneering digital resilience across the public and private sectors. A proud native of Tennessee, Johnson served in the U.S. Army for 11 years as a signal officer and holds two degrees, a Master of Science in information technology and a Bachelor of Business Administration.

During his military career, Captain Johnson held pivotal roles, including forward-deployed signal officer with the 2nd Infantry Division during Operation Iraqi Freedom, company commander with the 15th Signal Brigade at Fort Gordon and communications adviser to the Malian Army. His strategic leadership extended to national defense efforts as a military liaison at the National Security Agency (NSA) and as chief of the Network and Cybersecurity Operations Centers with Joint Task Force Guantanamo Bay (JTF GTMO).

Johnson continued shaping cyber defense policy and infrastructure as a cyber operations planner at U.S. Cyber Command and later as senior cybersecurity engineer at the U.S. Department of

Defense Consolidated Adjudications Facility. His expertise deepened through contracted roles at NSA's Cybersecurity Directorate and the Cybersecurity and Infrastructure Security Agency (CISA), where he managed critical information security programs.

Today, Johnson serves as chief of Software Product Delivery for ZT ROAM, an automated zero-trust assessment platform developed by Tensley Consulting Inc., where he leads innovation in IT and OT architecture security. Johnson spoke earlier this year at TechNet Cyber in Baltimore where he presented: "Zero Trust in Operational Technology: Adapting Modern Security Frameworks for Legacy Industrial Environments."

Adversarial AI Attacks and How To Mitigate Them

Tommy Gardner, Chief Technology Officer, HP Federal, HP Inc. ·
thomas.gardner@hp.com

ABSTRACT

As most agencies in government are rushing to take advantage of new AI capabilities, are we considering how these new systems will be attacked by our adversaries? The style and methods of the attacks on AI programs and capabilities are far different from the conventional attacks we see today. Will the U.S. Air Force and U.S. Space Force be ready? Will they have the proper defense and mitigation?

How will your AI systems be attacked by adversaries? Are your defenses ready? Will you be able to detect the subtle methods, tactics and procedures being used? These attacks are not necessarily trying to shut down the system but cause you to make bad decisions in specific circumstances.

There is no AI without data. Data collection involves serious risk of bias and compromise. If training data is manipulated, your results may show a bird as a plane. It almost takes Superman to distinguish what went wrong.

This talk will first cover types of data and model poisoning. Then it will broaden out into the AI attacks on the supply chain. Finally, it will touch on how to detect and mitigate these new kinds of attacks.

- Defending enterprise AI against subtle adversarial attacks
- Analyzing various types of data and model poisoning designed to influence corporate decision-making
- Identifying how adversaries manipulate training data to create persistent and subtle behavioral biases
- Exploring the expanding threat landscape of AI supply chain attacks targeting third-party libraries and models
- Implementing advanced detection methods and provenance tracking to identify compromised datasets
- Strategies for mitigating adversarial AI risks through continuous red teaming and runtime monitoring

This talk is a condensation of a 14-week course taught to graduate students at Catholic University. The objective is to warn and prepare the students about this new wave of attacks on AI programs and systems.

BIO: Tommy Gardner is HP's chief technology officer for HP Federal, spanning U.S. federal agencies, higher education, K-12 education, state and local government customer segments, as well as federal systems integrators. His current responsibilities include technology leadership, strategic technology plans, product and technology strategies, sales force technical support, and customer and partner relationships.

Gardner has served as the chief technology officer for Jacobs Engineering, Scitor and MANTECH. Earlier in his career, he was a senior technical executive at Raytheon. In the U.S. Navy, he served as the deputy for science and technology for the chief of naval research. He oversaw the Navy's Deep Submergence Program as well as its Advanced Technology Program. He also commanded the nuclear submarine, USS San Juan (SSN 751).

Gardner's educational background covers multiple disciplines and fields of interest including cybersecurity, data science, blockchain, quantum information science, artificial intelligence, high-performance computing and systems integration in government markets.

Gardner holds a B.S. in mechanical engineering from the U.S. Naval Academy, a master's degree in public administration from Harvard University, an M.S. in management of technology from MIT and a Ph. D. in energy economics from George Washington University. He is a professional engineer, an ASME fellow and serves as chair of the ASME Industry Advisory Board.

Gardner was awarded as the public Chief Technology Officer of the Year for 2021.

Post-Quantum Cryptography (PQC): Are You Ready?

Tommy Gardner, Chief Technology Officer, HP Federal, HP Inc. ·
thomas.gardner@hp.com

ABSTRACT

As billions of dollars are invested each year by the United States, its allies and adversaries are developing cryptographically relevant quantum computer (CRQC) systems. Are we taking the best steps now to protect our data and secure transmissions?

The National Institute of Standards and Technology (NIST) has spent a decade analyzing potential replacements of RSA and elliptic curve cryptography (ECC) for the day a CRQC becomes workable. While that date is estimated to be around 2030, the adversary has a strategy of harvest now, decrypt later. For example, while RSA 256 encryption was designed to be protected against a brute force hack for 100 years, if in four years a CRQC is in the hands of our adversaries, our encrypted data could all be read then, if we don't change our primary encryption methodology.

NIST took more than 125 submissions of new methods of encryption and in August 2024 released new standards for three algorithms to be used for post-quantum computing. This talk will cover the basic knowledge needed to understand the key encapsulation mechanisms, digital signatures and the mathematical foundations involved. It will also describe why, in addition to the new algorithm standards, your hardware has to be designed to incorporate the new PQC standards. The administration is looking very hard at this problem and expects specific guidance and direction. The sooner you implement the changes, the better protected you will be.

BIO: Tommy Gardner is HP's chief technology officer for HP Federal, spanning U.S. federal agencies, higher education, K-12 education, state and local government customer segments, as well as federal systems integrators. His current responsibilities include technology leadership, strategic technology plans, product and technology strategies, sales force technical support, and customer and partner relationships.

Gardner has served as the chief technology officer for Jacobs Engineering, Scitor and MANTECH. Earlier in his career, he was a senior technical executive at Raytheon. In the U.S. Navy, he served as the deputy for science and technology for the chief of naval research. He oversaw the Navy's Deep Submergence Program as well as its Advanced Technology Program. He also commanded the nuclear submarine, USS San Juan (SSN 751).

Gardner's educational background covers multiple disciplines and fields of interest including cybersecurity, data science, blockchain, quantum information science, artificial intelligence, high-performance computing and systems integration in government markets.

Gardner holds a B.S. in mechanical engineering from the U.S. Naval Academy, a master's degree in public administration from Harvard University, an M.S. in management of technology from MIT and a Ph. D. in energy economics from George Washington University. He is a professional engineer, an ASME fellow and serves as chair of the ASME Industry Advisory Board.

Gardner was awarded as the public Chief Technology Officer of the Year for 2021.

Hardware Zero Trust

Tommy Gardner, Chief Technology Officer, HP Federal, HP Inc. •
thomas.gardner@hp.com

ABSTRACT

Zero trust is a philosophy and method used to secure systems and data. The focus has primarily been on identity management or one software security. This talk will discuss the need for hardware zero trust and the need for a hardware and firmware certification to achieve the optimum security of your systems and data. NIST SP 800-207 defines the specifics of a zero-trust effort. Often the hardware and firmware component of a system are taken as a given because of the many years between replacement.

Software and hardware must work together in any system. Understanding the level of security that your hardware provides is important in optimizing the overall protection.

NIST SP 800-193 on hardware resilience provides a good starting point. Working this through the hardware system design for a root of trust and a trusted compute module in light of the DOW zero-trust program office's pillars can bring insight into the need for a hardware evaluation of zero trust. This talk will bring everyone up to date on the discussions with the DOW, the services, DISA and NSA on the subject.

BIO: Tommy Gardner is HP's chief technology officer for HP Federal, spanning U.S. federal agencies, higher education, K-12 education, state and local government customer segments, as well as federal systems integrators. His current responsibilities include technology leadership, strategic technology plans, product and technology strategies, sales force technical support, and customer and partner relationships.

Gardner has served as the chief technology officer for Jacobs Engineering, Scitor and MANTECH. Earlier in his career, he was a senior technical executive at Raytheon. In the U.S. Navy, he served as the deputy for science and technology for the chief of naval research. He oversaw the Navy's Deep Submergence Program as well as its Advanced Technology Program. He also commanded the nuclear submarine, USS San Juan (SSN 751).

Gardner's educational background covers multiple disciplines and fields of interest including cybersecurity, data science, blockchain, quantum information science, artificial intelligence, high-performance computing and systems integration in government markets.

Gardner holds a B.S. in mechanical engineering from the U.S. Naval Academy, a master's degree in public administration from Harvard University, an M.S. in management of technology from MIT and a Ph. D. in energy economics from George Washington University. He is a professional engineer, an ASME fellow and serves as chair of the ASME Industry Advisory Board.

Gardner was awarded as the public Chief Technology Officer of the Year for 2021.

Intersection of AI and Security

Gina Scinta, Deputy Chief Technology Officer, Thales Trusted Cyber Technologies •
gina.scinta@thalestct.com

ABSTRACT

AI is rapidly reshaping the operational environment, accelerating decision-making and transforming how missions are executed across all domains. As AI capabilities evolve, adversaries are increasingly leveraging AI to disrupt, deceive or degrade U.S. and allied operations. Ensuring secure and trustworthy AI is now essential to maintaining information dominance and mission assurance.

This session examines the critical security issues at the intersection of AI and defense operations. The speaker will address:

- Countering the malicious use of AI by criminal actors, terrorists and hostile nation-states seeking to automate attacks, conduct influence operations or compromise military systems.
- Identifying and mitigating adversarial attacks designed to deceive or manipulate AI models by exploiting model weaknesses, training pipelines or operational data flows.
- Protecting the high-value data that fuels AI systems, ensuring its integrity, confidentiality and availability in contested, denied or degraded environments.
- Employing AI to strengthen cybersecurity, enhancing early threat detection, improving automated defense responses and increasing resilience across defense information systems.
- Implementing security architectures and access-control protocols specifically designed to defend against “synthetic access” exploits generated by autonomous agentic AI.

BIO: Gina Scinta, deputy CTO, serves as the company’s technology evangelist. She helps our U.S. federal government customers learn effective ways to solve their mission-critical cybersecurity challenges. Scinta has more than 30 years of experience in the technology community.

Best Practices for Implementing Quantum-Resistant Security

Gina Scinta, Deputy Chief Technology Officer, Thales Trusted Cyber Technologies •
gina.scinta@thalestct.com

ABSTRACT

The time is now to start the transition to quantum-safe cryptography. The military must modernize outdated cryptographic solutions and adopt NIST-approved post-quantum cryptography (PQC) algorithms by the end of 2030. A critical challenge in this transition is addressing how to harden existing command and control networks against the quantum threat.

To migrate efficiently, agencies must understand the evolving quantum threat landscape and the government and industry initiatives designed to mitigate associated risks. The November 2025 DOW memorandum, "Preparing for Migration to Post Quantum Cryptography," outlines the necessary steps for migration and underscores security, interoperability and department-wide coordination for PQC implementations.

This presentation will discuss best practices for the migration to quantum-resistant security including:

- Designating PQC migration points of contact to ensure a successful migration.
- Utilizing crypto inventory tools to learn where and how encryption is currently deployed within an agency's infrastructure.
- Prioritizing existing infrastructure for migration to post-quantum cryptography.
- Leveraging guidance from National Security Memorandum 10 and NCCoE's Migration to Post-Quantum Cryptography Project.
- Deploying crypto-agile solutions for PKI, data-at-rest and in-transit, and identity and access management.
- Applying a cryptographic bill of materials (CBOM).

BIO: Gina Scinta, deputy CTO, serves as the company's technology evangelist. She helps our U.S. federal government customers learn effective ways to solve their mission-critical cybersecurity challenges. Scinta has more than 30 years of experience in the technology community.

Hardening the Tactical Edge: Mission-Ready Cybersecurity From Core to Battlefield

Gina Scinta, Deputy Chief Technology Officer, Thales Trusted Cyber Technologies • gina.scinta@thalestct.com

ABSTRACT

Core computing capabilities once confined to data centers and cloud environments are now being pushed to the tactical edge to support time-critical operations. As this shift accelerates, the U.S. Department of War must ensure that data protection and cybersecurity controls transition seamlessly alongside compute capabilities.

However, extending enterprise-grade security to the edge presents significant challenges. Harsh and unpredictable environments; bandwidth-limited or disconnected operations; hostile or overrun scenarios; and stringent size, weight and power (SWaP) constraints all complicate efforts to maintain confidentiality, integrity and availability in forward-deployed systems.

True mission assurance requires data protection to extend all the way to the edge—without degrading operational tempo or limiting warfighter agility. This session will provide practical guidance for applying the same level of security used in core and cloud infrastructures to tactical edge environments. Topics will include:

- Strategies for addressing environmental, bandwidth and operational constraints unique to the edge
- Approaches for extending existing cybersecurity architectures, tooling and zero-trust principles to forward-deployed systems
- The critical role of supply-chain security in safeguarding edge devices, sensors and mission systems

BIO: Gina Scinta, deputy CTO, serves as the company's technology evangelist. She helps our U.S. federal government customers learn effective ways to solve their mission-critical cybersecurity challenges. Scinta has more than 30 years of experience in the technology community.

Collective Edge Defense: Local Threat Detection and Telemetry for Disconnected Cyber Operations

Nishawn Smagh, Director of Intelligence, GreyNoise Intelligence • shawn@greynoise.io

ABSTRACT

The modern threat landscape is facing a critical inflection point. Advanced state-sponsored groups increasingly target edge devices, including firewalls, VPN gateways, routers, SD-WAN platforms and load balancers, to gain access and maintain persistence while avoiding traditional security controls. These attacks are often low-volume, highly targeted and designed to blend into normal internet traffic, making them difficult to detect.

At the same time, the exposure window continues to widen. Edge device exploitation frequently outpaces patching, leaving critical internet-facing infrastructure exposed to compromise.

The network edge remains a significant blind spot for many organizations due to limited security telemetry. Advanced adversaries exploit this visibility gap by conducting targeted reconnaissance and carefully crafted attacks long before traditional monitoring tools generate alerts. Defenders need visibility into adversary behavior before a breach occurs—not just indicators after the fact.

Project SWARM extends cyber defense to disconnected, contested and bandwidth-constrained environments through lightweight deception sensors deployed at the tactical edge. These sensors emulate real-world routers, VPN gateways, firewalls and other edge technologies, attracting adversary reconnaissance and exploitation attempts while capturing high-fidelity telemetry, including PCAPs, payloads, HTTP headers, TLS metadata and behavioral artifacts. Local processing enables threat detection and prioritization at the point of collection, while efficient synchronization allows intelligence to be replicated to centralized mission systems when connectivity becomes available.

By combining local collection with global threat intelligence, Project SWARM enables defenders to distinguish opportunistic internet noise from activity uniquely targeting their environment. The result is earlier warning, improved threat hunting and resilient cyber defense for government, military and critical infrastructure operators operating in disconnected and low-bandwidth environments.

BIO: Nishawn Smagh is a senior executive at GreyNoise Intelligence, where he provides strategic direction for the company's cybersecurity mission and helps shape its role in advancing

global threat intelligence. He works across core business functions to align innovation with operational impact, ensuring GreyNoise delivers actionable insights to both government and commercial partners.

A retired U.S. Air Force intelligence officer with 25 years of service, Smagh most recently served as director of intelligence for the Cyber National Mission Force at U.S. Cyber Command, leading intelligence operations for a 2,000-member joint command charged with deterring, disrupting and defeating malicious cyber actors. He previously served as director of intelligence for Ninth Air Force (Air Forces Central), overseeing all Air Force intelligence operations across the Middle East.

Throughout his Air Force career, Smagh commanded at the squadron, group and wing levels, directing intelligence, surveillance and reconnaissance operations across the Central, Indo-Pacific, Strategic and Cyber Command theaters. His joint assignments included leadership roles at U.S. Strategic Command and the Joint Functional Component Command for Global Strike, where he supported strategic deterrence and global targeting missions. His military decorations include the Defense Superior Service Medal, Legion of Merit (with oak leaf cluster), Bronze Star Medal and Defense Meritorious Service Medal.

Smagh is a graduate of the U.S. Air Force Academy and holds master's degrees in international relations and management. He completed professional military education at the U.S. Army Command and General Staff College and undertook senior development education at the Congressional Research Service, Library of Congress, where he supported congressional oversight and policy analysis on national security issues.

At GreyNoise, Smagh brings deep operational and intelligence leadership to the private sector, translating decades of national defense experience into actionable insights that help organizations understand their adversaries, anticipate threats and strengthen resilience in today's complex cyber environment.

Agentic AI for ISR Fusion and Automated Combat Decisioning

Paul Jojy, Manager, Forward Deployed Engineering, Johns Hopkins University •
paul.jojy@dominodatalab.com

ABSTRACT

Cognitive bandwidth is a finite resource, and too much of it is going toward managing AI systems rather than leveraging them. Domino is built to flip that equation.

We'll walk through an agentic AI workflow that fuses ISR detections with contextual mission data to automatically surface course-of-action recommendations for U.S. Army operators with every step logged and traceable. When the recognition model hits unfamiliar signatures, watch Domino flag the drift, trigger automated retraining and redeploy through a governed approval gate. The full cycle runs in days instead of months, reducing operator cognitive load and keeping mission teams focused on the decision rather than the process.

BIO: Paul Jojy is a subject matter expert in AI/ML and holds a graduate degree in artificial intelligence from Johns Hopkins University. He has led and implemented machine learning initiatives for deployed top-secret space programs with total contract values exceeding $1 billion. Jojy brings deep expertise in image processing, signal processing and generative AI deployment in air-gapped networks, and he has received enterprise-level awards for novel work in signal detection.

Disconnected-First Edge Computing for Tactical Execution and Data Replication

Raj Iyer, President of Tsecond.ai, Tsecond Inc. • raj.iyer@tsecond.ai

ABSTRACT

Modern tactical operations increasingly depend on the ability to execute algorithms, process mission data and replicate operational databases at the edge, often in environments where connectivity is intermittent, bandwidth is constrained and access to centralized cloud infrastructure is unavailable. Problem Statement 6 highlights a critical operational requirement: delivering high-performance algorithmic execution and tactical database replication in a ruggedized form factor capable of supporting disconnected and low-bandwidth missions.

Tsecond's BRYCK platform addresses this requirement by bringing petabyte-scale storage, edge AI acceleration and resilient data movement directly to forward-deployed environments. Designed for disconnected-first operations, BRYCK enables mission teams to capture, process, infer, replicate and synchronize data locally without waiting on reach-back connectivity. This allows algorithms to execute at the point of need, tactical databases to remain available across distributed teams and mission-critical data to be synchronized efficiently when bandwidth becomes available.

By combining compact SWaP-conscious hardware, high-performance compute and intelligent data orchestration, Tsecond enables a new model for edge infrastructure: one where operational data remains accessible, actionable and resilient even in DDIL environments. This capability is essential for accelerating decision advantage, supporting autonomous and AI-enabled workflows and ensuring continuity of operations across contested, remote and bandwidth-limited mission sets.

Through BRYCK, Tsecond provides a scalable edge foundation for mission partners who require secure, ruggedized, high-capacity infrastructure that can operate independently, replicate tactically and synchronize intelligently across the battlespace.

BIO: Raj Iyer brings more than 35 years of experience establishing and leading technology and business transformation organizations in both the private sector and government. Iyer is currently president of a high-growth Silicon Valley-based deep tech startup.

Trust No Agent: Quantifying Where Autonomous AI Breaks Before Adversaries Do

Tyler Hallmark, Vice President of Data Science, Seekr • thallmark@seekr.com

ABSTRACT

As the U.S. Army fields autonomous, agentic AI to operate at machine speed, a new class of risk emerges. "Synthetic access" describes breaches in which manipulated or compromised agents gain unauthorized machine-to-machine (M2M) access. Conventional security controls were never designed to anticipate how AI agents, and the models behind them, fail under adversarial pressure, leaving M2M protocols validated against yesterday's threats rather than tomorrow's.

SeekrBreakr closes this gap with a mathematical, science-based approach to AI model and agent pen-testing. By systematically breaking LLMs and agents to understand precisely how and where they fail, SeekrBreakr delivers neuron-level insight and quantified assessments of adversarial susceptibility, including the prompt-injection and agent-layer manipulation vectors that drive synthetic access. The result is an empirical, repeatable foundation for validating M2M security protocols, hardening models before deployment and continuously monitoring them in operation.

This session shows how quantified adversarial testing transforms agentic AI from an unbounded liability into a measured, defensible capability, giving program owners the evidence they need to certify resilient M2M trust and know where their agents are vulnerable before adversaries do.

Hardening C2: Post-Quantum Trust Fabrics Against AI-Driven Signature Forgery

Harley "Trip" Stowell III, Founder and Managing Partner, Eminence Grey •
stowell@eminencegrey.ai

ABSTRACT

Command and control (C2) is no longer a closed garden; it is an enterprise C2 estate stitched across clouds, data centers, air-gapped enclaves and coalition networks—exactly the terrain where next-generation cryptographic breaks and AI-assisted signature forgery become mission weapons, not theoretical risks. The question is not whether classical PKI and legacy algorithms will erode under quantum and frontier model pressure, but whether we can re-platform trust fast enough that a forged order, policy change or code artifact cannot quietly traverse the enterprise and redirect outcomes at scale.

This session proposes a practical architecture for hardening existing enterprise C2 against that class of threat by treating cryptography, provenance and anomaly detection as first-class mission systems, not compliance afterthoughts. At the core is a sovereign, post-quantum secure trust fabric that sits underneath today's applications and mission systems, providing cryptographic agility, symmetric PQ key management and selective inclusion segmentation across commands, data centers and partner networks. Digital signatures remain necessary but never sufficient: every signed order, workflow or software update is bound into a provenance graph that captures who issued it, from what enclave, under what policy and with what behavioral history, then continuously scored by AI agents trained to detect low signature anomalies in command patterns, credential use and cross-domain movement.

We will walk through how to retrofit this model into existing C2 estates without ripping and replacing core systems. That includes lifting critical C2 traffic off the open internet onto private optical fabrics with PQ-secured VPN overlays; inserting fabric-level policy enforcement at enterprise interconnects and cross-domain gateways; and deploying "trust defense" agents that can quarantine suspect credentials, degrade or deny questionable commands, and provide auditable reasoning traces to commanders in real time. The result is not a claim of perfect security but a measurable shift in adversary economics: enterprise C2 environments that are materially harder to map, persist in and exploit—even when the attacker can forge signatures, generate backdoored code or chain actions at machine speed.

BIO: Harley Stowell III—known to many as "Trip"—is a serial entrepreneur, architect of advanced cybersecurity and networking platforms, and founder and managing partner of Eminence Grey. With more than two decades at the forefront of enterprise cloud infrastructure and defense technology, Stowell has led the development of breakthrough platforms including Red Cell, a mobile emergency management system; LineSider, the first software-defined networking platform (acquired by Cisco in 2008); and StratOS, an autonomous, defense-in-depth cybersecurity framework.

Formerly the CTO for Service Provider Cloud at Cisco, Stowell played a pivotal role in shaping the evolution of network virtualization. At Sea Street Technologies, he pioneered an autonomous cybersecurity fabric designed for scalable, cloud-native deployment across mission-critical environments.

In addition to his commercial and technical leadership, Stowell is a committed advocate for national security and veteran causes. He serves on the board of OPTAC-X, supporting satellite-based augmented reality telehealth solutions for military and emergency response. Through his continued work with the Special Forces Trust and hands-on contributions to cutting-edge network security architecture, Stowell combines visionary technology leadership with a grounded commitment to service.

Reducing Cognitive Burden Through Intelligent Operational Insights

Bill Roberts, Federal Field CTO, Riverbed • william.roberts@riverbed.com

ABSTRACT

U.S. Army operations generate unprecedented volumes of data across networks, applications, endpoints, cloud environments, platforms and mission systems. While access to data continues to increase, operators are often challenged by fragmented information sources, competing priorities and the growing complexity of managing digital environments. As data volumes expand across tactical and enterprise environments, success increasingly depends on reducing cognitive burden by transforming vast amounts of operational data into clear, actionable insights that help operators identify what requires attention, understand potential mission impact and make data-driven decisions with greater speed and confidence.

This session will examine how modern approaches to AI-driven analytics, intelligent alerting, automated correlation, root cause analysis and intelligent prioritization can help reduce operator workload and improve operational effectiveness. By surfacing the most relevant information at the right time, reducing noise, identifying meaningful relationships across disparate data sources and accelerating issue identification, organizations can enable operators to quickly understand what is happening, why it is happening and what actions require attention without manually sorting through multiple systems and dashboards.

Attendees will gain practical perspectives on reducing complexity, improving resilience and supporting faster, more data-informed decision-making in increasingly dynamic and contested environments. The discussion will explore how intelligent operational insights can help commanders, signal personnel, cyber defenders and network operators focus on mission execution rather than data collection and troubleshooting, while improving situational awareness, prioritizing mission-critical issues and enabling smaller teams to effectively manage increasingly complex enterprise and tactical environments. Ultimately, organizations can transform growing volumes of operational data into actionable information that strengthens mission readiness and supports mission success.

BIO: Bill Roberts is the federal chief technology officer at Riverbed, where he advises government clients on optimizing their IT investments. With more than 20 years of experience, he helps agencies modernize IT operations and improve mission resilience.

Wireless as an Attack Surface: Surveillance, Deception and Access

Brett Walkenhorst, CTO, Bastille Networks • noe@sacocopr.com

ABSTRACT

Wireless technologies are emerging as a critical, and often underappreciated, attack surface in defensive cyber operations. Capabilities once limited to advanced intelligence services, such as network impersonation, mobile device exploitation and persistent location tracking, are now more accessible, lower cost and increasingly adopted by a broader range of actors. This shift has direct implications for how adversaries conduct surveillance, identify targets and exploit operational vulnerabilities in both public and controlled environments.

This practitioner-focused session examines how attackers exploit the assumption that connectivity itself can be trusted to enable surveillance, deception and operational access. Drawing on field experience with wireless monitoring systems deployed across diverse customer environments, as well as case studies from publicly reported incidents, the presentation explores techniques including rogue base stations (IMSI catchers), commoditized cellular spyware, Evil Twin Wi-Fi attacks launched from mobile platforms and the exploitation of location and activity data exposed through consumer applications. Together, these examples illustrate how both active exploitation and passive data leakage can be leveraged for pre-operational reconnaissance, pattern-of-life analysis and targeting of individuals or critical assets.

The session highlights several recurring findings: that wireless environments are frequently treated as inherently trusted despite being easily manipulated; that data exhaust from personal and commercial devices can provide actionable intelligence without direct intrusion; and that existing security models often fail to account for adversaries operating simultaneously across cyber, physical and proximity-based domains. These gaps create opportunities for threat actors to achieve effects traditionally associated with sophisticated cyber operations using comparatively simple and accessible techniques.

Attendees will leave with a practical framework for identifying where these assumptions break down, how wireless-enabled threats intersect with operational missions and what steps can be taken to better detect, assess and mitigate risk. The session aims to inform both operational practice and policy considerations, encouraging a more integrated approach to defending against threats that increasingly span cyber, physical and human domains.

BIO: Brett Walkenhorst is the chief technology officer at Bastille, where he leads research and development focused on advancing wireless sensing and threat detection capabilities in complex operational environments.

One Fabric, Every Node: Unifying Fragmented Tactical Networks

Emedin Rivera III, Solutions Manager, Integrated Solutions, Tactical Communications Solutions, Mission Connections and Cybersecurity, Viasat •
Emedin.Rivera@viasat.com

ABSTRACT

Today's tactical network environment is a patchwork of incompatible platforms, legacy radio systems and siloed data paths that force warfighters to manage transport complexity instead of executing the mission. Fragmented architectures create dangerous gaps in situational awareness, introduce latency that degrades decision advantage and place an unsustainable cognitive burden on operators in contested, degraded, intermittent and limited (DDIL) environments. Multidomain operations demand split-second delivery of massive data volumes, but fragmented hardware and siloed networks buckle under the pressure.

Solving this challenge requires more than adding new transport capabilities. It requires unifying fragmented networks, platforms and radio systems into a single cohesive infrastructure while preserving existing investments and the individual functionality of each system. Rather than forcing a costly rip-and-replace, a unified mission network fabric provides a secure, vendor-neutral overlay that integrates disparate tactical networks and transport layers into a common operational framework.

In this presentation, Emedin Rivera III, solutions manager for integrated solutions within the tactical communications solutions division of Viasat's Mission Connections & Cybersecurity business, will outline how Viasat is helping government agencies return personnel from the server tent back to the fight through four critical steps:

- Automating primary, alternate, contingency and emergency (PACE) routing. By eliminating operator intervention, it enables multipath, multi-orbit and multiband transport from the tactical edge, eliminating manual network reconfiguration during mission execution.
- Adopting dynamic mesh management that spans space, air, land, maritime and cyber domains, ensuring uninterrupted high-volume data flow even in the most contested DDIL environments.
- Optimizing for AI/ML and data-intensive workloads to ensure intelligent quality of service. This guarantees that warfighters can harness deterministic, low-latency performance to support time-sensitive mission applications while accelerating decision advantage.
- Harnessing adaptive cryptography with dynamic crypto revocation, ensuring no physically captured or destroyed node exposes the enterprise cloud to adversaries. A single-pane-of-glass interface reduces cognitive burden, enabling operators to focus on the mission—not the transport.

Future network architectures must transition from isolated transport solutions to resilient, transport-independent mission fabrics that can integrate diverse networks into a single operational environment as the

U.S. Department of Defense continues to modernize for multidomain operations. The result is a unified infrastructure that reduces complexity at the tactical edge, provides commanders with a unified operational picture and enables the joint force to adapt as mission needs evolve.

BIO: Emedin "Rick" Rivera is the solutions manager for integrated solutions within the tactical communications solutions division of Viasat's Mission Connections & Cybersecurity business.

In this role, he leads the technical strategy and capability expansion for mission-focused network architectures, delivering integrated, purpose-built solutions that preserve connectivity among sensors, C2 nodes, edge platforms and cloud-enabled mission services

Before joining Viasat, Rivera completed a 26-year career in the U.S. Marine Corps, retiring as a chief warrant officer 4. Most recently serving as the senior enterprise and expeditionary communications adviser at Headquarters Marine Corps, he authored the Marine Corps' first transport strategy and established the $600 million Marine Corps Enterprise Commercial Satellite Services (MECS2) framework, expanding capabilities across 14 global teleports.

His extensive military background includes advising senior executive leadership on space and terrestrial network resilience, engineering communication architectures for major multinational exercises and coordinating presidential communications support aboard Marine One.

Throughout his career, Rivera has focused on resolving complex technical challenges to maintain resilient, mission-critical communications across varied operational environments. Recognized for his leadership in demanding conditions, his military decorations include the Legion of Merit, the Meritorious Service Medal and the Navy Commendation Medal. He is also a recipient of the A.B. Lasswell Award for in-service engineering innovation and the Department of the Navy Information Technology Excellence Modernize Award.

Software-Defined Everything: Integrating Fragmented C2 at Mission Speed

Anthony Zech, Director of Data and AI Community of Excellence, Everforth ECS •
anthony.zech@ecstech.com

ABSTRACT

The U.S. Army's hardest integration problem is rarely the radio, the platform or the network in isolation; it is the time and risk of building the software that makes them operate as one. Today, every new sensor, waveform or mission application triggers months of bespoke integration and a fresh accreditation fight. Fragmentation is, at its core, a software-delivery problem.

"Software-defined everything" reframes unification around the one layer that can actually move at mission speed. Agentic AI now collapses the build-integrate-test cycle from months to days but only when it rests on an enterprise architecture engineered to absorb that pace safely. The unlock is a hardened DevSecOps platform where disparate capabilities are onboarded behind one identity, one policy boundary and one service mesh, while each application keeps its native function.

ECS has built and tested a working reference implementation of this pattern: a Kubernetes platform aligned to the DOW DevSecOps Reference Architecture that unifies tactical awareness, chat, sensor pipelines and analytics under single sign-on, a mutual-TLS service mesh and policy-as-code guardrails. Transport rides an automated PACE ladder—primary, alternate and store-and-forward paths fail over with no operator action—behind a CSfC-style, FIPS-mode boundary.

The result is a single cohesive infrastructure that preserves individual functionalities while delivering automated PACE routing, dynamic mesh management, intelligent QoS and centralized boundary security. ECS pairs agentic engineering with zero-trust accreditation discipline to field this for the Army, and this session shows how.

BIO: Tony Zech is the data and AI community of excellence director at ECS. Zech is in charge of building a community of practice for data and AI at ECS to support ECS's many customers. Previously at ECS, he oversaw cyber analytics and architectures to secure customer environments in defense, government and the private sector.

Before joining ECS, Zech worked as a systems engineer at Forescout Technologies in the operational technologies business unit. In this role, Zech helped organizations secure critical cyber assets at the heart of their missions. Prior to Forescout, Zech worked at Cargill, a major agricultural manufacturer, leading analytics and orchestration for the Cargill Security Operations Center.

Zech served as an active-duty U.S. Marine Corps officer in intelligence and cybersecurity, deploying in support of Operation Iraqi Freedom, Operation Enduring Freedom and other operations in the Middle East. He continues in this role in the Reserves, currently serving on the joint staff as the Reserve deputy director for collection management (J26).

Zech holds a Bachelor of Science in international relations from the United States Naval Academy and a Master of Science in business analytics from the University of Minnesota.

Visualizing the Battlespace Without Collapsing Security Boundaries

Gerald Oliver, Senior Program Manager, High Sec Labs Inc. • jerryo@highseclabs.com

ABSTRACT

Modern command and control environments require personnel to interpret and act upon information from multiple systems, sensors, networks and security domains in near real time. However, traditional approaches often force users to work across separate displays, peripherals, workstations and rooms. This increases cognitive burden, slows decision-making, consumes limited command post space and makes it harder to deliver mission-critical information to decision-makers and front-line operators at the right time.

BIO: Gerald Oliver is a retired U.S. Naval Intelligence officer with a master's degree in engineering, serving as a program manager and project engineer.

Scalable, Agile, Modular Edge Services: C2 That Survives Disconnection

Anthony Zech, Director of Data and AI Community of Excellence, Everforth ECS •
anthony.zech@ecstech.com

ABSTRACT

At the tactical edge, the network is the first thing the adversary takes away. Algorithms and databases that depend on a clean link to the enterprise fail exactly when the fight begins. The requirement is an edge that keeps computing—and keeps its data coherent—through disconnection, low bandwidth and degraded power.

ECS has built and tested a modular edge command and control platform that runs the same way on one node or many. On a single ruggedized, fanless gateway, it hosts a full mission stack—tactical awareness, messaging, sensor pipelines, search and GPU-accelerated AI inference—entirely on device, with no reach-back. The same architecture scales out to a multinode, high-availability cluster, from a small team's minimal footprint to a command post's replicated configuration with no single point of failure. Tactical databases replicate synchronously across nodes and reconcile across sites by store-and-forward when a link returns, so no event is lost.

Connectivity and compute are treated as mission variables. Multiple transports are bonded behind automated PACE failover, and mission profiles add or shed services as power and bandwidth change. Onboard AI summarizes and prioritizes data so only what matters crosses a thin link, while local inference keeps decision support alive when the cloud is gone. Modular and standards-based, the platform accepts new capabilities—a better model, a new sensor, another radio—per mission, and an emergency cryptographic destruct protects data if hardware is compromised.

The result is high-performance algorithmic execution and tactical database replication that scale from a single node to an entire unit and survive the disconnected edge rather than assuming it away. ECS engineers this resilience end to end for the U.S. Army.

BIO: Tony Zech is the data and AI community of excellence director at ECS. Zech is in charge of building a community of practice for data and AI at ECS to support ECS's many customers. Previously at ECS, he oversaw cyber analytics and architectures to secure customer environments in defense, government and the private sector.

Before joining ECS, Zech worked as a systems engineer at Forescout Technologies in the operational technologies business unit. In this role, Zech helped organizations secure critical cyber assets at the heart of their missions. Prior to Forescout, Zech worked at Cargill, a major

agricultural manufacturer, leading analytics and orchestration for the Cargill Security Operations Center.

Zech served as an active-duty U.S. Marine Corps officer in intelligence and cybersecurity, deploying in support of Operation Iraqi Freedom, Operation Enduring Freedom and other operations in the Middle East. He continues in this role in the Reserves, currently serving on the joint staff as the Reserve deputy director for collection management (J26).

Zech holds a Bachelor of Science in international relations from the United States Naval Academy and a Master of Science in business analytics from the University of Minnesota.

Red Hat Device Edge and AMQ: Overcoming the Siloed Sensor in DDIL Environments

Master Sgt. Benny Fields, USAF (Ret.), Senior Solution Architect, Red Hat LLC •
befields@redhat.com

ABSTRACT

Future operational overmatch dictates that decision dominance must occur at the point of action to minimize the latency of the OODA loop. However, deploying high-performance algorithmic execution within ruggedized, SWaP-constrained environments presents a critical challenge. When tactical forces operate in disconnected, intermittent and limited (DDIL) bandwidth scenarios, traditional centralized reach-back fails. The fundamental blocker is the "siloed sensor" problem: legacy hardware locked into single-purpose functions because they lack a unified Red Hat Enterprise Linux (RHEL) foundation.

This session outlines a strategic transition from "hardware-fixed" to "mission-adaptive" capabilities by standardizing on the Red Hat edge portfolio. By purchasing and leveraging RHEL Image Mode and Red Hat Device Edge (incorporating MicroShift), the U.S. Department of Defense can treat an entire operating environment as a transactional container image. This decouples mission-critical AI/ML workloads from underlying proprietary hardware, allowing for rapid, atomic software updates using Red Hat Ansible Automation Platform over highly contested tactical networks.

BIO: Benny Fields is a senior solution architect supporting the U.S. Department of Defense and U.S. Army. He served 20 years and retired from the U.S. Air Force. Fields joined Red Hat in 2019 as a senior consultant and then transitioned to his current role.

A Practical Path to Interoperable Army Modernization

Matthew Domaratzky, Product Owner, SAIC • matthew.o.domaratzky@saic.com

ABSTRACT

U.S. Army organizations are modernizing networks, communications and mission systems while continuing to operate legacy platforms across increasingly complex operational environments. The challenge is not simply deploying new technology; it is integrating fragmented networks, platforms and communications into a cohesive operational environment without disrupting mission execution or limiting future flexibility.

This session explores a practical, low-risk approach to modernization that enables organizations to integrate existing and emerging capabilities through open, interoperable architectures. Rather than replacing proven systems, organizations can preserve existing investments, reduce modernization risk and improve operational effectiveness by connecting data, communications and mission systems across the battlespace.

Attendees will gain insight into how to:

- Modernize operational networks while preserving interoperability with existing platforms and mission systems.
- Integrate fragmented communications, data and tactical environments through open, standards-based architectures.
- Improve resilience across contested, disconnected and low-bandwidth environments.
- Leverage commercial technologies that preserve customer ownership of data while reducing vendor lock-in.
- Build a scalable foundation that supports future Army and joint modernization priorities.

Designed for Army modernization leaders, network architects and mission owners, this session demonstrates how organizations can modernize with confidence while preserving the flexibility required to adapt to evolving operational requirements.

BIO: Matt Domaratzky is the product owner for SAIC's products portfolio, leading the strategy and execution of the company's mission data products, including MDP, Aether and Koverse.

Securing AI Where It Executes: The Rise of the Endpoint Agents

Jeff Worthington, Executive Strategist, CrowdStrike •
jeff.worthington@crowdstrike.com

ABSTRACT

Powerful computer-use agents like Claude Code, OpenAI Codex and OpenClaw have transformed the endpoint into a critical control plane for AI security. These agents can inherit full permissions of their users, autonomously act and take high-risk actions that never cross network boundaries, like running terminal commands and modifying local files. Attend this talk to learn how to assess and defend the agentic blast radius on the endpoint.

BIO: Col. Jeff Worthington, USA (Ret.), sits on the Public Sector Executive Strategy Team at CrowdStrike, providing strategic advisory services related to enterprise cybersecurity solutions. Worthington capped a 30-year career as the chief information officer of Joint Special Operations Command.

The Agentic Edge for Air-Gapped Environments

Sarah Joy, Technical Education Engineer, Splunk • sarjoy@cisco.com

ABSTRACT

Disconnected and air-gapped mission environments often depend on fragmented command systems, sensor feeds, network telemetry and security tools, increasing operator burden and slowing response. This session presents an agentic AI architecture for mission network observability that uses Splunk as the trusted local evidence layer, enriched by Cisco and infrastructure telemetry, to unify disparate data into an actionable operational picture.

A governed agent layer leverages RAG, LLMs and controlled tool access to support contextual reasoning, guided investigation and operator-ready summaries without requiring cloud connectivity or uniform network architectures. Designed around modular, auditable, human-in-the-loop principles, the approach supports CMOSS/SOSA-aligned integration while reducing cognitive load and improving situational awareness across heterogeneous mission environments.

BIO: Sarah Joy is a senior technical curriculum developer at Cisco, specializing in cybersecurity training and detection engineering. A retired U.S. Army CW4 with extensive cyber operations experience, she designs practical, AI-assisted learning experiences.

A Secure-by-Design Approach to Resilient Agentic Ecosystems

Baron Rawlins, Principal Architect, Army, Google Public Sector •
bmrawlins@google.com

ABSTRACT

Developing validated, resilient machine-to-machine (M2M) security protocols to prevent "synthetic access" breaches driven by autonomous agentic AI is crucial, especially given that current protocols like the Model Context Protocol (MCP) often offer considerable freedom in design, leading to ambiguous and potentially insecure usage. This flexibility creates new attack paths, as servers might query and execute actions for connected clients, inverting traditional interaction patterns and making them vulnerable to arbitrary code execution (ACE), privilege escalation and data exfiltration by autonomous agents.

A multilayered, adaptive strategy is required. This centers on adopting secure-by-design frameworks like Google's Secure AI Framework (SAIF) to embed life cycle-wide security. It must feature robust identity and access control, using least-privilege and zero-trust principles to grant AI agents separate identities and fine-grained permissions. Continuous monitoring and detection are essential, utilizing real-time behavioral monitoring, chain-of-thought analysis and anomaly detection alongside AI "supervisors" to identify misalignment, unexpected actions or injection attempts while suppressing evasion. Additionally, architectural resilience and isolation via clear trust boundaries, environment isolation and sandboxing will limit blast radiuses and prevent cascading failures.

Ensuring secure communication requires message authenticity, confidentiality and replay protection through cryptographic signatures and strict validation. Proactive prevention and response strategies must combine automated blocking, human-in-the-loop interventions for high-risk scenarios and instance shutdown capabilities. The integrity of the agentic supply chain must be reinforced through provenance tracking, verification and continuous vulnerability management for all tools and components.

Finally, adversarial testing and continuous feedback loops, such as regular red-teaming, are critical to validate resilience and refine evolving protocols. Comprehensive auditing and logging remain foundational for incident response and accountability.

Attendees will learn or gain:

- A deep understanding of novel AI agent threats: insights into how autonomous agentic AI introduces new attack vectors like agent goal hijack, tool misuse and memory poisoning, specifically targeting M2M protocols.
- Practical strategies for architectural and operational security: knowledge of frameworks (e.g., SAIF, AI Control Roadmap), core security principles (e.g., zero trust, least privilege) and technical controls (e.g., agent identity, sandboxing, secure supply chain) to build resilient M2M protocols.

- Methods for continuous validation and adaptive defense: approaches to employing adversarial testing, comprehensive logging and real-time behavioral monitoring to ensure M2M security protocols can withstand and adapt to evolving AI-driven threats.

BIO: Baron Rawlins, a principal architect at Google Public Sector, delivers mission-critical cloud solutions built on two decades of DOW experience. A former Army reservist, Rawlins is passionate about applying AI and quantum to empower the warfighter.

Hardening Networks Against Cryptographic Threats

Mark Maglin, Vice President of Cybersecurity, ECS Federal •
mark.maglin@ecstech.com

ABSTRACT

The most effective defense against next-generation cryptographic threats is continuous visibility into cryptographic assets, rapid cryptographic agility, hybrid post-quantum deployment and continuous monitoring of trust relationships.

ECS, through the Army Endpoint Security Solution (AESS) program, is protecting the U.S. Army's network for more than 600,000 endpoints cloud to device, providing a complete cryptographic inventory for certificates, libraries, algorithms and cryptography.

Our solution provides the foundational cryptographic inventory and risk intelligence required to operationalize all four. ECS Federal, the Army's ACDI delivery lead, converts that intelligence into executed remediation, integration and sustained resilience within the mission environment. Tychon supplies the cryptographic ground truth, and ECS partners with the Army to operationalize it at echelon.

Hardening command and control (C2) networks against next-generation cryptographic and algorithmic threats requires a combination of cryptographic visibility, cryptographic modernization, identity assurance and continuous monitoring. A specific and actionable approach to this includes:

- Establishing a complete cryptographic inventory first. Organizations cannot protect what they cannot identify or see. Discover all instances of RSA, ECC, TLS, SSH, IPsec, PKI certificates, code-signing certificates, cryptographic libraries and embedded cryptography across C2 infrastructure.
- Identify and prioritize quantum-vulnerable cryptography. Assess where Shor-vulnerable algorithms (RSA, ECDSA, ECDH, Diffie-Hellman) protect mission-critical communications, authentication systems, software signing processes and operational data stores.
- Plan and prepare for cryptographic agility. Design systems to support rapid replacement of algorithms, certificates and trust anchors without requiring major architectural changes or system downtime.
- Adopt hybrid classical-plus-PQC architectures. As CNSA 2.0 and NIST standards mature, deploy hybrid key exchange and digital signature mechanisms that combine current approved algorithms with post-quantum alternatives to reduce migration risk.

- Strengthen software supply chain trust. Advanced signature forgery threats place increased importance on validating code provenance, software bills of materials (SBOMs), cryptographic bills of materials (CBOMs), certificate chains and signing infrastructure.
- Protect and monitor PKI infrastructure. Certificate authorities, registration authorities, hardware security modules (HSMs) and code-signing systems become increasingly attractive targets as adversaries seek to undermine trust relationships rather than directly attack endpoints.
- Validate mission systems against emerging forgery scenarios. Conduct exercises and assessments that assume compromised certificates, forged digital signatures, manipulated software updates and corrupted trust chains to ensure operational resilience.
- Deploy continuous cryptographic monitoring. Treat cryptographic risk similarly to vulnerability management. Continuously monitor for weak algorithms, expired certificates, deprecated protocols, unauthorized cryptographic implementations and policy violations.
- Prepare for harvested-data risk now. Sensitive operational traffic encrypted today may be captured and retained by adversaries for future decryption. Prioritize protection of long-lived mission, intelligence, logistics and operational planning data.

BIO: Mark Maglin is the vice president for DOD cybersecurity at Everforth ECS Federal, where he leads business development and oversees the delivery of cybersecurity and AI solutions to defend the nation's most strategic assets. Maglin also leads ECS Federal's services and solutions for post-quantum cryptography and quantum computing.

In 2016, Maglin began work with ECS Federal to take on a new challenge to deploy and deliver endpoint security as a service to the U.S. Department of Defense (DOD), integrating multiple vendor security tools into a single cyber defense platform delivered as a service on the unclassified and classified global networks.

Before joining ECS, Maglin was a senior program manager at CACI, where he provided enterprise program management, acquisition, financial management and systems engineering support to DOD intelligence community customers for acquisition of full life cycle support for major ACAT information technology systems. Previously at CACI, Maglin provided program management and systems engineering support to develop and field SHARKSEER enterprise cyber defense platform and cyber threat indicator sharing systems.

Prior to his industry career, Maglin served in the U.S. Navy for more than 23 years. After an initial tour and qualification as a surface warfare officer, Maglin transitioned to naval aviation where he flew more than 3,000 hours in the E-2C Hawkeye, C-2A Greyhound and a variety of other aircraft. Maglin's final duty station brought him back to the U.S. Naval Academy where he continues to support the academy as a varsity offshore sailing team coach. Even after major deployments and years at sea, Maglin still enjoys the ocean and is a competitive sailor. Maglin is an active pilot and flight instructor. He holds a bachelor's degree in systems engineering from the U.S. Naval Academy and a master's degree in strategic studies from the U.S. Naval War College.

Unifying the Tactical Edge Through Identity Security and Zero Trust

Andrew Whelchel, Manager, Solutions Engineering, Saviynt •
andrew.whelchel@saviynt.com

ABSTRACT

The future battlespace demands more than interconnected infrastructure. As the U.S. Army modernizes its network for multidomain operations, commanders face an increasingly complex challenge: integrating fragmented networks, platforms, radio systems and mission applications into a unified operational environment while preserving the specialized capabilities of each system. The ability to deliver automated PACE routing, dynamic mesh networking, intelligent QoS prioritization and centralized boundary security depends on more than transport modernization alone. Success requires a common command layer capable of establishing trust, controlling access and enabling mission execution across heterogeneous environments.

In contested, disconnected, intermittent and low-bandwidth (DDIL) conditions, traditional approaches to identity, access and system authorization often become operational bottlenecks. Delays in onboarding personnel, provisioning access to mission systems or integrating mission partners can degrade decision advantage and limit commanders' ability to maneuver across the battlespace. As initiatives such as the Network Plan of Execution (NPE) seek to create a more agile and resilient network architecture, identity must become a foundational component of mission command rather than an administrative function.

This session examines how identity-centric architectures can serve as the connective tissue across tactical and enterprise environments, enabling seamless movement of personnel, applications and data across diverse transport paths and operational domains. Through real-world examples and emerging best practices, attendees will explore how automated identity governance, policy-driven access controls and continuous zero-trust authorization support mission continuity even when networks are degraded or dynamically changing.

The discussion will highlight approaches that enable rapid operator onboarding, accelerated mission-system access and secure mission-partner integration while maintaining zero-trust principles. Leveraging capabilities available through modern identity platforms such as Saviynt, organizations can automate access decisions, reduce administrative burden and ensure that the right users gain access to the right resources at the right time, regardless of location, connectivity or platform.

Attendees will expect to learn key capabilities including:

- Understand the role of identity as a unifying layer across heterogeneous tactical and enterprise networks.
- Explore how Saviynt enables rapid onboarding and mission-system access in DDIL and NPE-driven environments.

- Learn how identity-driven automation supports PACE routing, dynamic mesh operations and zero-trust security.
- Identify strategies for improving operational resilience while reducing administrative overhead and access delays.

Attendees will gain practical insights into how identity can function as the command layer that unifies disparate communications and mission systems into a secure, resilient and operationally effective infrastructure. By aligning identity, access and authorization with network modernization efforts, military organizations can improve readiness, increase operational tempo and strengthen mission assurance across the tactical edge.

BIO: Andrew Whelchel, CISSP-ISSEP, is a manager of solutions engineering at Saviynt, advising in identity security and zero trust. He is pursuing a master's degree in intelligence and security studies at Augusta University and contributed to SP 1800-3: ABAC Project.

Preventing Synthetic Access: Identity Security for Autonomous Agentic AI

Andrew Whelchel, Manager, Solutions Engineering, Saviynt •
andrew.whelchel@saviynt.com

ABSTRACT

As autonomous AI agents increasingly interact with enterprise systems, APIs, cloud services and other agents, traditional machine-to-machine (M2M) security models face a new threat: synthetic access. Unlike conventional credential theft, synthetic access occurs when autonomous agents create, inherit, misuse or chain identities and permissions in ways that bypass established governance controls, resulting in unauthorized access without direct human intervention.

This presentation proposes an identity-centric framework for developing validated and resilient M2M security protocols that address the emerging risks of agentic AI. The approach combines small language model AI capabilities with Saviynt's Identity Security platform to establish a model where every autonomous agent is treated as a governed digital identity with verifiable ownership, authenticated credentials, defined privileges and continuous monitoring.

The framework introduces four core controls: identity validation, policy-based authorization, runtime trust verification and continuous auditability. AI agents are issued machine identities that are cryptographically validated, restricted by least-privilege policies and continuously evaluated before accessing sensitive resources or interacting with other agents. Authorization decisions are dynamically enforced based on identity posture, context, risk and governance policies rather than static credentials alone.

Attendees will explore how autonomous agents can securely participate in M2M ecosystems while preventing unauthorized privilege escalation, synthetic identity creation, agent impersonation and uncontrolled agent-to-agent delegation. The session will also examine how AI-powered governance can continuously validate trust relationships and detect anomalous access behaviors before they evolve into security incidents.

Key outcomes include:

- A reference architecture for agentic AI identity governance.
- Methods for validating machine identities and agent provenance.
- Runtime authorization controls for agent-to-agent interactions.
- Detection and prevention strategies for synthetic access attacks.
- Governance and audit mechanisms supporting zero-trust principles in autonomous environments.

By extending identity security and governance principles to autonomous AI systems, organizations can establish resilient M2M security protocols that enable innovation while protecting critical resources from the next generation of AI-driven access threats.

BIO: Andrew Whelchel, CISSP-ISSEP, is a manager of solutions engineering at Saviynt, advising in identity security and zero trust. He is pursuing a master's degree in intelligence and security studies at Augusta University and contributed to SP 1800-3: ABAC Project.

Brain vs. Muscle

Derek Thurston, Associate Principal Solution Architect, Red Hat LLC •
dthursto@redhat.com

ABSTRACT

This proposal outlines a “Brain vs. Muscle” architecture that leverages edge-native AI to transform tactical network management from reactive processes to proactive, self-healing orchestration. By deploying containerized, quantized models on ruggedized hardware, the system ensures persistent intelligence and secure, automated decision-making even in disconnected or limited network environments.

Artificial intelligence can revolutionize tactical network management by transitioning systems from reactive processes to proactive, self-healing orchestration. Red Hat offers a framework for designing intelligent, real-time decision-making systems within demanding tactical environments. Predictive routing and agentic AI can address critical challenges, such as fragmented networks, quality-of-service optimization and complex PACE routing, without compromising operational security.

Advanced mechanisms, such as AIOps monitoring live RF spectrum data, can predict and mitigate network disruptions before they impact warfighter communications. Agentic AI can facilitate rapid root-cause analysis during mesh fragmentation, paired with event-driven automation, supporting system reliability. A “Brain vs. Muscle” design provides a framework for enforcing strict safety guardrails; in this model, AI serves as an analytical brain for anomaly detection, while the platform functions as the deterministic muscle, auditing execution and ensuring automated actions align with established policy-as-code boundaries.

Effective operation within denied, disrupted, intermittent and limited (DDIL) constraints is possible using a decentralized, “offline-first” architecture. Using edge-native software can minimize the hardware compute footprint, allowing AI inference to run on ruggedized edge devices. Technologies such as Modelcar can facilitate air-gapped deployments by packaging AI models into standard OCI containers, while model quantization optimizes these models to fit within restricted memory parameters without sacrificing tactical accuracy.

Finally, this architecture can ensure continued intelligence even when network links are severed, keeping local AI runtimes fully operational during disruptions. The system can efficiently synchronize telemetry data and configuration updates once connectivity is restored, helping maintain warfighter superiority in challenging conditions.

BIO: Derek Thurston is a senior solutions architect at Red Hat and has been working with open source since the mid ‘90s. Thurston started with SGI and HP/UX systems for a variety of commercial and government customers and quickly realized that Linux is the way to go. Since then, he has spent more than 25 years helping his customers find the right tools and technologies, keeping in mind their specific security requirements.

Quantum-Resistant Optimization for Electromagnetic Warfare in GPS-Denied Areas

Jim Cosby, CTO, Federal Public Sector and Partners, NetApp US Public Sector Inc. •
jim.cosby@netapp.com

ABSTRACT

As modern battlefields grow increasingly complex, the integration of quantum-resistant optimization into electromagnetic warfare (EW) and combat systems is critical for real-time threat analysis in GPS-denied environments. This session explores how proactive, resilient data security strategies—leveraging NetApp's Intelligent Data Infrastructure—can prevent and mitigate cyber, post-quantum cryptography (PQC) and ransomware threats. Attendees will learn how NetApp's built-in autonomous ransomware protection, data security posture management, instant data recovery and hybrid multicloud capabilities prevent attacks and enable robust recovery from immutable cyber vaults. By aligning quantum-resistant technologies with NetApp's data-centric security solutions, this presentation delivers actionable insights to ensure mission success while maintaining operational superiority in contested environments for the U.S. Army.

BIO: Jim Cosby is currently a CTO at NetApp US Public Sector and has more than 25 years of technology engineering and leadership experience supporting a variety of federal and U.S. Department of Defense agencies. Cosby has focused on AI, data management and cyber data security.

Developing Resilient M2M Security Protocols To Combat Synthetic Access Breaches

Jim Cosby, CTO, Federal Public Sector and Partners, NetApp US Public Sector Inc. •
jim.cosby@netapp.com

ABSTRACT

In an era where autonomous agentic AI poses significant threats, developing validated and resilient machine-to-machine (M2M) security protocols is paramount to preventing "synthetic access" breaches. This session will delve into proactive and resilient data security measures, utilizing autonomous ransomware protection and data security posture management to guard against cyber, post-quantum cryptography (PQC) and ransomware attacks. Attendees will discover how NetApp's built-in data protection and hybrid multicloud capabilities provide robust recovery from immutable cyber vaults. By leveraging NetApp's Intelligent Data Infrastructure, this presentation offers critical insights to ensure mission success and operational security for the U.S. Army.

BIO: Jim Cosby is currently a CTO at NetApp US Public Sector and has more than 25 years of technology engineering and leadership experience supporting a variety of federal and U.S. Department of Defense agencies. Cosby has focused on AI, data management and cyber data security.

Intent to Action: Reducing Operator Cognitive Load Across the Zepharis™ Suite

Nate Delgado, Director of Software Products, Sealing Technologies •
nathan.delgado@sealingtech.com

ABSTRACT

This presentation covers the challenges of operator cognitive load at the tactical edge and how SealingTech's Zepharis™ Software Suite—Zepharis™ AI, Zepharis™ Kit Deployer and Zepharis™ Lifecycle Management—addresses it through intuitive, error-resilient interfaces that let cyber warfighters and operators focus on high-level reasoning rather than menu navigation. At the edge, operators burn scarce mental bandwidth on the mechanics of their tools: composing complex query syntax, navigating menu-deep workflows and hand-assembling data across disconnected interfaces, often while fully offline. This load falls hardest on junior operators, who can articulate intent but lack the experience to execute, pulling entire teams away from the reasoning the mission demands.

To address this, the Zepharis Software Suite applies a single principle across three capabilities: collapse complex, error-prone, multistep work into one deliberate action.

Zepharis AI replaces query syntax with natural-language querying, letting operators move from intent to action across their SIEM, IDS/IPS and hypervisor tools while automating detection engineering—elevating junior analysts toward senior-level capability without added training.

Zepharis Kit Deployer replaces manual, babysat setup with one-push deployment that configures and networks 20-plus tools in hours rather than days through standardized, error-free provisioning.

Zepharis Lifecycle Management retires the spreadsheets used to track fleet status, patching, licensing and warranties, surfacing that data through a single view that relieves operator toil while giving decision-makers and PMOs real-time visibility. To meet the unique security requirements of cyber operations, the entire suite is built on a fully air-gapped architecture, ensuring these capabilities remain effective without reliance on external connectivity.

The presentation will share how the Zepharis Software Suite continues to evolve and expand its capabilities based on mission operator needs and a rapidly shifting technology environment. The deeper payoff is not saved clicks but reallocated cognition: by absorbing the mechanical load of the operator's stack, these interfaces let teams reason through their data, asking the system to help think through what a detection is actually telling them, and concentrate on the judgment only humans can provide. By bridging the gap between complex, error-prone tooling and the disconnected warfighter, SealingTech ensures that defenders can focus on hunting adversaries more effectively and efficiently in any challenging environment.

BIO: Nate Delgado is a distinguished product leader at the forefront of artificial intelligence and cybersecurity innovation. As the director of software products at Sealing Technologies (SealingTech), a Parsons Corporation company, his team is building the first AI cyber analyst designed specifically for offline environments. Prior to SealingTech, Delgado scaled global managed detection and response (MDR) programs serving Fortune 500 clients and led the product team at a cutting-edge malware analysis software company.

Delgado comes to SealingTech with a proven track record of leading complex AI and machine learning products, including advanced threat hunting capabilities for major federal agencies. His commitment to advancing the field extends to the next generation where he actively mentors cybersecurity students through university programs across the United States.

He holds a Bachelor of Arts in economics from the University of Southern California.

Governing Agentic AI Actions: Building Real-Time Auditability Before the Threat Emerges

Patrick McGarry, Federal Chief Data Officer, ServiceNow •
patrick.mcgarry@servicenow.com

ABSTRACT

The U.S. Army's agentic AI initiatives are outpacing the governance frameworks designed to control them. As machine-to-machine workflows scale across multidomain operations, a new vulnerability is emerging: autonomous AI actions executed on valid credentials within policy boundaries, with no human authorization gate.

The threat is not the agent itself. The threat is the absence of a governance layer that answers three questions in real time: What data did this agent act on? Under whose authority? Was that data trustworthy when the action occurred?

Drawing on active federal CDO and CAIO engagements across defense and intelligence agencies, this session examines the governance architecture required to make agentic AI operationally effective while remaining fully auditable. You'll learn how data provenance, policy enforcement and access controls must be woven into the workflow layer, not bolted on after deployment, to prevent unauthorized synthetic access before it occurs. We'll also show how your existing Army governance frameworks (RMF, zero trust, data-tagging standards) extend rather than get replaced to close this gap.

BIO: Patrick McGarry is the federal chief data officer at ServiceNow, a role he assumed following the company's acquisition of data.world, where he previously built the public sector business. With two decades of experience spanning defense, intelligence and the private sector, he leads data strategy and AI governance for ServiceNow's U.S. federal clients, with particular focus on U.S. Department of Defense modernization initiatives.

McGarry began his career as an enlisted member of the U.S. Navy before transitioning to technology leadership roles at Red Hat, Alcatel-Lucent and SourceForge, where he specialized in building open developer ecosystems. His expertise in metadata management, knowledge graphs and functional data governance has made him a trusted adviser on AI-adoption strategies across federal civilian agencies, defense organizations and the intelligence community.

McGarry brings a unique sociotechnical perspective to organizational design and data strategy, recognizing that successful AI and data initiatives require institutional change, not just technical

deployment. He explores this thesis in his book, “The Adaptive Organization: Leading Change in the AI Era (Data Literacy Press),” which examines why AI transformation failures are rooted in organizational dynamics rather than technology gaps. In his daily work, he positions data infrastructure as trust infrastructure, helping federal leaders build durable capabilities that enable faster decision cycles while maintaining security, compliance and mission readiness in complex operational environments.

Intelligence Without Action Is Just Overhead: The Data Fabric That Makes Multidomain Command Integration Work

Patrick McGarry, Federal Chief Data Officer, ServiceNow •
patrick.mcgarry@servicenow.com

ABSTRACT

The U.S. Army has made significant investments in CMOSS and SOSA compliance as the standards backbone for integrating disparate command structures and sensors. What those standards don't solve is the semantic layer: whether data from a sensor in one domain means the same thing to a system in another. Network observability and flow management can tell you data moved. They can't tell you whether that data was understood, trusted or acted upon correctly. In multidomain operations, that distinction is the difference between decision advantage and compounded error.

This session examines what a federated data architecture looks like when designed to preserve meaning across command structures, not just connectivity. Drawing on implementation experience with federal data fabric programs and semantic interoperability frameworks aligned to W3C and PROV-O standards, we'll walk through the three foundational layers above transport that the Army needs to achieve true network observability: a unified data catalog that knows your data exists and what it means, policy-enforced lineage tracking that shows where data came from and who touched it, and workflow integration that closes the loop from intelligence to action. We'll also show how these capabilities layer onto your existing CMOSS and SOSA infrastructure without requiring rearchitecting.

BIO: Patrick McGarry is the federal chief data officer at ServiceNow, a role he assumed following the company's acquisition of data.world, where he previously built the public sector business. With two decades of experience spanning defense, intelligence and the private sector, he leads data strategy and AI governance for ServiceNow's U.S. federal clients, with particular focus on U.S. Department of Defense modernization initiatives.

McGarry began his career as an enlisted member of the U.S. Navy before transitioning to technology leadership roles at Red Hat, Alcatel-Lucent and SourceForge, where he specialized in building open developer ecosystems. His expertise in metadata management, knowledge graphs and functional data governance has made him a trusted adviser on AI-adoption strategies across federal civilian agencies, defense organizations and the intelligence community.

McGarry brings a unique sociotechnical perspective to organizational design and data strategy, recognizing that successful AI and data initiatives require institutional change, not just technical deployment. He explores this thesis in his book, "The Adaptive Organization: Leading Change

in the AI Era (Data Literacy Press),” which examines why AI transformation failures are rooted in organizational dynamics rather than technology gaps. In his daily work, he positions data infrastructure as trust infrastructure, helping federal leaders build durable capabilities that enable faster decision cycles while maintaining security, compliance and mission readiness in complex operational environments.

Edge Operations Without Limits: Unified Asset and Operational Intelligence for Disconnected Tactical Environments

Andrew Scherer, Federal Sales, ServiceNow • andrew.scherer@servicenow.com

ABSTRACT

The U.S. Army's tactical edge demands independent operations in constrained, contested environments. Yet systems that support edge operations remain fragmented, leaving commanders without visibility into assets or how they perform. The dilemma: operate blind or deploy systems too power-intensive for the field.

This session explores how ServiceNow's unified platform, optimized for the tactical edge, enables forward units to maintain operational clarity and asset control without constant connectivity to cloud or garrison infrastructure. Drawing on real Army deployments, we'll walk through the architecture that delivers mission-critical capabilities: unified visibility into IT and physical asset life cycles across ruggedized hardware, intelligent synchronization of mission-critical databases at the edge with automated conflict resolution in low-bandwidth environments, autonomous operational management that executes workflows and optimizes performance without centralized command and control, and agentic AI that responds to operational anomalies and executes contingency actions based on edge-local context.

Because your commands already use ServiceNow hardware asset management, enterprise asset management and IT operations management at scale, you can extend them to the edge without additional licensing costs. You accelerate time to value and let tactical units leverage systems already trusted enterprise-wide into your most challenging operational environments.

BIO: Andrew Scherer, based in Washington, D.C., boasts 25 years of experience in the financial and federal sales domains. His impressive track record includes 18-plus years of selling information technology services directly to both the U.S. Department of Defense (DOD) and civilian agencies. Scherer's forte lies in crafting customized solutions that yield powerful outcomes, all while keeping a keen eye on budget constraints and return on investment. His passion lies in collaborating with DOD clients to deliver enterprise-wide solutions that not only advance their mission but also equip them with world-class tools to enhance their work environment.

Optimizing the Last Tactical Mile: Adaptive Logistics, Resource Allocation and Autonomous Coordination Across Contested Networks

Michael Longoria, Mission Account Manager, U.S. Army, ServiceNow •
michael.longoria@servicenow.com

ABSTRACT

The next fight will be fast, spread out and changing constantly under uncertainty. That puts unprecedented load on the systems that move and prioritize people, equipment, supplies and autonomous assets. This session addresses optimizing logistics, resource allocation and autonomous coordination across domains in near real time while keeping systems working when bandwidth is tight and there is no central control.

Two requirements converge into one problem. First, sustainment: distributed, predictive planning with no single hub that reprioritizes how combat power moves as conditions, demand and losses change. That is the digital backbone of the NDS industrial base and readiness line of effort. Second, autonomy: running swarms of air, ground or sea platforms that adjust to mission, threat and losses without central authority. The optimization that counts is time. Every delay getting a reprioritized plan out across a contested, disconnected network means combat power arrives late. In a fight where sustainment is already tight, late means lost.

In the Indo-Pacific, contested logistics across long distances decide outcomes more than sensing does. That is a command and control and time problem, and it is the one most likely to decide a long war.

BIO: Michael Longoria is a former Army infantry officer and transformation executive with 17-plus years of leadership experience spanning joint military operations, enterprise technology and defense modernization. He is passionate about bridging operational warfighter challenges with emerging technologies to deliver mission outcomes at the speed of relevance.

At ServiceNow, Longoria is currently focused on helping defense and government organizations modernize command and control, operational workflows, enterprise platforms and data-driven decision-making in support of next-generation warfighting capabilities. He is experienced operating at the intersection of operational planning, enterprise transformation, AI-enabled modernization, cybersecurity and mission-focused technology strategy.

The Interface That Disappears: Cognitive-Load Reduction, Time and Error-Resilient Design at the Tactical Edge

Michael Longoria, Mission Account Manager, U.S. Army, ServiceNow •
michael.longoria@servicenow.com

ABSTRACT

The more systems we field, the more we load on the operator. Soldiers have to decide quickly across multiple feeds while tired, stressed and unsure. Too many menus, mismatched screens and fragile workflows pull attention off the mission and set them up to make mistakes. This session explores interface design that actually cuts that load: put the right information in front of the operator at the right time, cut the steps that do not matter and walk them through critical tasks in a way that prevents errors and speeds execution.

Cognitive load is really a time problem in disguise. Every click an interface demands, every screen a leader has to square away by hand, is time stolen from planning, rehearsal and decision. Under the one-third, two-thirds rule, time a leader loses fighting the tool set is time stolen straight from his subordinates' ability to get ready. A tool that fights the operator taxes the formation's most irreplaceable resource.

The rule is simple. Automation should take over repetitive admin and system babysitting, not judgment. Give the soldier back the attention and time for situational awareness, command decisions and his own headspace. It has to hold up in the field with little training, high turnover, movement and bad comms. In counter-C2 terms, the side whose operators spend their time on the enemy instead of on their own software decides and acts faster.

BIO: Michael Longoria is a former Army infantry officer and transformation executive with 17-plus years of leadership experience spanning joint military operations, enterprise technology and defense modernization. He is passionate about bridging operational warfighter challenges with emerging technologies to deliver mission outcomes at the speed of relevance.

At ServiceNow, Longoria is currently focused on helping defense and government organizations modernize command and control, operational workflows, enterprise platforms and data-driven decision-making in support of next-generation warfighting capabilities. He is experienced operating at the intersection of operational planning, enterprise transformation, AI-enabled modernization, cybersecurity and mission-focused technology strategy.

Compute That Survives Contact: Resilient Edge Analytics and Tactical Data Replication in Denied Environments

Michael Longoria, Mission Account Manager, U.S. Army, ServiceNow •
michael.longoria@servicenow.com

ABSTRACT

We cannot count on the cloud in the next fight. A peer enemy's first move is to cut the spectrum and sever reach-back. That means the tactical edge has to compute, analyze and decide on its own, or it does not get to decide at all.

This session explores edge systems that can do exactly that. Rugged, expeditionary kit that runs analytics, AI, sensor fusion and decision support right next to the formation and keeps mission data in sync across nodes on low bandwidth without corrupting it. The root problem is segmentation. When nodes cannot talk, people have to reconcile the picture manually, and that costs time the formation does not have.

What matters most is graceful degradation. Systems that keep running independently through jamming, cyber attacks and extended disconnection, then resynchronize fast when the link comes back. That aligns with NGC2 principles of edge survivability, built on open architecture and nonproprietary APIs so new capability comes through competition, not vendor lock-in.

Measure it the way a commander does: Can I get good, timely information and compute regardless of what the network is doing? The real question is not how powerful the edge box is. It is how little of the formation's time it costs to rebuild the picture when the network comes back.

BIO: Michael Longoria is a former Army infantry officer and transformation executive with 17-plus years of leadership experience spanning joint military operations, enterprise technology and defense modernization. He is passionate about bridging operational warfighter challenges with emerging technologies to deliver mission outcomes at the speed of relevance.

At ServiceNow, Longoria is currently focused on helping defense and government organizations modernize command and control, operational workflows, enterprise platforms and data-driven decision-making in support of next-generation warfighting capabilities. He is experienced operating at the intersection of operational planning, enterprise transformation, AI-enabled modernization, cybersecurity and mission-focused technology strategy.

Hardening Command and Control Networks Against Next-Generation Cryptographic and Algorithmic Threats

Jeffrey L. Berlet, Chief Technology Officer, Cyber & Intelligence Sector, Peraton

ABSTRACT

The cryptographic foundations underpinning U.S. Army command and control (C2) networks face an inflection point. The convergence of quantum computing maturation, AI-accelerated cryptanalysis and the emergence of adversary-developed algorithmic attack tooling has fundamentally altered the threat landscape for military communications security. Of particular concern is the growing viability of advanced digital signature forgery—the ability of sophisticated adversaries to fabricate, manipulate or invalidate the cryptographic signatures that authenticate orders, sensor data and automated C2 exchanges across Army tactical and enterprise networks. A successfully forged command signature does not merely represent a data breach; it represents the potential for adversary-injected orders to propagate through the force with the full appearance of legitimacy, with catastrophic consequences for mission integrity and warfighter safety.

Current C2 network security architectures rely heavily on classical public-key infrastructure (PKI), RSA and elliptic-curve cryptography (ECC), and legacy digital signature standards that were not designed to withstand quantum-enabled attacks or AI-driven cryptanalytic pressure. Nation-state adversaries—particularly China and Russia—are actively investing in quantum computing programs and harvesting encrypted military communications today for future decryption a strategy known as "harvest now, decrypt later." The window to harden existing C2 infrastructure before these capabilities mature is narrow and closing.

Based on Peraton research focused on this topic, we propose a comprehensive C2 Cryptographic Hardening Initiative to systematically assess, upgrade and validate the cryptographic resilience of Army C2 networks against next-generation threats. The initiative is structured around four lines of effort.

Post-Quantum Cryptography (PQC) Migration: accelerating the integration of NIST-standardized post-quantum algorithms, including CRYSTALS-Kyber (key encapsulation) and CRYSTALS-Dilithium (digital signatures), into existing C2 protocol stacks, with a prioritized migration road map based on network criticality and exposure risk.

Digital Signature Integrity Architecture: developing a layered signature verification framework that combines PQC-based signing, hardware-rooted trust anchors (TPM 2.0/HSM) and real-time signature anomaly detection to identify and quarantine forged or manipulated command authentications before they propagate through the C2 chain.

Algorithmic Threat Emulation & Red Teaming: constructing an adversarial testing environment that simulates quantum-enabled and AI-assisted cryptographic attacks against representative C2 network configurations,

enabling continuous vulnerability discovery and validation of hardening measures prior to operational deployment.

Crypto-Agility by Design: embedding cryptographic agility into C2 system architectures so that algorithms can be rapidly swapped in response to emerging threats without requiring full system reengineering, ensuring long-term adaptability as the cryptographic threat environment continues to evolve.

The integrity of Army C2 networks is the integrity of command authority itself. Hardening these networks against next-generation cryptographic threats is not a modernization option; it is an operational imperative that must be addressed with urgency, rigor and a forward-looking understanding of the adversary's rapidly advancing capabilities.

BIO: Jeffrey (Jeff) Berlet is the chief technology officer for Peraton's Cyber & Intelligence Sector. In this role, Berlet leads the internal research and development activities, solution development, technical workforce development and external engagement with industry partners for Peraton's cybersecurity, intelligence and national security programs. Berlet has more than 20 years of experience within Peraton's heritage companies, including Perspecta, Vencore, Bell Labs and Lockheed Martin. He previously held positions as director, chief engineer, chief technology officer, chief information officer, program manager, lead solution architect and a range of systems engineering roles. Earlier in his career, Berlet worked in a variety of engineering and information technology positions for Eli Lilly and Sun Microsystems.

Berlet previously served as a technical director in Peraton's Space & Intelligence Sector, where he developed technical solutions for the U.S. Space Force, Air Force Space Command and classified space customers. Berlet recently served as the chief engineer for the company's largest classified intelligence program, and he previously supported several cyber programs in the United Kingdom in chief engineer and program manager roles.

Berlet has earned several professional certifications, including International Council on Systems Engineering (INCOSE) Expert Systems Engineering Professional (ESEP), Lean Six Sigma Black Belt, Scaled Agile Framework (SAFe) Agilist, Information Technology Infrastructure Library (ITIL) Foundation, Enterprise Architect Center of Excellence (EACOE) Enterprise Architect, and Project Management Institute (PMI) Program Management Professional (PMP).

Berlet is a past president of the INCOSE Chesapeake Chapter and an adviser to the National Security Collaboration Center at University of Texas at San Antonio (UTSA). He is a member of the Space Information Sharing & Analysis Center (Space ISAC) and the Organization for the Advancement of Structured Information Standards (OASIS) standard organization. Berlet is a member of the Industrial and Professional Advisory Council (IPAC) for the Penn State College of Engineering.

Berlet is a graduate of Penn State University (B.S. in computer engineering) and University of Pennsylvania (M.S. in computer and information sciences).

Validated Resilient Machine-to-Machine (M2M) Security Protocols

Jeffrey L. Berlet, Chief Technology Officer, Cyber & Intelligence Sector, Peraton

ABSTRACT

The rapid proliferation of autonomous agentic AI systems has introduced a fundamentally new class of cyber threat: synthetic access—the unauthorized infiltration of networked systems by AI-driven agents that mimic, impersonate or autonomously negotiate legitimate machine-to-machine (M2M) trust relationships. Unlike traditional intrusion vectors that exploit human error or static software vulnerabilities, synthetic access attacks leverage the speed, adaptability and deceptive fidelity of large-scale AI models to subvert authentication handshakes, forge behavioral signatures and sustain persistent footholds across Army tactical and enterprise networks—often below the threshold of conventional detection.

Current M2M security architectures—including certificate-based mutual TLS, OAuth 2.0 machine credentials and API gateway controls—were designed for deterministic, human-supervised environments. They are structurally unprepared for adversaries that can dynamically synthesize valid-appearing protocol exchanges, adapt in real time to defensive countermeasures and operate at machine speed across thousands of simultaneous sessions. As Army systems increasingly depend on autonomous platforms, AI-enabled logistics and multidomain command and control (C2) pipelines, the attack surface for synthetic access expands proportionally.

Peraton recommends the development and validation of a next-generation M2M security framework to detect, resist and recover from synthetic access threats based on the following four foundational pillars.

Behavioral Attestation & Continuous Identity Verification: moving beyond static credential exchange to dynamic, context-aware behavioral profiling of machine agents, enabling real-time anomaly detection when an agent's interaction pattern deviates from its established baseline—even when its credentials remain valid.

Zero-Trust Agentic Architecture (ZTAA): extending zero-trust principles to autonomous agent interactions by enforcing least-privilege session scoping, cryptographic intent binding and mandatory human-on-the-loop checkpoints for high-consequence M2M transactions within Army operational networks.

Adversarial Validation & Red-Team Stress Testing: employing purpose-built adversarial AI agents to continuously probe M2M protocol implementations, generating synthetic attack scenarios that simulate nation-state-level agentic intrusion campaigns. Validation cycles will be integrated into the Army's existing cyber test and evaluation pipeline.

Resilience & Graceful Degradation Protocols: designing M2M security layers with fault-tolerant fallback modes that preserve mission-critical communications under active synthetic access conditions, ensuring

operational continuity even when portions of the authentication infrastructure are compromised or under active manipulation.

The presentation will propose validated protocol specifications, open reference implementations compatible with Army DevSecOps environments and a synthetic access threat taxonomy to inform doctrine, acquisition and training across ARCYBER and the broader DOD cyber enterprise. Deliverables will be aligned with NIST AI Risk Management Framework (AI RMF), NSA Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) and DOD zero-trust strategy requirements.

Addressing synthetic access is not a future-state concern. Adversary nation-states are actively developing and deploying agentic AI capabilities today. Establishing validated, resilient M2M security protocols now is essential to preserving the Army's ability to operate with confidence across all domains in an era of autonomous, AI-driven conflict.

BIO: Jeffrey (Jeff) Berlet is the chief technology officer for Peraton's Cyber & Intelligence Sector. In this role, Berlet leads the internal research and development activities, solution development, technical workforce development and external engagement with industry partners for Peraton's cybersecurity, intelligence and national security programs. Berlet has more than 20 years of experience within Peraton's heritage companies, including Perspecta, Vencore, Bell Labs and Lockheed Martin. He previously held positions as director, chief engineer, chief technology officer, chief information officer, program manager, lead solution architect and a range of systems engineering roles. Earlier in his career, Berlet worked in a variety of engineering and information technology positions for Eli Lilly and Sun Microsystems.

Berlet previously served as a technical director in Peraton's Space & Intelligence Sector, where he developed technical solutions for the U.S. Space Force, Air Force Space Command and classified space customers. Berlet recently served as the chief engineer for the company's largest classified intelligence program, and he previously supported several cyber programs in the United Kingdom in chief engineer and program manager roles.

Berlet has earned several professional certifications, including International Council on Systems Engineering (INCOSE) Expert Systems Engineering Professional (ESEP), Lean Six Sigma Black Belt, Scaled Agile Framework (SAFe) Agilist, Information Technology Infrastructure Library (ITIL) Foundation, Enterprise Architect Center of Excellence (EACOE) Enterprise Architect, and Project Management Institute (PMI) Program Management Professional (PMP).

Berlet is a past president of the INCOSE Chesapeake Chapter and an adviser to the National Security Collaboration Center at University of Texas at San Antonio (UTSA). He is a member of the Space Information Sharing & Analysis Center (Space ISAC) and the Organization for the Advancement of Structured Information Standards (OASIS) standard organization. Berlet is a member of the Industrial and Professional Advisory Council (IPAC) for the Penn State College of Engineering.

Berlet is a graduate of Penn State University (B.S. in computer engineering) and University of Pennsylvania (M.S. in computer and information sciences).

The Human-in-the-Loop Advantage: Operationalizing AI for Secure, Distributed C2

David Herbst, Director of Solutions - Federal, Mattermost

ABSTRACT

Across the U.S. Army and joint force, commanders and staffs are under pressure to move faster, fuse more data and synchronize effects across domains—all while operating in highly contested, communications-degraded environments. AI and ML promise to accelerate sense–make–act cycles, but without secure, resilient workflows that connect humans, data and machines, those capabilities rarely translate into operational advantage at the tactical edge.

This session explores how to operationalize AI-enabled workflows inside distributed command and control environments in a way that keeps humans in the loop and trust at the center. Rather than focusing on a single product, we will examine patterns for embedding AI outputs into secure collaboration environments where mission teams plan, rehearse and execute—across echelons, classification levels and coalition boundaries.

Attendees will learn practical approaches to:

- Integrate AI/ML-generated insights into battle rhythms, COPs and mission threads without overwhelming operators.
- Enable secure, persistent chat, tasking and workflow automation that function across air-gapped, intermittent and low-bandwidth networks.
- Design human–machine teaming constructs that preserve commanders' intent, auditability and compliance with zero-trust principles.
- Reduce tool sprawl by consolidating mission communications, data interaction and automation into a cohesive operational fabric.
- Using real-world patterns from cyber operations, tactical formations and joint headquarters, the session will focus on how units can move from "AI experiments" to repeatable, defensible workflows that help deliver faster, more confident decisions in support of JADC2 and distributed C2 missions.

BIO: David Herbst is a federal sales engineer at Mattermost, recognized as an AI/ML innovator and a strategic leader in federal and defense technology. With more than 15 years of experience, Herbst has driven high-stakes technology operations in some of the most secure environments, spearheading complex cloud migrations and orchestrating large-scale infrastructure initiatives

with flawless execution. He is known for applying advanced AI/ML approaches—such as natural language processing and multimodal data fusion—to solve the nation's toughest security challenges and deliver transformative mission results.

Herbst's track record spans winning and executing multimillion-dollar federal contracts, which combines his deep technical expertise with strategic business insight to accelerate growth and ensure mission success. Prior to his role at Mattermost, Herbst held key positions at leading companies including Virtualitics, Primer.ai, Rebellion Defense, Descartes Labs and Exeter Government Services, where he continuously led technical programs and solutions architecture across federal agencies and defense organizations. His skills include ETL, data analysis, artificial intelligence, machine learning and executive-level technology leadership.

Herbst holds a bachelor's degree in defense systems management with a concentration in acquisition program management from Defense Acquisition University, and he has formal training in electronic systems technology from Air University, U.S. Air Force Institute of Technology.

Trusted Data Across Contested Networks: Metadata as the Common Language for Secure Information Exchange

Greg Colla, Chief Technology Officer, Janusnet • thomas@gdistrategies.com

ABSTRACT

As the U.S. Department of Defense modernizes communications across enterprise, tactical and coalition environments, significant progress has been made in connecting fragmented networks, platforms and radio systems. Yet the ability to securely exchange information across these heterogeneous environments depends on more than network connectivity. It depends on the data itself.

This session examines how machine-readable metadata, security classification markings and minimum essential metadata (MEM) provide the common language that enables trusted information exchange across disparate systems. Attendees will explore how metadata supports attribute-based access control (ABAC), automated policy enforcement, auditability and mission partner interoperability while preserving data integrity across connected, disconnected and contested environments.

Drawing on operational examples from classified and coalition networks, the discussion addresses practical considerations for metadata creation, persistence, governance and enforcement throughout the information life cycle. The session also examines the relationship between metadata and zero-trust architecture, demonstrating how authoritative security attributes enable consistent policy decisions regardless of transport, platform or network topology.

Participants will gain practical insight into implementing metadata-driven security controls that strengthen information-sharing, improve operational resilience and enable trusted collaboration across modern defense communications architectures.

BIO: Greg Colla is chief technology officer at Janusnet, where he leads the design and development of data-centric security technologies supporting government, defense and enterprise organizations. For more than two decades, he has worked at the intersection of information security, data classification, metadata and secure information-sharing, helping organizations implement practical solutions to protect and control sensitive information across email, documents and enterprise systems.

His experience includes supporting high-assurance and classified environments, with a particular focus on data-tagging, policy enforcement, interoperability and zero-trust architectures. Colla regularly works with defense and government stakeholders to address the operational challenges of securing, sharing and governing information in complex and mission-critical environments.

Adaptive Mission Networking: Using Cloud Computing To Operationalize the Army Unified Network

Derek Strausbaugh, Microsoft Federal CTO for DOW, Microsoft •
derek.strausbaugh@microsoft.com

ABSTRACT

As the U.S. Army transitions from a collection of legacy tactical, enterprise and platform-specific networks toward a data-centric unified network, one of the most significant technical challenges remains: how to integrate thousands of disparate radios, transport systems, cloud environments, sensors, command posts and mission systems into a single operational fabric without disrupting existing mission capabilities.

Recent Army modernization efforts emphasize reducing network complexity, enabling seamless data movement across echelons, implementing zero-trust security and delivering resilient communications in denied, disrupted, intermittent and limited-bandwidth environments.

This session explores how commercial cloud service can act as the orchestration layer for a unified Army network, enabling existing tactical and enterprise transport technologies to operate as a cohesive, adaptive and policy-driven infrastructure. Rather than replacing radios, SATCOM, MANETs, private 5G systems, tactical data links or enterprise networks, the commercial cloud can provide a software-defined control plane capable of integrating and managing these heterogeneous environments as a single operational system. The cloud can provide the Army with centralized routing and hybrid connectivity capabilities, large-scale mesh networking and policy-driven connectivity—foundational capabilities for a modern military transport architecture.

Attendees will learn how emerging cloud and edge technologies can automate the execution of primary, alternate, contingency and emergency (PACE) communications plans through telemetry-driven routing decisions. The presentation will discuss architectural patterns that leverage network performance measurements, link availability, security status and mission priorities to dynamically add and operate network nodes and select transport paths while remaining transparent to end users. These concepts extend traditional failover models by enabling adaptive routing across terrestrial, aerial, satellite and tactical networks in real time.

Finally, the session will also examine how AI-enabled operations and observability can improve network resilience and operational effectiveness and achieve continuous visibility across tactical and enterprise environments while automating responses to network degradation, cyber threats and infrastructure failures.

Attendees will leave with practical design patterns, implementation considerations and architectural insights for building resilient, self-healing and mission-aware communications infrastructures capable of supporting future Army and joint force operations across contested environments.

WHAT IS AFCEA?

AFCEA is a member-based, nonprofit association for professionals that provides highly sought-after thought leadership, engagement and networking opportunities. We focus on cyber, command, control, communications, computers and intelligence to address national and international security challenges.

The association has more than 30,000 individual members, 139 chapters and 1,600 corporate members. For more information, visit www.afcea.org