



# TechNet

---

## INTERNATIONAL

---

### INNOVATION SHOWCASE 2025

JUNE 4-5, 2025 • BRUSSELS, BELGIUM



**SIGNAL**  
AFCEA INTERNATIONAL MEDIA



# 2025 TechNet International Innovation Showcase

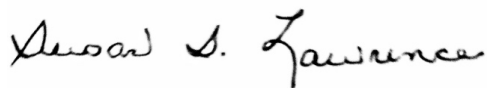
Exploring the Future: The Crucial Role of New Technologies and Global Cooperation in Advancing Defense and Security in the Digital Age

The landscape of command, control, communications, computers, cyber, intelligence, surveillance and reconnaissance (C5ISR) is rapidly changing, and exploring new technologies is more important than ever. During this two-day TechNet International conference, hosted by AFCEA Europe, defense information technology experts will have a chance to discuss evolving warfighting requirements and explore unconventional solutions.

AFCEA Europe's goal is to maintain and refresh the relationship between NATO, the EU, industry and academia, thus choosing Brussels as the home of the 2025 conference. Participants can network and debate on neutral ground, sparking insightful conversation between military, government and academia with a focus on new technology. The conference's exhibition showcase will feature industry leaders eager to get their innovative technologies in front of decision-makers and influential buyers. Exhibitors will have the opportunity to expand their presence in the European and NATO-wide marketplace.

Developing and integrating new technologies while strengthening global cooperation is essential to advancing defense and security in the digital age. AFCEA is determined to foster efficient and effective collaboration between industry and government to promote innovation in defense technologies. The companies and their innovative technologies below represent the future of security and defense in this digital world.

Best wishes,



**Lt. Gen. Susan S. Lawrence, USA (Ret.)**

President and CEO  
AFCEA International

# Table of Contents

Firmware: The Invisible Battlefield—Securing the Foundation of Modern Systems Christian Walter, Managing Director, Firmware, 9elements GmbH .....	9
Zero Trust: The Paradigm Shift for Critical Infrastructure Cybersecurity Derek Kernus, Chief Executive Officer, Aethon Security Consulting LLC .....	10
Symmetric Quantum Safe Authentication and Encryption for Modern Operations Phil Burn, Director of Professional Services, Arqit Ltd.....	11
Automating Insights Using LLMs in the Common Operating Picture Nathan Keegan, CTO for Booz Allen Europe, Booz Allen Hamilton.....	12
Data-Driven Defense: Harnessing AI and Data Cataloging for Strategic Advantage Caleb Loomis, Senior Data and AI Policy Analyst, Booz Allen Hamilton .....	13
The Importance of Fiber-Optic Sensing for Critical Infrastructure Protection and Maritime Domain Awareness Zack Spica, CEO, Ciena with Lumetec .....	14
Integrated Counter Unmanned Aerial Systems Training Chris Brewer, System Integration Engineer III, Client Solution Architects .....	15
Stakeholder Perspectives on Next-Generation Constructive Simulation: Bridging Transatlantic Requirements for Cloud-Based Training Charles Burrow, Exercise Planning Team Lead, Client Solution Architects .....	16
Repeatable, High-Fidelity, Up-To-Date Threat Emulation Exercises Are Crucial Experiences for Building Warfighters’ Muscle Memory Toward Readiness and Resilience Col. Anthony M. Perkins, USAF (Ret.), Head of Defense, CYBER RANGES .....	17
Global Cooperation of Secure Cloud Infrastructure Rapid Deployment: The Keio JRAMP Cloud Initiative Use Case Christopher Grady, Co-Founder and Chief Technology Officer, CyLogic .....	19
DoD Cyber Talent Management Mark Gorak, Principal Director for Resources and Analysis, Department of Defense .....	20

AI-Enabled Mission Command: The Future Is Here	
Karthik Srinivasan, Vice President, Defense & Intelligence Strategy, ECS Federal.....	21
Resilient LEO SATCOM in GNSS Degraded Environments	
Jonathan George, Senior Director of Business Development, Eutelsat America Corp. & OneWeb Technologies .....	22
AI Implementation in Defense: Navigating the Triad of Development, Evaluation and Adoption	
Brian Hensarling, Director of AI and Analytics, Far West Federal .....	23
The Rise of State-Sponsored Hacktivists: Targets, Techniques and an Intelligence-Based Outlook	
Simon Guiot, Security Researcher, Forescout .....	24
A Novel Data-Centric Coding Framework To Deliver 10X Enhanced Throughput, Secure and Resilient Data Communication	
Jing Song, Managing Director, Genesis Codes Inc.....	25
Preparing for Multidomain Operations: Essential Technological Foundations	
Richard Goodman, EMEA Defense Lead, Hexagon.....	26
Accelerating Multidomain Operations With Pentaho+ DataOps: Leveraging OSINT for Strategic Advantage	
Pragyansmita Nayak, Chief Data Scientist, Hitachi Vantara Federal .....	27
How Small Businesses Can Be Better Trained and Equipped To Combat Cyber Crime Committed by Nation-State Actors and Criminal Actors	
Joshua Huettner, Director of Operations, HuetTech LLC .....	28
Data-Centric Security: Classified Information vs. Classified Data	
Paolo Pezzola, Principal Sales and Account Manager - International Organizations, Infodas GmbH. ....	29
CEMA: Joint Cyber and EW Operations in the EMS With Feedback From Current Deployments and Multinational Operations	
Fulvio Arreghini, Head of Global Business, Infodas GmbH.....	30
From Document-Centric to Data-Centric Intelligence	
Peter Partridge, Director of Product Strategy (Solutions), Janes.....	32

Owning the Architecture	
Stefan Hefter, Partner, KPMG AG.....	33
Secure and RF-Free Data Communication With LiveDrop	
Martijn Antzoulatos-Borgstein, Senior Sales Director, Defense & Security, LiveDrop BV.....	34
Building an Intelligent Mission Environment	
Matthew Heideman, VP, Public Sector, Mattermost .....	36
Strategic Cyber Defense: Leveraging Diverse AI Solutions	
Roy Boivin, Federal COO, MixMode .....	37
Advancing Defense and Mission Outcomes by Leveraging Modern Data-Centric Security, AI and Intelligent Data Infrastructure	
Jim Cosby, CTO, Public Sector and Partners, NetApp U.S. Public Sector Inc. ....	38
Enhancing Multidomain Cyber Operations With ZeroLens	
Terry Dunlap, SVP Corporate Strategy & Development, NetRise .....	39
Pushing the Limits: The Future of Modern Satcom	
Emma Snowden, Business Development, Paradigm.....	41
Post-Quantum Cryptography: Safeguarding Europe's Digital Future	
Matthias Christian Brickel, Global Commercial Business Manager, PQShield .....	42
Challenges for Technology Talent in the New Era of Government Contracting	
Jake Frazer, President, Precision Talent Solutions.....	43
The AI-Driven SDR and Covert Communication	
Ion Gheorghisor, Director, Project Management Services SRL.....	45
Building the Foundation for AI/ML and GenAI in Government: Why Data as a Service Is Critical	
Jae Yi, Managing Director, Emerging Technology, Recro.....	47
Stream Data and Applications Between the Core and the Edge: A Proposed Framework To Accelerate the Time to Mission and Maximize Resilience and Interoperability in Multidomain Operations	
Giuseppe Magnotta, Associate Principal Solution Architect, Red Hat .....	49
Securing Velocity: How CI/CD and Compliance Drive Digital Transformation in Defense	
Luke Strebel, Senior Product Manager, Rise8 .....	51

Generative AI for ITOps	
Lee Koepping, Chief Technologist, ScienceLogic.....	53
Introducing an AI-Assisted Cost-Benefit-ROI Model for U.S. AI Use Cases	
Jim Liew, Founder, SoKat Consulting LLC.....	55
Rugged, Low-Power, High-Performance and Portable Edge Infrastructure	
Manavalan Krishnan, Co-Founder and CTO, Tsecond Inc.....	57
Tackling Global Security Challenges With GenAI	
Nick Bray, CBE, Vice President of Global Defense and Security, Vantiq .....	58
Spill Coffee Not Data: How To Secure Sensitive Assets and Avoid Being Roasted by Adversaries	
Andrew Forsyth, Director of Business Development, Varonis U.S. Public Sector LLC .....	59
Encryption as a Weapon: Preparing for the Inevitable Impact of Artificial Intelligence Fortified by Quantum Computing	
Joseph Warren, Encryption Strategist, Viasat.....	60
Empowering Defense in the Digital Age: Secure, On-Premise Geospatial Intelligence	
Bart Adams, CTO, xyz.ai .....	61

Submissions



# Firmware: The Invisible Battlefield— Securing the Foundation of Modern Systems

**Christian Walter, Managing Director Firmware, 9elements GmbH •**

christian.walter@9elements.com

## ABSTRACT

Firmware is the foundational layer of every modern computer system—yet it often remains overlooked in cybersecurity strategies. As digital infrastructure becomes a critical component of modern warfare, firmware emerges as a key attack surface, capable of undermining system integrity at the deepest level. This talk explores the role of firmware in modern computing, the risks posed by closed and proprietary implementations and how open-source firmware can strengthen transparency, resilience and trust in mission-critical environments. Drawing from real-world examples, we'll examine how secure firmware development practices are becoming essential for operational readiness.

**BIO:** Christian Walter is the managing director of 9elements Cyber Security and co-founder of Blindspot Software, where he focuses on advancing open-source firmware and secure firmware development practices. With a background in low-level software engineering and a strong track record in enabling secure and transparent firmware solutions for critical infrastructure, Walter has been at the forefront of driving adoption of open-source firmware in the defense, aerospace and enterprise sectors. He is an active contributor to projects like coreboot and openBMC, and he's a founding member of the Open-Source Firmware Foundation.

# Zero Trust: The Paradigm Shift for Critical Infrastructure Cybersecurity

**Derek Kernus, Chief Executive Officer, Aethon Security Consulting LLC •**

derek.kernus@aethonsecurity.com

## ABSTRACT

The escalating cyber threat landscape necessitates a paradigm shift in critical infrastructure cybersecurity. Implementing zero trust architecture (ZTA) is crucial for fortifying defenses, particularly within sectors requiring stringent compliance like the national defense organizations and their contractors. Traditional perimeter-based security is increasingly vulnerable to sophisticated attacks; ZTA, with its “never trust, always verify” principle, offers a robust alternative. This approach demands rigorous authentication and continuous monitoring for every access request, regardless of user or device location.

Integrating ZTA within regulatory requirements enhances security across multiple cybersecurity control groups, including access control, system and information integrity, and incident response. Granular control and continuous verification, inherent in ZTA, support “need-to-know” and “least privilege” principles, improving anomaly detection and limiting lateral movement during incidents.

Beyond enhanced security, ZTA improves operational efficiency and agility. It reduces the attack surface, minimizes incident impact and facilitates flexible security frameworks for modern work environments. However, implementing ZTA requires significant planning, investment in technologies like MFA and network segmentation, and comprehensive employee training.

Despite implementation challenges, ZTA's long-term benefits are substantial. It provides a proactive, adaptive security model aligned with evolving cyber threats, strengthening an organization's compliance posture and overall resilience. This presentation explores ZTA's practical implications for critical infrastructure, offering implementation ideas and tools for enhancing security posture.

**BIO:** Derek Kernus is the CEO of Aethon Security, a CMMC Level 2 Certified MSSP that supports cybersecurity efforts for U.S. defense contractors, specializing in DFARS 252.204-7012 and CMMC Level 2 compliance. He designs and implements CMMC requirements using the ZTA concepts and ensures thorough documentation via system security plans aligned with NIST SP 800-171A. He and his team have already guided multiple contractors, from SMBs to enterprise organizations, to earn their own CMMC Level 2 certifications. Kernus holds the CISSP and CCSP certifications, Lead Certified CMMC Assessor designation and an MBA from The College of William and Mary.

# Symmetric Quantum Safe Authentication and Encryption for Modern Operations

Phil Burn, Director of Professional Services, Arqit Ltd. • [pbriscoe@blueplanet.com](mailto:pbriscoe@blueplanet.com)

## ABSTRACT

As organizations embrace a more dynamic, remote and interconnected digital landscape, the traditional security perimeter has become obsolete. The zero trust security model assumes no trust by default and requires continuous verification of users and devices, emerging as a critical strategy to safeguard sensitive data and systems.

This talk explores integrating continuous authentication with quantum-safe symmetric keys and ratcheting mechanisms within a zero-trust framework. Symmetric key cryptography is a highly efficient and secure method for authentication. This unique method enables fast, scalable authentication, while ratcheting continuously evolves cryptographic keys with each interaction, ensuring compromised keys can't be reused, thus reducing long-term exposure risks.

This novel solution enhances session security by independently verifying and continuously refreshing each authentication event. This supports a real-time security posture, ideal for high-risk environments where frequent reauthentication and key updates are needed to counter evolving threats. Implementing ratcheting symmetric keys allows organizations to maintain a dynamic and resilient security architecture that adapts to modern cyber threats, effectively enforcing zero-trust principles.

This approach is scalable, performant and secure, addressing key challenges in maintaining security without sacrificing operational efficiency, particularly in large, distributed environments. Applications span the breadth of data in transit use cases, from 5G and deployed radio networks to autonomous systems and C4ISR, supporting interoperability, scalability and flexibility in a challenging changing environment.

**BIO:** Phil Burn is the director of professional services at Arqit, a cybersecurity company leading in high assurance, scalable, quantum-safe security. He is an innovator and an integration specialist with a proven track record of delivering successful projects across a diverse range of industries, including telecommunications, government, defense and IoT.

He has led multiple award-winning projects, with recent highlights including 2x GLOMO awards at MWC24 (CTO Choice: Outstanding Mobile Technology and Best Mobile Security Solution), The Cyber Defence Product of the Year 2024 and the IET Communications and IT Award 2023. He has an MSci in natural sciences from the University of Cambridge, specializing in physics.

# Automating Insights Using LLMs in the Common Operating Picture

**Nathan Keegan, CTO for Booz Allen Europe, Booz Allen Hamilton •**

marlin.mcfate@cohesity.com

## ABSTRACT

The increasing complexity of military operations requires innovative solutions to manage and interpret vast amounts of real-time data. In this context, automating insights through large language models (LLMs) presents an opportunity to enhance common operating pictures (COPs) and improve decision-making processes.

We propose showcasing how LLM APIs can be leveraged to automatically generate summaries, identify trends and provide actionable insights without the need for human intervention. By integrating LLMs into a COP, data from multiple sources—such as intelligence reports, mission updates and publicly available information—can be processed and distilled into clear, concise summaries. These insights will empower commanders to make more informed decisions rapidly, enhancing interoperability among partner nations. The ability to automate these tasks will reduce cognitive load, increase the efficiency of information processing and support faster reaction times.

At TechNet Europe, we aim to demonstrate the feasibility of this approach and discuss its potential to improve operational effectiveness and decision support across NATO forces. Additionally, we will explore the implications of LLM-driven automation on future command and control capabilities and outline pathways for integrating this technology into future federated interoperability efforts.

**BIO:** Nathan Keegan is the chief technology officer for Booz Allen Europe. He is responsible for comprehensive technical strategy across 11 countries in Europe, delivering technical implementation on major contracts and leading hiring, upskilling and training for all technical employees.

Keegan joined Booz Allen in 2015 and has over a decade of experience leading technical teams in the private (energy, aviation, pharmaceutical) and public (Treasury, DoD) sectors. He has worked across the commercial, civil and JCC markets and has supported Booz Allen in Singapore, Malaysia, Brazil, Germany and Italy. He is a Boren Fellow, a certified AWS practitioner and a certified Databricks architect who has delivered a number of emerging technical capabilities during his tenure at Booz Allen, including AI, computer vision, large language models and integrated lakehouses.

# Data-Driven Defense: Harnessing AI and Data Cataloging for Strategic Advantage

**Caleb Loomis, Senior Data and AI Policy Analyst, Booz Allen Hamilton •**

loomis\_caleb@bah.com

## ABSTRACT

Big data and artificial intelligence (AI) are transforming military operations and NATO's strategic capabilities, presenting both opportunities and challenges. Effective data cataloging is crucial for defense organizations to overcome inefficiencies. Our organization has developed a centralized framework that consolidates data assets into a unified environment enriched with metadata. This framework ensures real-time data availability, empowering military data stewards to maintain integrity and mitigate latency issues. AI-driven applications, like chatbot-based data discovery, enhance accessibility, understandability and reuse.

In this presentation, we will outline practical steps to unlock the value of our data holdings using AI. We will demonstrate how advanced data cataloging can streamline governance processes and improve decision-making across military operations. This, in turn, will save time and enable AI-powered insights critical to national security. We will also explore strategies to transform NATO's big data approach and drive defense innovation.

**BIO:** Caleb Loomis is the senior data and AI policy analyst at U.S. European Command, where he drives initiatives to centralize data, automate processes and leverage AI to inform decision-making. As a champion of innovation, Loomis fosters a culture of collaboration and creativity, frequently organizing and participating in hackathons to bring people and ideas together. With a background in open-source intelligence and digital forensics, Loomis' academic foundation includes a B.A. in government from Patrick Henry College, an M.S. in digital forensics from Champlain College and ongoing studies in the Chief Data and Artificial Intelligence Officer Program at Carnegie Mellon University.

# The Importance of Fiber-Optic Sensing for Critical Infrastructure Protection and Maritime Domain Awareness

**Zack Spica, CEO, Ciena with Lumetec • [zspica@lumetec.com](mailto:zspica@lumetec.com)**

## ABSTRACT

Subsea fiber networks carry over 95% of global data. These cables facilitate internet access, financial transactions and communications and are part of our critical infrastructure. Unfortunately, they are increasingly prone to failure and sabotage—risks that are costly for many industries and potentially threaten our economic stability.

NATO's recent "Baltic Sentry" initiative responds to incidents in the Baltic Sea and demonstrates the importance of safeguarding subsea fiber cables. This initiative recognizes that such systems are vital for national security and global economic stability. Protecting such infrastructure over vast regions is challenging and demands multiple layers of security and cooperation. A key component toward that goal is enabling these networks to self-monitor, transforming them into high-fidelity sensors.

Fiber-optic sensing technologies using distributed acoustic sensing, state of polarization or even carrier phase tracking enable real-time high-resolution monitoring fibers. By converting tens to thousands of kilometers of cable into distributed sensors, these methods equip networks to gather detailed intelligence on their surroundings and detect both imminent and approaching threats. Integrating artificial intelligence and machine learning amplifies these capabilities, creating new possibilities in critical infrastructure protection, pipeline surveillance, perimeter security, maritime traffic management, MASINT and coastal surveillance.

Leveraging fiber networks to protect themselves offers unprecedented early detection of anomalies, preventing expensive outages and bolstering infrastructure security worldwide. We will discuss emerging sensing capabilities of next-generation coherent modems and the kinds of AI/ML processing that can be applied to yield a holistic warning and monitoring system for critical fiber infrastructure.

**BIO:** Zack Spica is a leading fiber-optic sensing expert, recognized for his pioneering contributions to the field for over a decade. He studied fiber-optic sensing at Stanford University and the University of Tokyo and currently leads a top research group at the University of Michigan, specializing in subsea fiber sensing.

# Integrated Counter Unmanned Aerial Systems Training

**Chris Brewer, System Integration Engineer III, Client Solution Architects •**

christopher.brewer@csaassociates.com

## ABSTRACT

Recent events in Eastern Europe have transformed modern warfare, shifting from cumbersome and costly armored brigades to small, inexpensive and highly effective drone units. Adversaries across the board have either stood up or are standing up dedicated drone warfare units. We must quickly adapt our training and simulation programs to meet this new battlefield by utilizing a blend of COTS and GOTS hardware and software to rapidly develop integrated counter UAS (C-UAS) and counter small UAS (C-sUAS) training solutions using as much existing technology as possible to reduce costs and implementation time. There are currently several standalone training programs that either use actual drones and counter drone weaponry or virtual reality solutions; however, none of them can integrate into our existing simulations, such as Virtual Battlespace, which relates to little more than individual training. It is imperative that units learn to meet drones on the battlefield as a cohesive front in a simulated environment where the conditions and parameters can be changed and reset within minutes.

The Stryker Virtual Collective Trainer (SVCT), which uses the Virtual Battlespace (VBS3) simulation as the base, could be coupled with multiple external virtual reality training platforms in a modular, reconfigurable format capable of providing that training environment at a fraction of the cost for not just U.S. forces but all allied nations.

**BIO:** Chris Brewer is a U.S. Army Field Artillery veteran and simulations engineer with 14 years of international small- and large-scale simulations experience and multiple cyber security certifications.

# Stakeholder Perspectives on Next-Generation Constructive Simulation: Bridging Transatlantic Requirements for Cloud-Based Training

**Charles Burrow, Exercise Planning Team Lead, Client Solution Architects •**

charles.burrow@csaassociates.com

## ABSTRACT

This abstract analyzes stakeholder perspectives on the U.S. Army's Next-Generation Constructive (NGC) simulation, focusing on NATO and allied participation requirements. Driven by the need for streamlined development, cost efficiency and agile training delivery, the NGC initiative seeks to transition constructive simulations to a cloud-based environment. This shift necessitates a comprehensive assessment of stakeholder needs, particularly those of NATO and allied nations, to ensure seamless integration and interoperability.

Analyzing the NGC initiative through the DOTMLPF-P lens reveals critical requirements from our perspective in a European theater. Doctrinally, NGC must reflect allied operational concepts and procedures, fostering a common understanding of multidomain operations. Organizationally, the initiative necessitates clear frameworks for data sharing, security protocols and collaborative development between the United States and its allies. Training implications include establishing standardized curricula, incorporating diverse language requirements and ensuring equitable access to the cloud-based platform. Materiel considerations encompass the compatibility of allied command and control systems with NGC, necessitating robust interoperability testing and potential technological adaptations. Leadership and personnel aspects highlight the need for cultural sensitivity, collaborative planning and inclusive decision-making processes involving all stakeholders. Facilities and policy considerations involve establishing secure cloud access points for allied nations, harmonizing data governance frameworks and navigating potentially divergent national policies on data security and sovereignty.

Meeting these requirements is crucial for NGC's potential. A collaborative approach, reflecting NATO and allied nations' perspectives, will ensure a robust, interoperable and effective cloud-based simulation environment capable of supporting collective training objectives in an increasingly complex security environment.



# Repeatable, High-Fidelity, Up-To-Date Threat Emulation Exercises Are Crucial Experiences for Building Warfighters' Muscle Memory Toward Readiness and Resilience

**Col. Anthony M. Perkins, USAF (Ret.), Head of Defense, CYBER RANGES •**

a.perkins@cyberranges.com

## ABSTRACT

To date, the United States, NATO allies, the European Union and Ukraine have been sharing valuable attack analyses, malware samples and threat intel mostly by means of workshops and tabletop exercises.

TRYZUB (i.e. trident) is a unique operational program developed by Ukraine's State Service for Special Communications and Information Protection (SSSCIP) and CYBER RANGES. This private-public partnership offers the unique advantage of fast-designing, fast-building and fast-sharing cyber attack experiences through repeatable, high-fidelity emulations for training and fast-track practice toward the acceleration of preparedness, resilience and deterrence.

This presentation will address the following key objectives of effective cyber exercises:

"What if we could safely put our organization through a real cyber attack, with real malware and artifacts, and have that attack unfold in a high-fidelity sandbox environment where we can observe our teams respond to it?"

"What if we could experience the attack without the negative impact and play and replay it at will until our team has developed the necessary muscle memory to deal with it in the field?"

"What if, besides the IoCs and threat information, we would actually timely share the experience of dealing with the actual attack among our allies?"

Brig. Gen. Oleksandr Potii, head of Ukraine's SSSCIP, will be able to connect remotely, join the presentation and share his team's field experience in developing these cyber exercises.

**BIO:** Tony Perkins is a distinguished leader with over two decades of experience in business strategy, portfolio management and cybersecurity, specializing in delivering growth and operational excellence across public and private sectors.

A retired U.S. Air Force colonel, Perkins commanded critical cyberspace and communications units, directing operations for over a thousand personnel across multiple geographies and managing multimillion-dollar budgets.

Perkins' unique blend of technical expertise, strategic vision and leadership acumen drives innovative solutions and success in complex, high-stakes environments.

Perkins holds a master's degree in telecommunications management from George Mason University and a bachelor's in business administration from the U.S. Air Force Academy.

# Global Cooperation of Secure Cloud Infrastructure Rapid Deployment: The Keio JRAMP Cloud Initiative Use Case

**Christopher Grady, Co-Founder and Chief Technology Officer, CyLogic •**

Chris.Grady@cylogic.com

## ABSTRACT

Keio University, a leading research institution in Japan, sought to establish a highly secure private cloud to demonstrate that advanced cybersecurity infrastructure could be rapidly deployed in that region. The initiative aimed to support national security efforts and enhance Japanese collaboration with U.S. military branches in the Asia Pacific theater.

To meet this challenge, CyLogic partnered with a leading global data center and network provider to design and implement a Japan-specific version of its managed FedRAMP High Ready/IL5-aligned integrated cloud solution. This deployment was successfully deployed geographically in under six weeks including all logistics—a fraction of the time that comparable solutions typically require.

The result was the Keio JRAMP Cloud, a functioning FedRAMP High Ready IL5-aligned cloud in Tokyo with private transpacific network connectivity delivering under 140 milliseconds of latency to support NOC, SOC, continuous monitoring and all other functions from the United States. This project not only proved that secure cloud systems could be established in record time, globally, but also set a new standard for highly dispersed cloud deployments, taking the cloud operating model back to the edge, on-prem or as a sovereign cloud for U.S. ally countries. The initiative demonstrated the technological capabilities to support the global coordination between U.S. and Department of Defense mission partners to rapidly enhance joint security posture to meet national and international defense requirements.

**BIO:** Christopher Grady is the co-founder and chief technology officer of CyLogic, developer of CyCloud, a FedRAMP High Ready Cloud Platform. With over 30 years of experience, his background spans from working on one of the first U.S. drones used in combat by the U.S. Marine Corps to spending the last 15 years of his career focused on designing and implementing highly secure, enterprise cloud architectures from a security-first perspective. As a recognized expert in cloud architecture and cybersecurity, Grady has advised Global Fortune 500 companies and was an early pioneer in the FedRAMP process, leading one of the first Cloud Service Providers through the FedRAMP Joint Authorization Board certification process in 2014. He has also served as a lecturer in the graduate information assurance program at Georgetown University, sharing his extensive expertise in cybersecurity.

# DoD Cyber Talent Management

**Mark Gorak, Principal Director for Resources and Analysis, Department of Defense •**

matthew.m.isnor.civ@mail.mil

## ABSTRACT

In today's rapidly evolving threat landscape, the U.S. Department of Defense (DoD) faces an unprecedented challenge: maintaining its technological edge against increasingly sophisticated cyber adversaries. The solution lies in cultivating a robust and agile digital workforce capable of meeting these challenges head on.

This keynote presentation will underscore the urgent imperative for the DoD to prioritize the development of its cyber workforce. It will delve into the critical role of education and training in forging a highly skilled and adaptable force capable of meeting the evolving challenges within the cyber domain. The presentation will emphasize the importance of a collaborative and multidisciplinary approach to equip cyber professionals with the knowledge and expertise needed to ensure national security.

Attendees will gain valuable insights into the future of the DoD Cyber Workforce Framework, the DoD 8140 Cyberspace Workforce Management and Qualification Program, and the Cyber Excepted Service. The presentation will highlight how these programs, alongside targeted development initiatives, are shaping a dynamic and responsive workforce equipped to tackle emerging cyber threats.

By exploring the DoD's holistic talent management strategy, this keynote will inspire attendees to embrace innovative solutions and commit to building a future-proof cyber workforce capable of safeguarding national security in the digital age.

# AI-Enabled Mission Command: The Future Is Here

**Karthik Srinivasan, Vice President, Defense & Intelligence Strategy, ECS Federal •**

karthik.srinivasan@ecstech.com

## ABSTRACT

The time we have to receive data, analyze, consider alternatives, plan and deploy shrinks the closer we get to the action. The decision space, regardless of physical distance, is compressed even further with the development of swarm drones, hypersonic weapons that travel at five to seven times the speed of flight path. AI becomes a necessity as an agent more than a tool to enable mission command decision support today more than ever before. This presentation will discuss the remarkable surge of AI advancement to support current and future warfare, enabling multidomain operations, application of AI in a complex cyber and space domain, and the electromagnetic spectrum and how the U.S. Army is at the forefront of rapidly exploiting windows of superiority. This presentation will also discuss how Modular Open Systems Approach (MOSA), developments in infrastructure and simulation powered by AI will drive rapid deployments.

**BIO:** Karthik Srinivasan is the vice president of Defense & Intelligence Strategy at ECS. He is responsible for strategy and delivery of mission-oriented solutions across all of ECS Defense & Intelligence agencies. In his role, Srinivasan oversees the growth and operations of a diverse portfolio of leading-edge digital transformation services, advanced analytics and AI, cybersecurity and enterprise modernization programs.

Srinivasan has over 30 years of experience leading large federal and commercial accounts and driving innovation. He is a frequent speaker at AFCEA, AUSA and homeland security events. He holds executive leadership certifications from University of Michigan and Cambridge University (UK) and an MBA from Wayne State University.

# Resilient LEO SATCOM in GNSS Degraded Environments

**Jonathan George, Senior Director of Business Development, Eutelsat America Corp. & OneWeb Technologies • [jonathan.george@eacowt.com](mailto:jonathan.george@eacowt.com)**

## ABSTRACT

Due to the nature of LEO SATCOM orbital dynamics, user terminals require accurate positioning and timing to connect with the satellites, which is normally achieved through an internal Global Navigation Satellite Services (GNSS) receiver. If this signal is degraded or denied, it can significantly affect LEO SATCOM communications. To provide our customer base a reliable complimentary GNSS solution, EACOWT developed an external A-PNT receiver called AstraPNT. AstraPNT is a software-defined receiver capable of receiving PNT signals from GNSS and multiple alternate sources and bands, processing, identifying the best source of PNT and converting that signal to a common SMA port with an output compatible with the standard GPS L1 interface. These alternate sources of PNT can range from L-band (Iridium and Inmarsat) and S-band (GlobalStar) to other frequencies as broadcast capabilities. AstraPNT provides users the PNT resilience necessary to operate in GNSS-challenged environments.

**BIO:** Jonathan George is a retired U.S. Marine Corps intelligence officer with a vast background in intelligence operations, electronic warfare and space operations. In his current role, he serves as the senior director of business development for Eutelsat America Corp. & OneWeb Technologies.

# AI Implementation in Defense: Navigating the Triad of Development, Evaluation and Adoption

**Brian Hensarling, Director of AI and Analytics, Far West Federal •**

brian.hensarling@farwestfederal.com

## ABSTRACT

Defense organizations face mounting pressure to rapidly implement artificial intelligence across the operational spectrum yet cannot afford the consequences of failed initiatives. The journey from concept to operational capability involves three critical elements—development, evaluation and adoption—each presenting unique and significant challenges. This presentation examines how these interconnected elements form a decisive triad that ultimately determines whether AI-optimized systems succeed or fail in defense applications, offering practical frameworks to navigate this complex landscape.

Our approach addresses development challenges by balancing upfront requirements with in-stride adjustments, emphasizing deep customer engagement within agile methodologies and embedding DevSecOps throughout, rather than attempting to bolt it on as an afterthought. This foundation ensures flexibility, security and interoperability are built in from inception.

For evaluation, we present frameworks that account for the inherent randomness of generative AI systems, discuss how to establish meaningful metrics aligned with operational outcomes and embrace the reality that AI systems continuously evolve through use; software is never truly “done.”

The adoption phase often determines ultimate success, requiring developers to deeply understand operational processes and pain points, to identify and support “super users,” to acknowledge legitimate resistance factors (i.e. “adoption drag”) and to establish feedback mechanisms that drive iterative improvement.

Drawing from Far West Federal’s experience supporting defense organizations, this presentation offers practical strategies to navigate these challenges, providing defense stakeholders with actionable frameworks to accelerate responsible AI integration and maximize the impact and chances of success of critical security initiatives.

**BIO:** Brian Hensarling is currently the director of AI and analytics at Far West Federal, a leading provider of applied AI and digital transformation for the U.S. government. Prior to taking his current role, Hensarling served 21 years in the U.S. Marine Corps, initially as an attack helicopter pilot, before completing his career as the program lead for an AI software development project at the U.S. Department of Defense’s (DoD’s) Chief Digital and Artificial Intelligence Office. In that role, he presented his work in many forums, including the U.S. National Institute of Standards and Technology’s Software and Supply Chain Assurance Spring Forum and the DoD Supply Chain Security Leadership Forum.

# The Rise of State-Sponsored Hacktivists: Targets, Techniques and an Intelligence-Based Outlook

**Simon Guiot, Security Researcher, Forescout** • [simon.guiot@forescout.com](mailto:simon.guiot@forescout.com)

## ABSTRACT

Hacktivist groups, formerly independent actors with a sociopolitical agenda, have been increasingly aligning with nation-state interests in geopolitical conflicts. These groups expanded their techniques beyond website defacements and distributed denial of service to include disruption of cyber physical systems within critical infrastructure via exploitation of vulnerable connected devices.

State-sponsored actors also started adopting hacktivist personas to conduct cyber attacks. Examples include the Iranian Cyber Av3ngers and the Cyber Army of Russia Reborn. This shift may be driven by several strategic factors, such as enhanced campaign visibility and plausible deniability for the perpetrators.

In this session, we will detail an analysis of 780 hacktivist attacks in 2024, claimed by four groups operating on opposing sides of the Russia-Ukraine and Israel-Palestine conflicts. This analysis includes targets, techniques, goals and, most importantly, defensive actions that can be taken based on this intelligence. We will also discuss how we expect state-sponsored hacktivist groups and techniques to develop in 2025 and beyond.

**BIO:** Simon Guiot has been a researcher on Forescout's Vedere Labs team for three years, specializing in threat intelligence and honeypots. He was invited to speak at multiple cybersecurity conferences, like BlackHat US or leHack in France. He strives to make his work and that of his colleagues useful and accessible.



# A Novel Data-Centric Coding Framework To Deliver 10X Enhanced Throughput, Secure and Resilient Data Communication

**Jing Song, Managing Director, Genesis Codes Inc.** • [song@genesis-codes.com](mailto:song@genesis-codes.com)

## ABSTRACT

Genesis Codes has developed a data-centric software solution that revolutionizes data movement with unparalleled speed, security and resilience. Our technology delivers 10-100 times enhanced data throughput compared to current internet standards (TCP/IP), 2-20 times bandwidth reduction, superior data integrity and enhanced resilience, even under challenging network conditions. Trusted by the U.S. military, our solution leverages the fast performance of the UDP protocol, addressing its unreliability with innovative forward error correction. Operating at the data packet level, our solution enhances transport efficiency across any packet-switching network. It is compatible with all hardware, systems and communication technologies, ensuring exceptional data resilience against interference, accelerating global data movement and streamlining cloud operations. We've demonstrated exceptional performance (10 times enhanced throughput, while maintaining 99.999% delivery guarantee, same as TCP) across channels like satellite, cellular, tactical radio and the global internet. Our advancements in channel coding (FEC), data transport, compression and encryption deliver superior performance across multiple channels, including the global internet, Starlink, cellular networks, RF and optical communication. With limitless application potential, our technology propels industries into new realms of efficiency, security and reliability.

**BIO:** Jing Song is the co-founder and managing director of Genesis Codes. He is a serial entrepreneur, founder and CEO of several high-tech companies: Apemesh, Datamart, etc. Formerly, he was a Xerox executive and led a team to develop more than 10 high-tech products and solutions, generating a combined sale of \$2 billion. Song is a business-driven technologist and strategist with tracking records to deliver business results with technology products. He earned a master's degree in electrical and computer engineering and an MBA from the University of Rochester.

Besides his accomplishments, Song represents Genesis Codes, a team of several leading scientists and engineers with more than 120 years combined of related industry and academic experience. They are inventors of more than 120 U.S. and international patents and authors of more than 200 technical papers. They have been working for well-known high-tech companies: Google, Amazon, Meta, Sony, IBM and Xerox. They are serial entrepreneurs working hard to explore deep tech. They all graduated from top universities with advanced degrees.

# Preparing for Multidomain Operations: Essential Technological Foundations

**Richard Goodman, EMEA Defense Lead, Hexagon • [richard.goodman@hexagon.com](mailto:richard.goodman@hexagon.com)**

## ABSTRACT

There are many aspects being discussed around the concept and implementation of multidomain operations (MDO), whether at national or international levels. With building blocks such as digital backbone, culture, assurance, integration, processes and agility, the actual technology could be overlooked. Whilst COTS technology may be ahead of defense in terms of development rates nowadays, there are various foundational blocks that technology needs to have to work in MDO, or any mode of operations. These foundations include interoperability, the ability for software and systems to exchange and make use of information, and standards that help achieve interoperability, however need to require levels of detailed information to make the exchange worthwhile. Technology needs to be open and useable, in that today's service personnel understand its purpose and operation easily, fit for purpose and current. Plus, there is the data, the lifeblood of the systems, with its access and sharing issues and semantics of attributes. By looking at these and other foundations, this talk will highlight what commercial companies and defense agencies can be doing now to be ready to fight using MDO. Examples will be given of relevant and current implementations exemplifying these foundation blocks.

**BIO:** Richard Goodman is a geography graduate with a background in geographic data production, software support and presales. His current role involves business development for Hexagon around defense, setting strategy, gaining market recognition within defense agencies and supporting the wider sales team and partners.

Initially working in photogrammetry and with early digital cameras for aerial survey, Goodman led a department capturing mapping data, telecoms data and creating ortho images and elevation data from aerial images.

Having moved to Hexagon, Goodman has worked in customer-facing roles such as software support, training provision, presales and business development, often multitasking. His technical knowledge includes geographic data management, exploitation, analysis and visualization. Industries he has worked with include national mapping agencies, defense, utilities and transportation.

# Accelerating Multidomain Operations With Pentaho+ DataOps: Leveraging OSINT for Strategic Advantage

**Pragyansmita Nayak, Chief Data Scientist, Hitachi Vantara Federal •**

[pragyan.nayak@hitachivantarafederal.com](mailto:pragyan.nayak@hitachivantarafederal.com)

## ABSTRACT

The modern battlespace demands rapid, data-driven decisions across land, sea, air, cyber and space with trusted data and robust AI infrastructure as the critical backbone of the solution architecture. Seamless integration of open-source intelligence (OSINT)—including publicly available information (PAI) and commercially available information (CAI)—is essential for multidomain operations (MDO), with NATO-EU collaboration critical for interoperability and mission success.

This session highlights how the Pentaho DataOps platform empowers military data scientists by automating OSINT aggregation, analysis and orchestration. Pentaho's open architecture accelerates multisource ingestion, transformation and analysis, providing real-time insights for faster, informed decisions. Learn how Pentaho automates intelligence cycles, integrates PAI and CAI, and enhances situational awareness with AI-powered analytics and automated data pipelines with streamlined and secure information sharing. Pentaho fortifies operational and tactical analytics using machine learning for anomaly detection, predictive maintenance and threat analysis.

Join us to see how Pentaho DataOps drives multidomain integration, accelerates OSINT workflows and strengthens transatlantic security in a rapidly evolving threat landscape.

**BIO:** Pragyansmita Nayak serves as the chief data scientist at Hitachi Vantara Federal, where she bridges the “art” and “science” of data-centric solution architectures. Her expertise lies in orchestrating data, APIs, algorithms and applications to deliver cutting-edge solutions. With over 25 years of experience in software development and data science, her specialties include analytics, machine learning, deep learning and generative AI. Nayak has successfully led numerous projects for diverse U.S. federal government agencies, spanning both U.S. Department of Defense and civilian sectors. Her work encompasses areas such as federal accounting, operational analytics, data mesh, object storage, metadata management, records management and data governance.

Academically, Nayak holds a Ph.D. in computational sciences and informatics from George Mason University and a B.S. in computer science from BITS Pilani, India. She is a prolific contributor to the AI and data science community, having published and presented her work at esteemed conferences such as AFCEA West, AFCEA TechNet Cyber, AFCEA TechNet Transatlantic, NLIT and BrightTalk summits. She has also delivered guest lectures at institutions like George Mason University, George Washington University and the National Defense University.

# How Small Businesses Can Be Better Trained and Equipped To Combat Cyber Crime Committed by Nation-State Actors and Criminal Actors

**Joshua Huettner, Director of Operations, HuetTech LLC •**

joshua.huettner@huettect.com

## ABSTRACT

Small businesses are increasingly targeted by nation-state cyber actors but often lack the resources to defend themselves effectively. This paper explores how small businesses can be better trained and equipped with free or low-cost cybersecurity tools to combat these threats. It examines practical, accessible training programs that enhance cybersecurity awareness and response capabilities, as well as open-source and budget-friendly security solutions that mitigate risks. Additionally, the study highlights the role of government and industry initiatives in providing small businesses with affordable cybersecurity resources. By leveraging education, threat intelligence sharing and cost-effective tools, small businesses can strengthen their defenses against sophisticated cyber threats without significant financial strain.

**BIO:** Joshua C. Huettner was born in New Mexico and has traveled the world supporting the U.S. Department of Defense. He is a seasoned cybersecurity and intelligence professional with more than 22 years of experience in cyber defense operations, intelligence planning and risk management.

# Data-Centric Security: Classified Information vs. Classified Data

**Paolo Pezzola, Principal Sales and Account Manager - International Organizations,**  
Infodas GmbH • p.pezzola@infodas.de

## ABSTRACT

Military operations today increasingly rely on information superiority, crucial for decision dominance within MDO doctrines. Achieving this requires data to be available where and when needed, possessing specific characteristics to support decision-making. However, in real operational scenarios, the need to know often conflicts with the need to share, essential for mission success. The traditional mandatory access control (MAC) model, suitable for document and visual information exchange, shows limitations when applied to data.

The data-centric security (DCS) paradigm offers a solution, balancing the need to know and the need to share. DCS, part of NATO's strategic roadmap, enables the Alliance to deliver shareable, protected information, controlled for life. It redefines access control strategies, replacing the MAC model with the attribute-based access control (ABAC) model. This shift enhances interoperability in classified information exchange and transforms how information is protected and shared in the digital environment.

This contribution introduces the conceptual differences between classified information and data, outlines the challenges of applying legacy access control mechanisms in the digital world and how these strategies conflict with MDO doctrines. It also provides real examples of applying DCS to balance the need to know and the need to share.

**BIO:** Paolo Pezzola is an Italian navy captain (reserve), specialized in mines and mine countermeasures. After graduating from the Naval Academy in 2001, he served aboard mine hunters, patrol vessels, frigates and destroyers, occupying positions ranging from principal warfare officer to commanding officer. Throughout his career, Paolo served twice in the NATO Mine Countermeasures Standing Groups, as mine warfare officer and principal staff officer. From 2020 to 2022, he was posted as a seconded national expert in the European External Action Service in Brussels, as part of the European Military Staff. In 2022, after more than 25 years of service in the navy, during which he developed a rich toolbox of soft and hard skills, Pezzola decided to leave the navy and join Infodas, where he is now the principal sales and account manager – international organizations.

# CEMA: Joint Cyber and EW Operations in the EMS With Feedback From Current Deployments and Multinational Operations

**Fulvio Arreghini, Head of Global Business, Infodas GmbH •**

f.arreghini@infodas.de

## ABSTRACT

The concept of CEMA tries to bring together the EMSO and the cyber operation, starting from the awareness that, even if the real-world observable effect of most EW activities concentrates on the use and dominance of the EMS, under the hood, the functionality and ability of most modern EW systems to perform their mission is dependent on computer systems and networks.

In fact, EW systems today are exposed to new threats coming from the cyber world. In the general formulation of the CEMA concept, the attacker would mainly try to disrupt the capabilities of the victim system to accomplish its mission, which, in cybersecurity terms, may be considered equivalent to a denial-of-service (DoS) attack. Nonetheless, if we observe the recent tendencies of cyber warfare, it appears evident that the DoS strategy is less and less used for several reasons: It is quite easy to prevent and detect, and it produces a disruption on the victim's system as a unique effect.

If we analyze, for example, the evolution of malware in recent years, we will observe a predominance of ransomware, which is not anymore the elementary malware that was simply encrypting the data on the victim system (hence also in this case acting in a kind of DoS fashion) but has grown more and more sophisticated to include a complete kill chain, which starts with beaconing (the notification to the attacker that the malware has successfully reached the target system) and goes on with footprinting (gathering of information about the target system), exfiltration of data from the target system mainly in a silent and nondetectable way and eventually installation of RAT (remote access tools), allowing the attacker to gain a command and control capability on the target system. Only in its final stage, ransomware today deploys the encryption payload (after a significant quantity of data has been exfiltrated), allowing the attacker to perform the double extortion (threat of nondecrypting data and threat of selling/making public data that has been exfiltrated).

If we translate this modus operandi into CEMA, where the motivation of the attacker would be more political/tactical than economic, we may derive some considerations applicable to EW systems that make them vulnerable to some attack techniques.

First, EW systems are inherently exposed to a low classification domain, being the part of the system connected to the EW sensors and effectors. On the other side, an EW system inherently has a high classification security domain in it, which is where classified information is stored (e.g. EW libraries, frequency and jamming patterns) or assessed (e.g. correlation and fusion of EW observations with other data). This

makes EW systems inherently operating in a cross-domain environment and vulnerable to a kill chain similar to the one described for ransomware, where the ultimate goal of the attacker would not just be disrupting system functionalities, but stealing data about the system internals.

Second, EW systems are in general not operating standalone but as part of a mission network where they are connected to BMS/CMS systems, which can be eventually from other mission partners in joint and/or combined operations. In this case, we can see that one or more other security domains are being added to the scenario (e.g. the BMS system from a partner nation), and while information shall be shared with these systems, it is also important that some classified or sensitive pieces of information (such as the already quoted EW libraries) are protected from unintended leakage.

In conclusion, CEMA should not be analyzed just looking at the implication of a possible DoS attack coming from the EW spectrum and targeting the cyber portion of an EW system but should be looked at also from a wider cyber perspective, taking into account all the security domain transitions in an EW operation and being sure that the mission-critical data is safeguarded from unintended leakage. In fact, while the impact of a DoS attack could be easily mitigated, for example by using redundant independent systems, the loss of mission-critical data has a wider and deeper impact on the operational capability of the system, which goes well beyond the current mission disruption.

The proposed contribution analyzes the CEMA concept from a cyber point of view, taking into specific account the security domain transitions and the problem of data loss prevention.

**BIO:** Fulvio Arreghini is a retired commander of the Italian navy (engineering corps) with 25 years of active service, during which he was working mainly in the area of high security systems: C2, communication and cybersecurity.

He's been part of several multinational groups in NATO, EDA and industry organizations such as the Wireless Innovation Forum.

Since 2020 in the private sector, Arreghini has been the head of Global Business at Infodas GmbH, a leading company in the field of cross-domain solutions and cybersecurity consulting, with strong orientation to the defense market.

# From Document-Centric to Data-Centric Intelligence

**Peter Partridge, Director of Product Strategy (Solutions), Janes •**

[peter.partridge@janes.com](mailto:peter.partridge@janes.com)

## ABSTRACT

The transformation from a disconnected document-centric organization to an entity-based interconnected intelligence has been a journey that Janes has been on since early 2010. While the transformation was on unclassified data sets that were created using OSINT methodologies, the foundational principles and learning points also apply to classified environments and to overall data management and governance approaches. The new data models and ontologies that Janes has developed are allowing for far richer data discovery and interoperability across internal and third-party data sets, as well as providing foundational data to power RAG AI models to answer complex queries faster and more accurately and being used to train and build advanced NER models.

**BIO:** Heading up the product solutions team, Peter Partridge and his unit work closely with national security and defense industry clients on a global basis to support their integration and optimization of Janes data for a variety of missions. With over 25 years at Janes, Partridge has extensive experience as an analyst, manager and leader of teams, as well as in his current role of data structuring, modeling and supporting customers.



# Owning the Architecture

**Stefan Hefter, Partner, KPMG AG** • stefanhefter@kpmg.com

## ABSTRACT

Companies in the United States have unrivaled capacities for innovative, cutting-edge technological products. A lot of solutions for defense, especially in the command-and-control domain, incorporate these products. With recent developments in the United States, the question of technological sovereignty has become urgent again. This presentation will show a possible approach to combine the best products and sovereignty by having firm control over the architecture of solutions.

**BIO:** 01.22 – today: Partner Defense, KPMG AG Wirtschaftsprüfungsgesellschaft

06.21 – 12.21: Cluster Lead Defense & Intelligence, IBM Global Business Services

03.18 – 05.21: Partner IBM Global Business Services, Business Unit Leader Digitization

04.15 – 02.18: Associate Partner, IBM Global Business Services

09.11 – 03.15: Senior Managing Consultant, IBM Global Business Services

01.07 – 08.11: Department Head Inter- & Intranet, BWI Systeme GmbH

01.06 – 12.06: Senior Managing Consultant, IBM Global Business Services

03.01 – 12.05: Senior Consultant, IBM Software Group

Selected Projects:

- Digital media of the German armed forces (Bundeswehr.de, bmvg.de)
- SecuTABLET: high-security mobile device
- ConnectLw/ConnectBw: social business collaboration

# Secure and RF-Free Data Communication With LiveDrop

**Martijn Antzoulatos-Borgstein, Senior Sales Director, Defense & Security, LiveDrop BV** • [martijn@livedrop.eu](mailto:martijn@livedrop.eu)

## ABSTRACT

Modern military and security operations require secure, reliable and efficient communication channels for data transfer. Current solutions, including USB devices, Bluetooth, radio and satellite communications, are vulnerable to interception, jamming and spoofing.

LiveDrop introduces a revolutionary secure data transfer solution that ensures seamless and threat-resistant communication for defense and security forces.

LiveDrop enables encrypted, contactless data exchange without reliance on traditional networks, significantly enhancing operational security and flexibility.

Our white paper outlines the core technology, operational use cases and the distinct advantages LiveDrop provides to defense ministries and security organizations worldwide.

LiveDrop represents the future of secure, contactless military and security data transfer.

By eliminating vulnerabilities associated with conventional communication methods, it ensures that defense and security forces maintain a strategic advantage in cyber-secure operations. Defense ministries and security organizations interested in evaluating LiveDrop can request a classified briefing and live demonstration tailored to their operational requirements.

**BIO:** Martijn Antzoulatos-Borgstein is a senior leader with more than 21 years of experience in business management, strategy, global sales and CX, defense and security, digital transformation, global supply chain, SaaS, IaaS, cyber, IT security, public administration and compliance. Before joining LiveDrop BV as senior sales director Defense & Security, Antzoulatos-Borgstein held roles of increasing leadership responsibility with Rockwell Automation Inc., a United States-based global multinational in industrial automation and digital transformation.

Antzoulatos-Borgstein is also the owner of Antzoulatos Business Consulting, a venture erected to help the European security and defense sector become more competitive. Antzoulatos-Borgstein is a member of the Dutch liberal party VVD and its thematic network for defense.

In September 2023, Antzoulatos-Borgstein graduated cum laude from the Executive MBA Program of Maastricht University School of Business & Economics. He majored in sustainability and ethical leadership and was bestowed with the titles “best in class” and “student of the year 2023.”

Antzoulatos-Borgstein is a strong networker with a positive, can-do mindset. He thrives in fast-paced, complex environments where being strategic goes hand-in-hand with being pragmatic and solution-oriented. He effectively combines his extraordinary people skills with his hard skills and years-long, diversified experience to identify winning opportunities that he can drive to success together with his teams, stakeholders and partners.

Throughout his career, Antzoulatos-Borgstein has always been a trusted and respected leader and strategic adviser for C-Level executives and board members. He writes about macroeconomics, geopolitics, global security and international trade and provides strategic consulting in these areas. Antzoulatos-Borgstein's primary objective is to connect, inspire and achieve with his teams and partners, guided by his core values of empathy, integrity and excellence.

# Building an Intelligent Mission Environment

Matthew Heideman, VP, Public Sector, Mattermost • ssteinman@req.co

## ABSTRACT

Success in modern warfare depends on the ability to communicate, collaborate and act with speed and precision. As military operations grow more complex—spanning multiple domains, coalition partners and contested environments—maintaining seamless command and control is critical. Without the right infrastructure, our warfighters face delays, fragmentation and compromised decision-making.

This session will explore how global defense organizations can create intelligent mission environments that enable secure, real-time data sharing, automated workflows and resilient command-and-control structures. Matt Heideman, vice president of public sector at Mattermost, will discuss how emerging technologies and interoperable networks can enhance mission agility, ensuring information flows securely across forces to deliver decision advantage while maintaining data sovereignty. Heideman will also highlight how tactical teams can stay coordinated, efficient and mission ready by leveraging automated playbooks, integrating the tools they rely on and extending their collaborative environment to cut through the noise.

Attendees will gain practical insights into overcoming communication barriers, streamlining decision cycles and strengthening resilience, cyber or physical, in high-stakes missions. By integrating AI-driven analytics, adaptive security frameworks and unified communication strategies, military leaders can eliminate bottlenecks and move at the speed of the mission—ensuring readiness, coordination and strategic advantage in every mission.

**BIO:** Matthew Heideman is the vice president of public sector at Mattermost Inc., where he leads the company's growth in the federal market, focusing on driving adoption among key public sector customers, including the U.S. Department of Defense. With a strong background working at industry leaders such as Lockheed Martin, Deloitte and Red Hat, Heideman has deep expertise in mission IT, cybersecurity and governance risk and compliance. His leadership is instrumental in helping federal agencies enhance operational efficiency and mission readiness through secure, real-time collaboration solutions. Heideman's ability to navigate both government and commercial sectors enables him to foster strategic partnerships and deliver innovative solutions that address critical national security needs. He is committed to empowering government teams to make faster, more informed decisions in high-stakes environments.

# Strategic Cyber Defense: Leveraging Diverse AI Solutions

Roy Boivin, Federal COO, MixMode • Roy.Boivin@MixMode.ai

## ABSTRACT

In today's rapidly evolving digital landscape, artificial intelligence (AI) stands as a transformative force in cybersecurity, offering innovative solutions to combat increasingly sophisticated threats. However, not all AI tools are created equal; understanding the diversity among AI systems is crucial for effective defense strategies. This presentation explores the nuanced differences between various AI approaches—such as rule-based systems and machine learning models—and how each excels in specific cybersecurity contexts. By examining real-world applications and challenges, we highlight the importance of applying the right AI tool for the task at hand. A key focus will be on contextual reasoning within AI, which enhances defensive strategies by enabling more informed and adaptive responses to cyber threats. Join us as we discuss how a tailored approach to AI can significantly bolster your cybersecurity measures, ensuring robust protection against an ever-changing threat landscape.

**BIO:** Roy Boivin is a U.S. Air Force veteran with more than 20 years of experience in cybersecurity. Over the last 20 years, Boivin has worked at the Defence Threat Reduction Agency, Federal Aviation Administration, FBI, the White House and other highly targeted environments.

# Advancing Defense and Mission Outcomes by Leveraging Modern Data-Centric Security, AI and Intelligent Data Infrastructure

**Jim Cosby, CTO, Public Sector and Partners, NetApp U.S. Public Sector Inc. •**

Jim.cosby@netapp.com

## ABSTRACT

Mission and agency data is constantly growing, and it is becoming harder to share and manage across defense agencies and commands. Modernized data management today requires applying intelligence to the data to reduce the size and speed up access to data. It also requires modern data security features and capabilities to enhance zero trust across coalitions while leveraging AI to detect cyber attacks and provide instant recovery methods. Join this session to learn how intelligent data infrastructure can integrate AI, security, efficiency and flexibility to advance positive outcomes for defense agencies as well as mission partner environments and multidomain operations.

**BIO:** Jim Cosby is currently a CTO at NetApp U.S. Public Sector and has over 25 years of technology, engineering and leadership experience supporting a variety of federal and U.S. Department of Defense agencies. Jim has focused on data management and storage security for more than 20 years, including on-premise and hybrid multicloud intelligent data infrastructure technologies, which include multidomain operations and foreign mission environments. Cosby has a passion for teaming with agencies, customers, partners and colleagues to drive winning outcomes, and he thrives on helping customers architect optimal, cost-efficient and secure data management solutions using NetApp technology.

# Enhancing Multidomain Cyber Operations With ZeroLens

**Terry Dunlap, SVP Corporate Strategy & Development, NetRise •**

Terry.dunlap@netrise.io

## ABSTRACT

Cyber warfare, hybrid threats and technological advancements in artificial intelligence and autonomous systems increasingly shape the modern battlespace. Cyber superiority requires advanced offensive and defensive capabilities and rapid adaptability to emerging threats in critical infrastructure, embedded systems and defense networks.

ZeroLens, a cutting-edge capability within the NetRise platform, enhances computer network operations and offensive cyber operations by automating the identification of potential zero-day exploits at scale. It leverages symbol-less variable dataflow analysis and hybrid detection models to identify vulnerabilities across firmware and embedded systems and compiled binaries from multiple vendors and architectures. ZeroLens also evaluates exploitability and reachability, enabling defense operators to prioritize and weaponize vulnerabilities across vast target sets efficiently.

This talk will explore ZeroLens' role in accelerating military cyber capabilities, providing case studies on its application in real-time vulnerability discovery, automated target identification and multivendor exploit correlation. Furthermore, it will discuss the implications of software supply chain weaknesses on national security and how ZeroLens enhances interoperability between allied forces in NATO and the European Union.

As geopolitical competition intensifies, platforms like ZeroLens will be crucial in securing digital infrastructure, identifying strategic cyber vulnerabilities and enhancing mission readiness in an era of multidomain warfare.

**BIO:** Being arrested at 17 years old (circa 1985) for hacking with a Commodore 64 and a 300 baud U.S. Robotics modem didn't stop Terry Dunlap from:

- Obtaining a top-level security clearance with the U.S. government (2001)
- Working offensive cyber operations with the U.S. National Security Agency (2002)
- Launching Tactical Network Solutions to provide offensive cyber capabilities (2007)
- Spinning out ReFirm Labs to reverse engineer IoT firmware (2017)

- Selling ReFirm Labs to Microsoft for over \$20 million (2021)
- Launching Gray Hat Academy to teach cybersecurity pros how to think and act like a hacker (2023)
- Becoming senior vice president of Corporate Strategy & Development with NetRise (2024)

Prior to his federal sales roles, Musson successfully owned and operated ACTT Hawaii, demonstrating his entrepreneurial acumen and ability to build a multi-million dollar business. His extensive technical skill set, coupled with exceptional communication and negotiation abilities, positions him as a valuable asset in the technology sales landscape.



# Pushing the Limits: The Future of Modern Satcom

Emma Snowdon, Business Development, Paradigm • emma@paracomm.co.uk

## ABSTRACT

"Pushing the Limits: The Future of Modern Satcom" will explore how innovation in satellite communication technology is driving simpler, more efficient solutions for mission-critical operations. Featuring Paradigm's new RAGNO manpack solution, this lightweight (7.5kg), multiband, field-proven terminal delivers high-speed, secure communications with best-in-class RF performance. Powered by the Paradigm Interface Module, the intelligence behind Paradigm's terminals, the RAGNO offers customizable and futureproof features, including multiple power input options, alternative geolocation (onboard, external, GPS-denied/spoofed), Wi-Fi functionality and unlimited profile configurations.

In today's fast evolving satcom landscape, simplicity is key. Advanced technology doesn't have to be complicated. The goal is to make satellite connections as easy to use as modern smartphones, allowing users to focus on mission success, not satellite operations. By simplifying deployment and leveraging AI-driven interfaces, the RAGNO reduces the need for intensive training and accelerates setup times (on air in under two minutes). The compact, single-piece design, combined with field changeable RF cartridges and TRANSEC enabled security, ensures maximum performance with minimal effort.

As satcom needs to diversify, the future of ground satcom terminals must support multi-orbit, multiband and multinetwork capabilities while remaining intuitive and interoperable. The future of satcom lies in solutions that are powerful yet simple, enabling users to operate advanced technology across multiple constellations with ease—ensuring reliability and simplicity without compromise.

**BIO:** Emma Snowdon, business development at Paradigm, supports the growth and development of key partnerships. With a focus on collaboration and understanding of end user needs, Snowdon works to identify opportunities for improvement and help drive meaningful progress within the organization. Her goal is to contribute to Paradigm's success by combining a practical understanding of market trends with a dedication to fostering strong relationships and delivering value through thoughtful, customer-centered solutions.

# Post-Quantum Cryptography: Safeguarding Europe's Digital Future

**Matthias Christian Brickel, Global Commercial Business Manager, PQShield •**

matthias.brickel@pqshield.com

## ABSTRACT

The advent of quantum computing threatens to break classical public-key cryptography, endangering secure communications, digital identities and national security. As quantum advancements accelerate, governments, defense agencies and private enterprises must act now to implement post-quantum cryptography (PQC). This transition is complex, requiring coordinated efforts to ensure security without disrupting existing infrastructure.

PQShield, a key contributor to NIST's PQC standardization and European cybersecurity initiatives, is driving the development of quantum-resistant solutions for hardware, software and secure communications. This session will examine the quantum threat landscape, regulatory preparedness and the technical challenges of PQC adoption. It will provide insights into how Europe can lead the global shift toward quantum-safe security, ensuring the resilience of critical infrastructure and digital sovereignty in a post-quantum world.

**BIO:** Matthias C. Brickel is the global commercial business manager at PQShield, a global leader in post-quantum cryptography (PQC) and cybersecurity. With expertise in technology strategy, entrepreneurship and international economics, he facilitates the adoption of PQC across government, defense and enterprise sectors. His work bridges cryptographic innovation with real-world implementation, ensuring organizations remain resilient against quantum threats. An invited speaker at international cybersecurity forums, Brickel contributes to thought leadership on quantum-safe security and has collaborated with senior stakeholders across Europe and the United States. He holds a number of leadership roles and a postgraduate degree from the University of Oxford and academic credentials from leading institutions in Europe and the Americas.

# Challenges for Technology Talent in the New Era of Government Contracting

**Jake Frazer, President, Precision Talent Solutions** • [jake@pts.careers](mailto:jake@pts.careers)

## ABSTRACT

The international government contracting (GovCon) sector includes all areas of the U.S. government, NATO and international allies. The shifts in the U.S. government and NATO in the first quarter of 2025 have ushered in a “new era” for the GovCon industry, disrupting traditional budgetary trends, drastically reshaping the employment landscape on both sides of the Atlantic and altering perceptions of job stability in government-related work. This evolving environment presents both challenges and opportunities for GovCon firms as they recruit, screen and select the right technology talent.

Prior to this year’s government transformations on both sides of the Atlantic, the government and its contractors faced a significant shortfall of top technology talent, with over 400,000 unfilled roles in cybersecurity, AI and data science. Government employers continue to lose ground in the competition for top talent, as they struggle to match the salaries, benefits and career development opportunities offered by companies like Google, Amazon and Microsoft.

Traditionally, job stability and security have been key advantages of working in or with the government. However, the current era of uncertainty threatens this perception, making it even harder to attract top-tier candidates. To remain competitive, GovCon companies must:

- **Emphasize Mission-Driven Work:** Highlight the opportunity to contribute to national security and public service.
- **Offer Competitive Incentives:** Provide security clearance sponsorships and fund professional certifications to attract and retain skilled professionals.
- **Tap into Military Talent:** Focus on transitioning military personnel who already possess security clearances, relevant certifications and a strong commitment to mission-oriented work.

Our discussion will look into each of the facets to help governments and contractors become more competitive in a highly challenging and dynamic talent environment.

**BIO:** Jake Frazer is president and owner of Precision Talent Solutions (PTS), an executive search and recruitment firm focused solely on the government contracting industry. PTS has 30-plus team members in 12 countries and is a technology-driven recruitment business that spans the industry, providing executive search, technical/classified recruitment, career concierge and

business development services, with a specific focus on technology talent.

Prior to building PTS nine years ago, for almost a decade, Frazer was co-owner and executive leading TWI, a European prime contractor that also supported DLA, GSA and most of the primes across the industry. Frazer spent his early career as a cavalry officer deployed to Bosnia with IFOR, and then he returned to the Balkans with BRS/KBR where he helped build the foundations for LOGCAP III. He has valuable industry perspective from the military, working in KBR, leading a medium-sized enterprise and now innovating talent solutions across the industry.

Jake has a BA from Vanderbilt University and an MBA from Rochester Institute of Technology and is practitioner certified in MBTI and 16 PF.

Scinta has more than 30 years of experience in the technology community. Prior to joining Thales TCT, Scinta served as a Senior Solutions Architect with Thales Digital Identity & Security. In this role, she focused on providing solutions for protecting data using world class encryption and key management for data at rest in data centers and cloud infrastructures.

# The AI-Driven SDR and Covert Communication

**Ion Gheorghisor, Director, Proiect Management Services SRL • [promanse@starnets.ro](mailto:promanse@starnets.ro)**

## ABSTRACT

Most people see AI as an optimization tool that recognizes human speech, predicts outcomes or enhances automation. But the intersection of AI and SDR is an unseen warzone, a silent battle of intelligence, adaptability and control over the electromagnetic spectrum.

At its core, radio is physics, and physics is just mathematics waiting to be manipulated. AI introduces a new paradigm: software-driven intelligence shaping raw electromagnetic chaos into structured, interpretable information—an act of converting uncertainty into dominance.

There are deeper silent patterns that shape this field, which almost no one notices:

- **The Spectrum as a Living Entity:** Radio waves are not passive information carriers. The spectrum behaves like a dynamic battlefield, with signals colliding, interference shifting and noise evolving unpredictably. The top 0.1% of experts don't just use AI to process signals. They use AI to predict and manipulate the spectrum before transmitting the signal.
- **Exploiting the "Blind Spot" of Existing Radios:** Every radio receiver is optimized for something specific—Wi-Fi, military bands, mobile networks. But between those optimizations are vulnerabilities: unexpected waveforms, AI-generated noise patterns and unclassified frequency modulations. A genuinely advanced AI-SDR system doesn't "break" encryption; it bends the perception of the receiving radio, tricking it into believing the incoming signal is part of its normal operations.
- **The Illusion of Randomness:** Most modern security systems rely on cryptographic randomness. But randomness is only an illusion—at high enough intelligence, it becomes just another pattern. The most advanced AI models don't just classify signals; they predict the cryptographic randomness of frequency-hopping algorithms and intercept signals at precisely the right moment.

**BIO:** SC Proiect Management Services SRL Director General  
University "POLITEHNICA" of Bucharest (UPB)  
Faculty of Automation and Computers

Paper Published:

1. Ion F. Gheorghisor - Cognoscenti Agents, submitted to 2009 IEEE 5th International Conference on Intelligent Computer Communication and Processing, Technical University of Cluj-Napoca, August 27-29, 2009, Cluj-Napoca, Romania

2. Ion F. Gheorghișor - HOMOOMERICAL RELATIONSHIPS AND COGNOSCENTI AGENTS, submitted to be published at U.P.B. Sci.Bull., Series ..., Vol. ..., No. ..., 2009 ISSN 1454-234x
3. Ion F. Gheorghișor - Cognizant Objects and Cognoscenti agents, submitted to THE 17th INTERNATIONAL CONFERENCE ON CONTROL SYSTEMS AND COMPUTER SCIENCE May 26-29, 2009, Bucharest, Romania
4. Ion F. Gheorghișor, Communication Specific Relationships between Elements' Identity and Set Definition ("Proposal of an ontological model for the implementation of a cognitive system that captures evolution"), submitted at The Scientific Session "Ph.D. A&C Student Days 2013" – 4th Edition, Faculty of Automatic Control and Computer Science, September 26-27, 2013
5. Ion F. Gheorghișor - ENHANCING e-LEARNING THROUGH USING STUDENTS' VIRTUAL CLONES – submitted to the 10th International Scientific Conference eLearning and software for Education, Bucharest, April 24-25, 2014, 10.12753/2066-026X-14-000
6. Ion F. Gheorghișor - Decreasing the Informational Entropy through Knowledge Acquisition – submitted to the 11th International Scientific Conference - eLearning and Software for Education, Bucharest, April 23-24, 2015, 10.12753/2066-026X-15-000

# Building the Foundation for AI/ML and GenAI in Government: Why Data as a Service Is Critical

Jae Yi, Managing Director, Emerging Technology, Recro • [jae@recro.com](mailto:jae@recro.com)

## ABSTRACT

As the U.S. government accelerates efforts to harness AI/ML and generative AI (GenAI) for mission success, the challenge is no longer just about building better models—it's about delivering the right data, at the right time, in the right context. Without a robust AI/ML infrastructure powered by data as a service (DaaS), agencies risk data silos, misinformation and model hallucination, ultimately leading to flawed decision-making.

To get ahead in AI/ML and GenAI, government agencies must establish a scalable and governed data foundation that ensures data is ingested, organized, labeled, tagged and contextualized through ontology frameworks, policies and retrieval-augmented generation architectures. Without this, AI models may produce unreliable or even harmful outputs.

Most organizations today are only scratching the surface of AI's potential, implementing models without fully addressing data integrity, provenance and accessibility. This session explores how DaaS can serve as the backbone for AI-driven initiatives, enabling agencies to move beyond experimental AI to operational, high-trust AI/ML capabilities. Attendees will gain insight into best practices, lessons learned and strategies for building AI-ready data infrastructure that ensures security, compliance and mission success—without falling into the trap of chasing AI hype over real-world effectiveness.

**BIO:** Jae Yi is a recognized leader in imagining and building consulting practices to partner with clients to establish centers of excellence and competency centers that enable organizations to bridge the gap between where they are today and where they strive to be. With a mission-focused approach, he has partnered with enterprises and government agencies to drive sustainable adoption of emerging technologies, solving foundational challenges that unlock incremental, sustainable transformation.

Yi has worked with emerging technology companies, including Cisco, BMC, hyper-scalers, Big 4 firms and global integrators, to develop emerging technology portfolios to help their clients navigate the complex digital landscapes. His foundational expertise lies in decoupling data and logic across cloud-native, disconnected edge architectures, leveraging automation and orchestration to accelerate modernization efforts toward digitalization and digitization of new capabilities.

As a thought leader and speaker, Yi has presented at AWS re:Invent, Gartner Symposium, IDC events, Microsoft Ignite, Google Next and other industry conferences, sharing insights on practical strategies for sustainable emerging tech adoption and scaling transformation initiatives effectively.

For more than 25 years, Yi has been helping organizations avoid the pitfalls of chasing technology fads by focusing on foundational strategies, pragmatic adoption and sustainable transformation, ensuring that emerging technologies deliver real, incremental, timely, long-term value rather than just fleeting hype.



# Stream Data and Applications Between the Core and the Edge: A Proposed Framework To Accelerate the Time to Mission and Maximize Resilience and Interoperability in Multidomain Operations

**Giuseppe Magnotta, Associate Principal Solution Architect, Red Hat •**

gmagnott@redhat.com

## ABSTRACT

In this session, Red Hat will demonstrate how it is possible to build a platform to stream data and applications between the core data center and remote locations such as deployed edge or tactical edge in a secure and soft real-time manner.

### Agenda:

- Strategic Autonomy and Sovereignty
- The Army's Journey to Digital Transformation
- Challenges To Solve
- Red Hat Proposed Framework
- Interesting Use Cases
- Conclusions
- Open Discussion

Objectives: Demonstrate to military organizations and their partners that enterprise open-source technology can:

- simplify the creation of smart systems that will operate outside of the physical perimeters of the core data center, such as autonomous edge devices
- speed the time to mission
- simplify interoperability
- reduce the time to integrate new systems
- keep high security standards

**BIO:** Giuseppe Magnotta is an associate principal solution architect at Red Hat.

A technology enthusiast with experience in many fields of the IT landscape, Magnotta is passionate about open source, software engineering, distributed computing, Unix environments and Kubernetes ecosystem.

He's always interested in discovering new technologies and new challenges. His mission is to be the catalyst of customer success.

In his current role, he helps his customers solve their challenges by adopting the power of enterprise open-source software.

# Securing Velocity: How CI/CD and Compliance Drive Digital Transformation in Defense

**Luke Strebel, Senior Product Manager, Rise8** • [lstrebel@rise8.us](mailto:lstrebel@rise8.us)

## ABSTRACT

Balancing continuous software delivery with stringent security and compliance requirements is a constant challenge for regulated sectors—health care, finance, government, defense and beyond. This presentation draws on experience building a secure release pipeline at the U.S. Department of Veterans Affairs and insights gained from work across innovative U.S. Air Force programs (Kessel Run, Space CAMP, AFWERX) and explores how prioritizing continuous delivery is essential for enabling digital transformation, driving both speed and security. For disruptors seeking to modernize their organizations, this talk will demonstrate how a strategic focus on secure continuous delivery delivers key benefits:

**Enhanced Security Posture:** By embedding automated cybersecurity testing (SAST, DAST, IAST) and vulnerability management throughout the delivery life cycle, secure continuous delivery enables proactive risk mitigation and continuous assurance, reducing exposure to cyber threats and compliance violations.

**Accelerated Delivery of Capabilities:** Secure continuous delivery streamlines the software release process, enabling faster deployment of critical updates and new capabilities, improving operational agility and responsiveness while maintaining compliance.

**Improved Compliance and Auditability:** Implementing secure continuous delivery provides automated compliance checks and continuous monitoring, simplifying audits, ensuring adherence to key frameworks (NIST, FedRAMP, HIPAA, etc.) and reducing compliance costs.

Luke Strebel will address the common misconception that compliance slows down delivery, illustrating how secure continuous delivery enables both speed and adherence to regulations, directly supporting compliance-driven initiatives. Finally, he will discuss the role of AI in managing the increasing complexity of cyber operations and compliance, providing insights on how AI can enhance visibility, automate threat detection and inform strategic decision-making.

**BIO:** Luke Strebel is a senior product manager at Rise8, where he leads the development of secure release CI/CD pipelines for applications at the U.S. Department of Veterans Affairs. His work focuses on enabling rapid and secure software delivery through the integration of

cutting-edge cybersecurity tools and automation. Prior to Rise8, Strebel gained experience at Google, where he optimized workflows for hyper-growth products like Google Wallet, and in the U.S. Air Force, where he led QA teams for cybersecurity software and drove digital transformation initiatives. Touching nearly every U.S. Department of Defense “Software Factory” (Kessel Run, Space CAMP, Kobayashi Maru, Platform One, Hangar 18) through his time as a product manager and later in his work with AFWERX, he is deeply knowledgeable about how disruptive technology can improve the lives of users. He possesses a master’s degree in applied systems engineering and holds certifications in PMP and CSEP. Strebel is passionate about bringing people and technology together to solve complex challenges and deliver impactful solutions.

# Generative AI for ITOps

**Lee Koepping, Chief Technologist, ScienceLogic** • lkoepping@sciencelogic.com

## ABSTRACT

In the rapidly evolving landscape of information technology operations (ITOps), generative AI is emerging as a revolutionary force capable of transforming enterprise systems and enhancing operational efficiencies. This presentation delves into the application of generative AI within ITOps, highlighting its potential to redefine enterprise monitoring, automate workflows and provide unprecedented IT service visibility.

### Key Points:

1. Enterprise Monitoring:
  - Explore how generative AI leverages machine learning algorithms to monitor complex IT environments continuously.
  - Discuss the advantages of proactive anomaly detection and predictive maintenance, reducing downtime and improving system reliability.
2. Workflow Automation:
  - Investigate how AI-driven automation can streamline routine and complex workflows, enhancing productivity and reducing human error.
  - Present case studies demonstrating significant improvements in efficiency and cost savings through AI-powered automation.
3. IT Service Visibility:
  - Examine how generative AI provides comprehensive visibility into IT services, offering actionable insights that enable better decision-making.
  - Highlight the role of AI in fostering a transparent and responsive IT environment that adapts to evolving operational needs.
4. Solutions to Unforeseen Problems:
  - Address the innovative solutions generative AI offers to challenges in the operating environment that the government and military have yet to encounter.
  - Discuss the potential of AI to anticipate and mitigate risks in critical infrastructure, ensuring mission success and operational continuity.

### Conclusion:

Generative AI is not just a technological advancement; it is a strategic enabler for the intelligence community, providing tools that enhance operational capabilities and resilience. As we navigate through uncharted territories in IT operations, embracing generative AI will be pivotal in maintaining a competitive edge and achieving operational excellence.

Join us to explore how generative AI is set to revolutionize ITOps and empower the intelligence community with cutting-edge solutions for the challenges of tomorrow.

**BIO:** Lee Koepping is a seasoned executive and technical leader with more than 30 years of experience in IT engineering, technical solutions sales and project and business management for both federal and commercial enterprises. His extensive career reflects a dedication to technological innovation and a profound understanding of complex IT environments.

Koepping currently serves as the chief technologist for ScienceLogic, where he plays a pivotal role in the public sector marketplace. In this capacity, he provides leadership and coordination of the company's technical direction, developing and establishing the go-to-market strategy and technology portfolio. His efforts are focused on delivering comprehensive solutions to the challenges faced by government and U.S. Department of Defense (DoD) organizations in today's rapidly evolving technology landscape.

Koepping began his illustrious career in the U.S. Navy, where he received formal education in electronics engineering. During his eight years of decorated service, he worked in naval intelligence, honing skills that would later prove invaluable in the IT industry. Following his military service, Koepping transitioned into the private sector, where he quickly made a name for himself as a technical leader and innovator.

Through his role at ScienceLogic, Koepping continues to push the boundaries of what is possible in the public sector. His work ensures that government and DoD organizations have access to cutting-edge technology solutions that enhance operational readiness, efficiency and security.

# Introducing an AI-Assisted Cost-Benefit-ROI Model for U.S. AI Use Cases

Jim Liew, Founder, SoKat Consulting LLC • jim@sokat.com

## ABSTRACT

This study analyzes 1,754 publicly disclosed U.S. federal AI use cases from AI.gov in 2024, providing a unique opportunity to examine their distribution, benefits, costs and return on investment (ROI). Using advanced AI models from OpenAI and Anthropic, the authors developed the McIntyre and Liew Model (MLM) to quantify and rank AI initiatives across 37 federal departments and agencies. The analysis reveals that AI applications are concentrated in health care, public safety and infrastructure agencies such as HHS, VA, DHS, DOI and USAID, with “mission-enabling” initiatives dominating, reflecting their alignment with agency-specific objectives. High-ROI applications often leverage commercially available tools, highlighting the integration of big tech innovations with public sector goals. Unlike private sector analyses, this dataset focuses on public interest-driven AI initiatives, and the MLM framework transforms textual disclosures into actionable metrics for evaluating diverse government challenges. The scalable methodology facilitates comparisons across agencies and operational problems while offering a foundation for innovative applications of AI to unresolved public issues. This research establishes a benchmark for future AI evaluations, fostering collaboration and enabling synthetic solutions to complex public sector challenges, ultimately demonstrating the transformative potential of AI in advancing mission-critical objectives and public interest goals.

Keywords:

Artificial Intelligence, AI.gov, AI Use Cases, Public Value, Government Technology, Evaluation Framework, Cost-Benefit Analysis, ROI Analysis

**BIO:** Jim Kyung-Soo Liew is the president and founder of SoKat and an associate professor of finance at Johns Hopkins Carey Business School. Liew revels in pushing the boundaries of financial knowledge and product development both as an academic and entrepreneur. He has published pioneering research in the intersection of social media/big data, cryptos/blockchain and financial markets. He currently serves as the faculty lead on AI for Business Essentials, Cryptos and Blockchain, Entrepreneurial Finance, and Wealth Management at the Johns Hopkins Carey Business School. Additionally, he served as ACT-IAC's co-chair of the AI Curriculum Committee and chair of the Data Readiness for AI Committee. He has received the Dean's Award for Faculty Excellence 2015-2019. He is on the editorial board of The Journal of the British Blockchain Association, Journal of Alternative Investments, Journal of Financial Data Science and the Journal of Portfolio Management, where he co-authored the most read Invited Editorial “iGDP?”

About SoKat Consulting LLC ([www.SoKat.com](http://www.SoKat.com)) - SBA 8(a) Certified

Liew founded SoKat Consulting LLC. SoKat creates award-winning, world-class machine learning/AI and blockchain products and services primarily servicing institutional investors, government agencies, academic institutions and select startups. SoKat unlocks the hidden value of data through thoughtful and creative solutions, comprising of actionable business intelligence, transparent data analytics, bold predictive models and next-generation investment products.

Previously, Liew has been with the Carlyle Asset Management Group, Campbell and Company, and Morgan Stanley. He holds a BA in mathematics from the University of Chicago and a Ph.D. in finance from Columbia University.

Previously served: EO DC Board Member | Co-Chair Finance and Governance



# Rugged, Low-Power, High-Performance and Portable Edge Infrastructure

**Manavalan Krishnan, Co-Founder and CTO, Tsecond Inc. •**

Manavalan.krishnan@tsecond.us

## ABSTRACT

Tsecond, an Aero Equity HorizonX portfolio company, specializes in innovation for edge infrastructure. Tsecond's patented technology enables large data capture, data transport and AI in disadvantaged, harsh, forward, tactical, mobile and flying edge environments. The flagship product, BRYCK, is a high-performance, petabyte-scale mobile data solution, weighing only 14 pounds, while consuming 500 watts of power in the form factor of a construction brick. Besides addressing data storage and data movement needs, Tsecond's latest innovation, BRYCK AI, enables AI right at the edge.

BRYCK AI Mini and BRYCK AI Block are innovative solutions designed by Tsecond to address the growing demand for rugged, low-power, high-performance and portable edge infrastructure. The BRYCK AI Mini stands out with its unique positioning, combining storage and AI inferencing capabilities into a single compact and portable device. Battery-powered and ruggedized for challenging environments, the BRYCK AI Mini enables AI inferencing on the move or in flight, offering real-time processing and decision-making in remote or mobile settings.

On the other hand, the BRYCK AI Block is a flexible, plug-and-play solution that allows any computer to gain AI inferencing and storage capabilities effortlessly. By integrating seamlessly with existing systems, BRYCK AI Block enables users to deploy AI-driven applications quickly without the need for extensive hardware upgrades. This makes it a powerful tool for organizations looking to enhance their computational capacity without compromising on space or energy efficiency. Both devices are engineered with Tsecond's commitment to delivering high-quality, reliable edge infrastructure solutions that cater to diverse industry needs, from field operations to remote data processing.

**BIO:** Manavalan Krishnan (aka Mana) is the CTO and co-founder of Tsecond. He is an energetic, entrepreneurial individual with extensive experience in building high-performing technical teams and delivering elegant solutions to complex problems.

Manavalan has architected and delivered several successful products from concept across various technical domains, such as scalable file systems, object storage, databases, NoSQL, big data processing, networking and mobile operating systems that led to major customer wins and two major acquisitions. These products and technologies are foundations for any cloud and data center data storage and analytics infrastructure.

During his tenure of 20 years in the industry, he has secured 15 patents and counting to his name in the areas of distributed data storage and data analytics platforms.

# Tackling Global Security Challenges With GenAI

**Nick Bray, CBE, Vice President of Global Defense and Security, Vantiq •**

nbray@vantiq.com

## ABSTRACT

Nick Bray, CBE, global vice president of defense and security, former head of the U.K. Ministry of Defence's international strategy and operations, and Royal Air Force commanding general in Afghanistan, brings decades of military leadership to tackling today's most pressing defense and security issues. He combines his military experience with eight years in cutting-edge technologies in civilian life. Drawing on real-world challenges, he discusses how generative AI and adaptive strategies are transforming disaster response, safeguarding critical infrastructure and shaping a safer, more secure world.

**BIO:** Nick Bray, CBE, is the vice president of global defense and security at Vantiq, where he leverages over three decades of military expertise to drive innovative solutions in defense technology. Joining Vantiq in March 2023, from PwC, Bray has a distinguished military background, having served 33 years in the Royal Air Force (RAF). His notable roles include commanding the RAF's specialist ground combat and security forces and serving as the director of international policy and plans for the U.K. Ministry of Defence. After retiring from active service in 2017, he continued to contribute as a reservist in the RAF's innovation organization, gaining valuable insights into defense advancements.

Prior to Vantiq, Bray held key advisory, business development and sales positions in defense innovation, drone development, large-scale digital twins and cybersecurity, where he successfully introduced cutting-edge technologies to a range of customers. His contributions have been recognized with prestigious awards, including being named a Commander of the Order of the British Empire (CBE) for his leadership on operations in Afghanistan and Iraq. Bray holds master's degrees in military strategy and technology from King's College London and international relations and diplomacy from the London School of Economics.

# Spill Coffee Not Data: How To Secure Sensitive Assets and Avoid Being Roasted by Adversaries

**Andrew Forsyia**k, Director of Business Development, Varonis U.S. Public Sector LLC •  
aforsyia@varonis.com

## ABSTRACT

The global community faces advanced cyber campaigns that threaten the public and private sectors and American security and privacy. By implementing zero trust (ZT) across agency systems, we aim to protect high-value assets. However, without a solid foundation, any zero-trust architecture will be ineffective. Agencies must strive to provide top-notch ZT-based security while satisfying compliance requirements. ZT represents a paradigm shift in protecting our assets and requires a multiphased deployment process. Just-in-time policy enforcement is central to ZT architecture, but agencies must first take steps like data labeling, data inventorying and remediation of high-risk systems. Only after building a solid data protection foundation can agencies rely on user behavior analytics and machine learning to drive policy. At the core of all ZT strategies is data protection. Without appropriately identifying, labeling and protecting core agency assets, any zero-trust strategy will fail.

In his session, Andrew Forsyia will review how data governance feeds directly into a successful zero-trust strategy. Forsyia will discuss the importance of the data pillar in deploying a zero-trust architecture and why it should be part of every agency's early strategic moves. Lastly, he'll address current mandates with a future-oriented approach to zero trust. This will help agencies drive toward long-term strategic goals while meeting the stringent requirements of a modern-day public sector network.

**BIO:** Andrew AJ Forsyia is a U.S. Army veteran. Serving as a military intelligence officer and senior U.S. Department of Defense executive, he has supported cyber, military intelligence, ISR and NSA for more than 30 years. He currently serves as a business development executive for Varonis. His last position in the government was as a senior executive where he established and served as the executive agent for Cyber Training Ranges for the Department of Defense. Forsyia is an innovator, disrupter and builder of teams.

He is a graduate of Seton Hall University and holds a master's degree in public administration from American University, a master's degree in cybersecurity from Brown University, and he is a senior executive fellow from the Harvard Kennedy School of Government.

# Encryption as a Weapon: Preparing for the Inevitable Impact of Artificial Intelligence Fortified by Quantum Computing

Joseph Warren, Encryption Strategist, Viasat • [Joseph.warren@viasat.com](mailto:Joseph.warren@viasat.com)

## ABSTRACT

History has proven that encryption capabilities can provide great strategic military advantages. At the same time, compromise of encryption (i.e. The Enigma), can result in a nation's greatest vulnerability. Artificial intelligence is already posing threats to existing encryption capabilities, and the inevitable breakthrough in quantum computing promises to increase threats exponentially. Even the most sophisticated weapons become less effective if secrecy of their use is compromised.

There are no single, silver bullet solutions to ward off such threats, and so a change in the way encryption solutions are delivered and updated becomes a crucial component of continuous threat deterrence. As we continue to make advancements in weapons and communications, encryption solutions must also be treated as a modern weapon each warfighter requires to carry out a mission. This paper explores the impact of quantum computing on modern encryption methods and the strategies needed to prepare for, rather than react to, these pending threats.

**BIO:** Joseph Warren is responsible for developing key strategies related to Viasat's high-assurance data in motion encryption devices. He is experienced with bringing new-to-world technologies to market, including the world's first Wi-Fi device certified to transmit U.S. top secret data. Today, Warren is focused on countermeasure strategies for the pending combined threats of quantum computing and artificial intelligence. By focusing on the impact on both diplomacy and warfighting, Warren brings a unique perspective to these emerging technologies and the rationale behind preparing for the inevitability of these threats.

# Empowering Defense in the Digital Age: Secure, On-Premise Geospatial Intelligence

**Bart Adams, CTO, xyzt.ai** • bart.adams@xyzt.ai

## ABSTRACT

In an era where technological advancements and global cooperation shape the future of defense and security, secure geospatial intelligence is a strategic necessity. xyzt.ai is proud to announce that its big data spatio-temporal analytics platform is now available for on-premise deployments.

The xyzt.ai platform is built for any spatio-temporal data and excels at integrating and analyzing vast, multisource datasets, including satellite and terrestrial AIS, ADS-B, GNSS, radar and sensor data. With interactive visual analytics and natural language interaction, users can seamlessly explore patterns and anomalies across space and time, uncovering mission-critical insights for maritime domain awareness, airspace monitoring, ground operations and threat detection.

Now available to system integrators and defense organizations for deployment on private servers and secure clouds, the platform ensures full data sovereignty, eliminating cloud-related risks and enhancing operational resilience while maintaining compliance with stringent security regulations.

Additionally, xyzt.ai facilitates secure information-sharing across allied forces and agencies, strengthening collaboration in mission-critical scenarios. From maritime surveillance to land and air monitoring and threat detection, xyzt.ai equips defense organizations with the intelligence needed to navigate the digital battlefield.

Join us to explore how xyzt.ai's on-premise solution is transforming defense operations and enhancing global security through innovation and cooperation.

**BIO:** Bart Adams is the founder and chief technology officer at xyzt.ai, a cutting-edge SaaS company providing a cloud-based platform for visualizing and analyzing large-scale location data from vehicles, vessels, aircraft, individuals and assets. With applications critical to safety and security, the platform offers actionable intelligence through advanced data analytics, enhancing situational awareness and decision-making for military and security operations. Adams' leadership has driven xyzt.ai to new heights with the development of the "Just Ask xyzt.ai" feature, enabling safety and security professionals to interact with complex datasets using natural language queries, simplifying the process of extracting key insights.

Before founding xyzt.ai, Adams was the chief innovation officer at Hexagon Geospatial, where he pioneered high-performance data visualization and analysis technologies with applications in intelligence and homeland security.

Adams holds a master's degree in engineering from the University of Leuven, for which he received the IBM Best Master's Thesis Prize. He later completed his Ph.D. in engineering and conducted postdoctoral research at Stanford University with fellowships from the Fund for Scientific Research Flanders and the Belgian American Educational Foundation.

A recognized leader in the geospatial industry, Adams has been named an IDC Geospatial Innovator and included in the Global Top 100 Geospatial Companies by Geoawesomeness. He is a sought-after speaker at events, such as those hosted by AFCEA International and other industry forums, where his expertise in geospatial intelligence and big data analytics is highly valued.

Adams is also an active member of the open geospatial community, working on standards that enhance interoperability in defense and security systems. His passion lies in transforming technological innovations into practical, customer-oriented solutions, especially in areas where data visualization and real-time analysis are critical to national security and safety operations.



