



TECHNET TRANSATLANTIC

FRANKFURT, GERMANY • 4 - 5 DECEMBER 2024 • #TechnetTransatlantic

2024 INNOVATION SHOWCASE

2024 TechNet Transatlantic Innovation Showcase

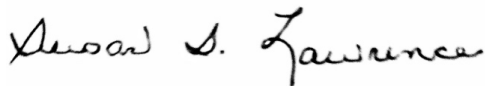
By strategic design, the theme for 2024 TechNet Transatlantic is “Leadership and Collaboration—Achieving Effectiveness in C4ISR and Cyber,” which underscores the importance of cooperation in advancing capabilities in command, control, communications, computers, intelligence, surveillance, reconnaissance (C4ISR), and cyber domains. TechNet Transatlantic continues to serve as an essential forum for staying ahead of evolving technologies and maintaining operational effectiveness.

AFCEA International is doing its part to share information, build partnerships and find solutions in the critical digital domain, including hosting these presentations that provide companies the opportunity to demonstrate cutting-edge solutions to government representatives and potential industry partners.

It’s imperative we discover and share the information and build the relationships to realize the whole-of-government approach that has practically become a way of life for the national security and defense community.

Yes, a lot of work still needs to be done, and there are many challenges to overcome to promote faster, more efficient and effective collaboration across our government and among multiple governments. And the content on these pages is an optimal place to start.

Best wishes,

A handwritten signature in black ink, reading "Susan S. Lawrence". The signature is fluid and cursive, with the first name "Susan" and last name "Lawrence" clearly legible.

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

President and CEO
AFCEA International

Table of Contents

SUBMISSIONS

Empowering the Cyber Warfighter: AI Solutions to Enhance Cyberspace Operations

Justin Hunsaker, Solutions Architect, Sealing Technologies, LLC 11

Advancing Trusted AI to Generate and Exploit Real-World Understanding

Nick Sutherland, Esri Europe National Government Lead, Esri 12

The Zero-Trust Data Centric Challenge—Building a Functional Data Centric Sharing Architecture With Effective Zero Trust Controls

Jim Cosby, CTO, Public Sector and Partners, NetApp U.S. Public Sector Inc. 13

The MPE Data and Information Sharing Conundrum—Building a Real Data Information Sharing Architecture With Intelligence, Efficiency, Flexibility and Security

Jim Cosby, CTO, Public Sector and Partners, NetApp U.S. Public Sector Inc. 14

The Data Interop Imperative—Architecting an Intelligent Data Infrastructure That Effectively and Securely Shares Critical Data to Ensure Mission Success

Jim Cosby, CTO, Public Sector and Partners, NetApp U.S. Public Sector Inc. 15

Achieving CJADC-2 Decision Dominance: Optimizing Cross-Domain Data Flows

John Carbone, Senior Technical Director & Chief CIP Solutions Architect, Everfox..... 16

Honeytokens for Cloud Threat Detection

Ralph Kahn, GM Federal, Acalvio 18

Asymmetric Advantage: The Crowd as a Force Multiplier

Kent Wilson, VP, Global Public Sector, Bugcrowd 19

SUBMISSIONS

Optimizing Cloud Storage Solutions for Military Operations: A Path to Enhanced Data Security and Resilience in European Operations

Indira Donegan, Chief Technology Evangelist, Red River
Jim Cosby, CTO Public Sector and Partners, NetApp.....21

Moving Information Superiority Warfare to the Cloud: Opportunities and Challenges

Benedikt Meng, Business Development & Public Affairs Manager, Infodas GmbH..... 23

Please Welcome Your New Employee!

Mark Matzke, Area Vice President, Department of Defense, ServiceNow..... 24

Enhancing Next-Gen C2 Systems for Streamlined, Secure Military Operations

Mark Matzke, Area Vice President, Department of Defense, ServiceNow..... 25

Beyond the Device: Quantum Encryption and the Future of Secure Military Communication

Indira Donegan, Chief Technology Evangelist, Red River 26

Mission Ready: Ensuring Technical Capability and MPE Integration Across U.S. Partners

Indira Donegan, Chief Technology Evangelist, Red River 28

AI in Action: Revolutionizing Military Decision-Making in Real Time Within the European Theater of Operations

Indira Donegan, Chief Technology Evangelist, Red River 30

Zero-Trust Implementation in Government: A VAR's Perspective on Achieving Cyber Resilience in the Mission Partner Environment

Indira Donegan, Chief Technology Evangelist, Red River 32

Table of Contents

SUBMISSIONS

Command and Control Redefined: Fostering a Unified Operational Picture with AI	
Indira Donegan, Chief Technology Evangelist, Red River	34
Empowering Government Agency Innovation through ServiceNow's Generative AI	
Eric Silverstein, Director, Solution Consulting Architecture, ServiceNow	36
Ensuring Business Continuity with ServiceNow: The Power of Mission Resiliency	
Eric Silverstein, Director, Solution Consulting Architecture, ServiceNow	37
Deploying Software as a Service (SaaS) for Government Agencies with ServiceNow	
Eric Silverstein, Director, Solution Consulting Architecture, ServiceNow	38
Zero-Trust Architecture With the Now Platform—Systematically Harden the Digital Attack Surface	
Scott Flynn, Advisory Solution Consultant, ServiceNow	39
Empowering the Cyber Workforce with Automation and Orchestration within ServiceNow	
Scott Flynn, Advisory Solution Consultant, ServiceNow	40
Leading at Flank Speed: How Digital Champions Secure Zero Trust Advantage	
Steven Kyle Denton, N-MRO Resource Sponsor, OPNAV N4	41
Creating Order out of Chaos—Understanding Your Cyber Adversary and How to Defeat Them by Modernizing Technology and Increasing Warfighter Productivity	
Jeff Worthington, Executive Strategist, CrowdStrike	42
Layered PACE Model for C2 Planning	
Chief Warrant Officer 3 William Holden, Network Operations Warrant Officer, Joint Multinational Readiness Center.	44

SUBMISSIONS

The Software Defined Enterprise & Autonomic Networking	
Ken Camp, Network Capabilities Leader - Office of CTO, Tyto Athene.....	45
A Practical and Scalable Implementation of the Vernam Cipher, under Shannon Conditions, Using Quantum Noise	
Adrian Neal, Senior Director and Global Lead for Post-Quantum Cryptography, Oxford Scientifica.....	47
GitOps for Edge Applications in Denied, Disrupted, Intermittent and Limited (DDIL) Environments	
Zachary Yates, Sr. Solution Architect, GitLab	48
Is Your Acquisition and Zero-Trust Plans Set Up to be Cyber Survivable?	
Steve Pitcher, Senior Cyber Survivability Analyst, Joint Staff J6	49
Future-Ready Defense Networks: Leveraging Zero-Trust Architecture for Secure, Real-Time Military Collaboration	
Rob Bair, CISO in Residence, Zscaler.....	51
Achieving Performance-Based Outcomes and Innovation When Outsourcing ICT Services With GSA AAS	
Michael Baumann, Division Director, Assisted Acquisition Services Army, U.S. General Services Administration	53
Cyber Threats and Mitigations for Briefing Rooms	
Zohar Vered, Vice President, Marketing & Sales, High Sec Labs	55
Cybersecurity Methods for Command and Control Centers	
Zohar Vered, Vice President, Marketing & Sales, High Sec Labs	56
Empowering Battlefield Commanders in Contested Environments: Leveraging Software-Defined Wide Area Networking (SD-WAN) for Mission-Critical Application Delivery	
Michael Maice, Sr. Technical Advisor, Juniper Networks	57

Table of Contents

SUBMISSIONS

Maintaining Mission Readiness and Protecting COP Collaboration with Physics not Software

Christian Hager, VP of Sales & Business Development, Fend Inc. 59

Preparing Defenders and Defenses in the Age of Cyberwarfare

Lee Rossey, Co-Founder & CTO, SimSpace..... 60

The “War Phone” — Eliminating the Signature Management and Active Espionage Risks of Commercial Mobile Devices in Military Operations

Michael Campbell, President and General Manager, Privoro Government Solutions..... 61

Building Next-Gen Secure Remote Capabilities and Enhanced Interoperability with Global Partners

Brian Kovalski, Senior Vice President, Federal, Hypori..... 63

Data Interoperability for Decision Dominance: Strategies as Executed at U.S. EUCOM and U.S. AFRICOM

Dominic Critchlow, Chief Scientist, Booz Allen Hamilton 64

The Path to C2 and an AI-Enabled COP

Nathan Keegan, CTO, Booz Allen Hamilton..... 65

Leveraging the Pentaho DataOps Platform for Enhanced Leadership and Collaboration in C4ISR and Cyber Domains: A Data Analytics Use Case from the Ukraine-Russia Conflict

Pragyansmita Nayak, Chief Data Scientist, Hitachi Vantara Federal 66

Interoperable Experimentation is Key to Warfighter Readiness Across European Allies

Nick Woodruff, Chief Growth Officer, Research Innovations Inc..... 68

SUBMISSIONS

Serving Defence’s Need for Information From a Data Soup
Richard Goodman, EMEA Defence Lead, Hexagon..... 69

Speaking the Same Language: Creating Conditions for MPE Success
James Stanger, Chief Technology Evangelist, CompTIA 70

NATO SPS Cube4EnvSec: Federated, Interoperable AI-Cubes for ISR and
Tactical Data Availability at Scale
Peter Baumann, Professor | CEO, Constructor University | rasdaman GmbH..... 71

Networking: The Superpower Fueling Success in Technology and Cyber
Operations
Seni Aguiar, COO, Digital Charter 73

SUBMISSIONS

Empowering the Cyber Warfighter: AI Solutions to Enhance Cyberspace Operations

Justin Hunsaker, Solutions Architect, Sealing Technologies, LLC •

justin.hunsaker@sealingtech.com

ABSTRACT

This session will explore how large language models (LLMs) and retrieval augmented generation (RAG) can be leveraged to augment cyber defense capabilities. Justin Hunsaker will highlight how AI agents can seamlessly integrate and interact with defense information systems, empowering cyber defenders in their efforts to safeguard critical data. Attendees will gain insight into cutting-edge artificial intelligence (AI) technologies that enhance the capabilities of junior and senior cyber defenders. These tools enable quick understanding of complex data and mission environments, allowing cyber defenders to rapidly deliver actionable intelligence to leaders. A demonstration will showcase how cyber defenders can be empowered to utilize open and secure AI technology to stay ahead of adversaries.

BIO: Justin Hunsaker is a principal solutions architect with SealingTech, working primarily in support of delivering advanced cyberspace warfighting capabilities to the U.S. armed forces. Prior to his time at SealingTech, Hunsaker served abroad in the U.S. Army for 20 years. Hunsaker has held several positions within the military, serving as a satellite communications operator/maintainer, network management technician, information protection technician and cyber warfare planner. His previous assignments include the Joint Communications Support Element, Army Cyber Command, Cyber Protection Brigade and the Cyber Center of Excellence. His work within the Cyber Mission Force has been instrumental to the development of evolutionary capabilities to answer complex problems for the cyber workforce. Hunsaker's contributions to the Cyber Mission Force have been recognized at the highest levels, as his developed concepts have directly impacted the strategic messaging across the Department of Defense and the broader cyber community. In 2017, Hunsaker was awarded the Saint Isidore (Silver) Army Cyber Command Award for demonstrating exceptional initiative, leadership, insight and excellence. Hunsaker received his Bachelor of Science in cybersecurity from the University of Maryland Global Campus in the spring of 2015.

Advancing Trusted AI to Generate and Exploit Real-World Understanding

Nick Sutherland, Esri Europe National Government Lead, Esri •

nsutherland@esri.com

ABSTRACT

Geo AI and generative AI enable the rapid capture and modelling of data and information, which can be used to represent the real world, gaining understanding of complex patterns and trends. These can be reviewed in a digital twin, which provides powerful tools to visualize, analyze and identify relationships linking events, people and places.

The presentation will examine how a geospatial approach is used to generate digital twins, building accurate 3D representations, extract and exploit information from multiple data sources. The results can be viewed and shared across communities of interest providing a common view and also the understanding required to enable timely and accurate decision making. It will also demonstrate how generative AI can be used to help build the tools to capture the underlying data itself.

BIO: Nick Sutherland has more than 35 years' experience in the defence and intelligence sectors. With 23 years of military service in the British Army, he filled leadership roles notably as deputy director of the UK Defence Geographic Centre providing geospatial intelligence (GEOINT) and services to operation, and was lead staff officer in SHAPE, NATO. He established a joint GEOINT unit in Northern Ireland, deployed to provide GEOINT in Kosovo, Kenya, Cyprus the United States and Norway and at the UN Mine Action Centre in Sarajevo.

The Zero-Trust Data Centric Challenge— Building a Functional Data Centric Sharing Architecture With Effective Zero Trust Controls

Jim Cosby, CTO, Public Sector and Partners, NetApp U.S. Public Sector Inc. •
cosby@netapp.com

ABSTRACT

Today there are multiple mission partner environments that need to securely share data across coalitions to enable joint all-domain operations for partners and allies. There are major limitations existing today due to unique and separate data technologies implemented by the different agencies and countries. Additionally, security of data must be maintained while being shared and should leverage the latest security and AI capabilities to protect sensitive information. Join this session to learn about an intelligent data infrastructure that provides true hybrid multi-cloud data sharing with built-in artificial intelligence driven security and zero-trust capabilities to ensure safe and effective mission execution.

BIO: Jim Cosby is a chief technology officer at NetApp U.S. Public Sector and has more than 25 years of technology engineering and leadership experience supporting a variety of federal and Department of Defense agencies. Cosby has focused on data management, storage and security for more than 20 years, including on-premises, hybrid and multi-cloud data fabric technologies, which include multi-domain 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.

The MPE Data and Information Sharing Conundrum—Building a Real Data Information Sharing Architecture With Intelligence, Efficiency, Flexibility and Security

Jim Cosby, CTO, Public Sector and Partners, NetApp U.S. Public Sector Inc. •
cosby@netapp.com

ABSTRACT

The United States mission partners all utilize state-of-the-art data sharing technologies. However, many commands have chosen their own unique technology and infrastructure that do not always communicate or share data effectively. In addition, maintaining security levels of data across disparate technologies for data is cumbersome and often ineffective. Join this session to learn how to architect an intelligent data infrastructure that effectively secures and shares data across data fabrics and data backbones for multiple partners and allies while ensure optimal efficiency, security, and flexibility of data management and access.

BIO: Jim Cosby is a chief technology officer at NetApp U.S. Public Sector and has more than 25 years of technology engineering and leadership experience supporting a variety of federal and Department of Defense agencies. Cosby has focused on data management, storage and security for more than 20 years, including on-premises, hybrid and multi-cloud data fabric technologies, which include multi-domain 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.

The Data Interop Imperative—Architecting an Intelligent Data Infrastructure That Effectively and Securely Shares Critical Data to Ensure Mission Success

Jim Cosby, CTO, Public Sector and Partners, NetApp U.S. Public Sector Inc. •
cosby@netapp.com

ABSTRACT

Effective data sharing across partners and allies can be very challenging in today's defense arena. Different technologies and types of data have driven siloed, unique infrastructures that do not play well together. Learn in this session how to architect a unified data sharing backbone and fabric that has built-in artificial intelligence to provide security, efficiency and flexibility for mission execution from the edge to the core and across hybrid multi-clouds.

BIO: Jim Cosby is a chief technology officer at NetApp U.S. Public Sector and has more than 25 years of technology engineering and leadership experience supporting a variety of federal and Department of Defense agencies. Cosby has focused on data management, storage and security for more than 20 years, including on-premises, hybrid and multi-cloud data fabric technologies, which include multi-domain 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.

Achieving CJADC-2 Decision Dominance: Optimizing Cross-Domain Data Flows

John Carbone, Senior Technical Director & Chief CIP Solutions Architect, Everfox •

john.carbone@everfox.com

ABSTRACT

Decision dominance is achieved by providing the right people and systems secure access to the right data at the right time. Making information accessible anytime, anywhere, by securely connecting all branches of service, partners and allies into an internet of military things is the vision of the CJADC-2 program. As part of the CJADC-2 program, cross-domain data integration will empower enhanced situational awareness, assist with decision-making, and improve real-time military operations from the data center to the tactical edge.

Join us for an informative session with John Carbone, PhD, senior technical director/chief solutions architect at Everfox, where he will uncover the intricacies of optimizing cross-domain data flows and enabling artificial intelligence to establish decision dominance for the CJADC-2 program.

BIO: For 35+ years, John Carbone, PhD, has served the defense industry as an engineering fellow, chief science advisor, technology director, chief engineer for innovation, chief data scientist and applied artificial intelligence (AI) with AI ethics and AI security, as well as advanced data science as adjunct professor at Southern Methodist and Baylor University.

His national and international innovations/patents were instrumental in forging bridges between the National Security Agency and Weather High Performance Computing and Big Data/Cloud warfighting architectures, C5ISR enterprise, MDA non-kinetic ISR algorithms, MESH comms architectures, UAV sensor fusion, JADC2 dominance focused 5G designs, dynamic DDIL communications, AI/behavior-based and recent space-based SDWAN & cross domain cybersecurity. Each enabling rapid fielding of vital weapon systems across Ground, Sea, Air and Space and Mission Partner Environments (MPEs).

Carbone has worked White House, H-EMP, and Defense Red Switch, and more recently 5G communications, satellite/space C2 planning, modeling and tracking systems, the first known enterprise, OCONUS big data/clouds, data fusion engines (Alphatec, Oasis, Rosetta), as well as the first android operational smart handheld devices (JSOC RATS) and tactical edge programs deployed to Iraq and Afghanistan (JIEDDO COIC, Navy/Army PGSS, PSDS2, THUNDR) and back CONUS and across the Department of Defense COCOMs, including INDOPACOM, and the intelligence community (IC).

Today, many of these clouds are considered major paradigm shifts for the DoD and the IC. (e.g. RTRG, Ghost Machine, RDP, BDP, Nimbus, DCGS IC/AF/Army/Navy, OpenStack, JIOC-IT, DI2E, NSA Cryptologic Cloud, Army G2 Fixed/ Mobile/ Cloud, Red Disk, CANES, DCGS-A LITE, THUNDR, JSOC RATS).

Carbone currently serves as senior technical director and chief CIP solutions architect at Everfox while developing and teaching transformational master's and PhD curriculum on applied artificial intelligence, self-learning machines and applied data science at Baylor and Southern

Methodist University.

Carbone has a 100+ AI, engineering and data science publications, including AI based Cyber Security, Mining Big Data to Improve National Security, Multi-Disciplinary Systems Engineering, and Applied Cyber Physical Systems to name a few, His newest book by Springer Publishing regarding AI, chatbots, and Large Language Models is “Chatbots, The good, The Bad, and The Ugly.”

Honeytokens for Cloud Threat Detection

Ralph Kahn, GM Federal, Acalvio • rk@acalvio.com

ABSTRACT

CHALLENGES

Cloud breaches are widespread, and insecure identities are the primary cause. Zero trust critically depends on identities being secure. Identity threats are involved in more than 80% of all cyberattacks, including APT threats, ransomware attacks and advanced malware. Attackers harvest identities from multiple cloud resources where secrets/keys are stored. Attackers target identities (user and service accounts, roles, policies) for privilege escalation and access to key cloud data resources. When the threat actors obtain access to valid cloud credentials, their activities and movement within the network are masked as legitimate traffic. In any cloud workload, the identity attack surface can be large, and eliminating all the attack surface is challenging for security teams.

SOLUTION

Honeytokens is a deception technology technique that is proven to be extremely powerful and effective in detecting a variety of identity threats. Honeytokens enable threat detection on all cloud resources. Honeytokens range from deceptive credentials (representing user and service accounts, roles, policies) in identity and access management (IAM) that are specifically designed to lure attackers and deflect them away from real credentials to secrets and data embedded in legitimate cloud resources such as compute instances, secrets manager/vault, serverless functions, container clusters, CI/CD pipelines, etc. where attackers look for leaked credentials. Honeytokens appear to provide attractive pathways for attackers to cloud resources. Any usage or manipulation of these honeytokens is a high-fidelity indicator of a threat. In addition, honeytokens disrupt and delay attacks providing valuable time to SOC to respond.

BIO: Ralph Kahn has more than 30 years' experience in the technology industry. He has held positions in systems engineering, product management, professional services, sales, sales management and business management. Kahn is a proven technologist, business developer and sales leader developing strategy and building teams to grow multiple businesses from zero to more than \$100 million in ARR in just a few years (most recently at Tanium). He has extensive experience in various areas of technology with the last 15 years exclusively in cybersecurity. He has experience in IT security (McAfee, Tanium, etc.) and OT security (Shift5). He is a recognized thought leader in cybersecurity and a resource for key government and industry executives. He is regularly invited to share his knowledge around the globe at top security conferences and in the media.

Asymmetric Advantage: The Crowd as a Force Multiplier

Kent Wilson, VP, Global Public Sector, Bugcrowd • kent.wilson@bugcrowd.com

ABSTRACT

In the realm of cybersecurity, the Department of Defense (DoD) confronts a landscape where asymmetric threats are the norm rather than the exception. Adversaries, wielding the element of surprise and the cloak of anonymity, often leave cyber defenders in a perpetual game of catch-up. This presentation posits a novel strategy to invert this dynamic, advocating for the integration of crowdsourcing as a pivotal component in the DoD's cybersecurity arsenal.

The core premise of our discussion is the inherent power of crowdsourcing to level the battlefield against asymmetric cyber threats. The concept of the “force multiplier” is well-understood, within military strategy, denoting a factor that dramatically increases (multiplies) the effectiveness of an item or group. In the context of cyber defense, we propose the crowd—a global, diverse, and agile assembly of cybersecurity enthusiasts, professionals, and researchers—as this critical force multiplier. By harnessing the collective intelligence, creativity, and skills of the crowd, the DoD can enhance its defensive capabilities far beyond what could be achieved through traditional means alone.

Our presentation will explore several key areas where crowdsourcing offers tangible benefits to cyber defense strategies. First, we examine the acceleration of vulnerability discovery in systems out to the tactical edge. Crowdsourced security programs, such as bug bounties and vulnerability disclosure policies, have proven their worth in the commercial sector by identifying and mitigating risks at a pace unattainable by in-house security teams alone. Applying these models within the DoD can significantly shorten the window of exposure to new threats, thereby reducing the adversary's advantage.

Second, we delve into the role of the crowd in enhancing the security of AI systems, which are increasingly at the heart of DoD operations. As AI technologies evolve, so too do the strategies of those who seek to exploit them. Crowdsourcing can facilitate a continuous, dynamic testing environment for AI systems, ensuring they are robust against both current and future threats.

Furthermore, we address the challenge of skill and knowledge transfer. Crowdsourcing initiatives not only serve as a mechanism for threat detection and mitigation but also as platforms for learning and collaboration. By engaging with the crowd, the DoD can tap into a wellspring of knowledge, staying abreast of cutting-edge techniques and technologies in cybersecurity and AI.

Finally, we propose a strategic framework for the implementation of crowdsourcing within the DoD. This includes guidelines for engaging with the cybersecurity community, ensuring ethical and secure collaboration, and leveraging outcomes to foster a culture of innovation and resilience within the DoD's cyber workforce.

In conclusion, “Asymmetric Advantage: The Crowd as a Force Multiplier” aims to inspire a paradigm shift in how the DoD approaches cybersecurity. By embracing the crowd as a key ally in the battle against cyber threats, the DoD can transform its cyber defense posture from reactive to proactive, from isolated to collaborative,

and from static to adaptive. In doing so, it can secure a decisive advantage in the digital domain, protecting national security in an era of unprecedented challenges and opportunities.

BIO: Kent Wilson is a distinguished technical business leader in the cybersecurity and public sector domain. Currently serving as the vice president of Global Public Sector at Bugcrowd, he is at the forefront of utilizing crowdsourced solutions to enhance the cybersecurity of government and public organizations globally. With a career spanning from a foundational role in the U.S. Army to pivotal positions at Symantec, Rapid7 and other leading cybersecurity firms, Wilson has a proven track record of driving growth, fostering team engagement and pioneering innovative security strategies. An engaging speaker at cybersecurity conferences and workshops, his expertise in building high-performing teams and leveraging crowdsourcing aligns with cutting-edge cybersecurity practices, making him a key figure in transforming public sector cybersecurity resilience.

Optimizing Cloud Storage Solutions for Military Operations: A Path to Enhanced Data Security and Resilience in European Operations

Indira Donegan, Chief Technology Evangelist, Red River • indira.donegan@redriver.com

Jim Cosby, CTO Public Sector and Partners, NetApp • cosby@netapp.com

ABSTRACT

As the U.S. military navigates the complexities of European operations, leveraging cloud technologies becomes paramount for enhancing communication and data sharing among mission partners. This session will explore how cloud solutions from NetApp, combined with Red River's deep understanding of military IT needs, can address the unique challenges faced by organizations across EUCOM, AFRICOM, SOCEUR and DISA EUR. We will discuss strategies for implementing secure, scalable and efficient cloud architectures that facilitate seamless collaboration in joint operations.

This presentation will explore how military organizations can leverage cloud storage solutions to enhance data security and resilience in operations. It will cover best practices for integrating NetApp's technologies with existing IT frameworks, emphasizing scalability, redundancy and compliance with military data protection standards. It will also provide actionable insights for policymakers and IT leaders on navigating cloud adoption while ensuring mission-critical data security.

BIO: Indira Rice Donegan is the chief technology evangelist for Red River Technology, LLC. With nearly \$2 billion in contract support to the DoD/IC and federal civilian agencies, Red River has made a legendary reputation as a trusted mission partner and reseller (VAR) in the U.S. public sector space for close to 30 years. Prior to this role, she was the chief strategy officer and senior strategist and executive business development lead for Data-Centric Hybrid Cloud Solutions at NetApp, U.S.P.S, for the Department of Defense and intel space, where she led strategy development, executive business development and program capture initiatives.

Donegan has a Bachelor of Arts in Spanish and Spanish literature, with extended studies in English, linguistics and organic chemistry from the University of Oregon, a Master of Arts in organizational management from the University of Phoenix, and a fellowship in political science and government affairs from The College of William & Mary, focused on interagency approaches to countering Chinese influence. With more than 20 years of military service as a U.S. Army signal officer, she focused on academic and defense IT/cyber initiatives and communications technologies coupled with a background in acquisition and finance.

Her last assignment on active duty was with the Joint Staff, J6 DD/Cyber Requirements Division, serving as its chief of integration and cyber requirements, cyber/IT budget and legislative affairs, overseeing a \$46 billion cyber/IT portfolio.

Prior to that, Donegan served as the JS J8 representative to the Chairman's Integrated Operations Division (IOD), which developed and advised the Chairman of the Joint Chiefs on strategic dynamic force employment (DFE) and costing for crisis management planning across the Department of Defense's theaters of operation.

Before serving on the Joint Staff, she served as the commander for the 63rd Expeditionary Signal Battalion, "The Nation's Signal Battalion" at Fort Stewart, Georgia, where she deployed the Battalion to Puerto Rico in support of Hurricane Maria disaster relief, conducted numerous MEX-MIL missions across the U.S.-Mexico border for counter narco-trafficking and human trafficking missions, and was the primary tactical signal asset to NORTHCOM for Canadian and Arctic TS/SCI support missions. She served as the executive assistant to the director at the Defense Information Systems Agency and Commander of JFHQ- DoDIN at Fort Meade, Maryland. Additional command positions include HHC, NETCOM, Fort Huachuca, Arizona, and Delta Company, 40th Signal Battalion, 11th Signal Brigade, which she deployed to Operation Iraqi Freedom with the 22nd Signal Brigade.

Donegan is a trustee for the U.S. Army's Command and General Staff College Foundation, serves as on the Executive Board of Directors for AFCEA D.C. Chapter and Rosaries For Heroes 501(c)3, vice president of the Albert J. Meyer Signal Corps Regimental Association for D.C., Virginia and Maryland, president-elect for the Gainesville/Haymarket VA Rotary Club, and is an executive mentor and ambassador for the 501(c)3's Warrior's Ethos and FourBlock, which support transitioning military service members from active duty to industry.

Jim Cosby is a chief technology officer at NetApp U.S. Public Sector and has more than 25 years of technology engineering and leadership experience supporting a variety of federal and Department of Defense agencies. Cosby has focused on data management, storage and security for more than 20 years, including on-premises, hybrid and multi-cloud data fabric technologies, which include multi-domain 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.

Moving Information Superiority Warfare to the Cloud: Opportunities and Challenges

Benedikt Meng, Business Development & Public Affairs Manager, Infodas GmbH •

b.meng@infodas.de

ABSTRACT

We are today in the era of information superiority warfare: modern military operations have become more than just military maneuvers and doctrines, such as MDO and CJADC2, which have highlighted the importance of having the right information at the right time and place to enable decision dominance. In this context, where traditional domains (land, sea, air and space) are interrelated and interconnected through the cyber domain, the need of having data available and accessible becomes imperative.

To cope with this need, nations and organizations are looking at the cloud as an immense source of opportunities. NATO itself, in its digital transformation implementation strategy has identified cloud computing as a part of its digital backbone. On a national level, multiple initiatives, (e.g. the German National Secure Cloud) are investigating how to bring the potential of cloud to military operations.

Alongside with the limitless opportunities offered by the movement to the cloud, there are several challenges and concerns to be considered, especially when dealing with classified information, to balance the need to know (security) with the need to share (connectivity).

The proposed speech elaborates on the current potentialities offered by the military clouds and the possible implementation strategies to bring the secure cloud to the battlefield.

BIO: At Infodas, a subsidiary of Airbus Defence & Space, Benedikt Meng is responsible for strategic business Development and representing the company in matters of public and governmental affairs. Previously, he acquired considerable experience in strategic analysis and strategy development while working for the Inhouse-Consulting of the German armed forces and as advisor for public and private institutions. Furthermore, he is a trained Army reconnaissance and military intelligence officer (Reserve) experienced in leading military teams and advising decisionmakers on various levels. Meng is a member of the Working Group of Young Foreign & Security Policy Experts of the Konrad Adenauer Foundation, a Mercator Foundation Fellow and an Alumnus of the Manfred-Wörner-Fellowship of the German Ministry of Defense and the German Marshall Fund. He regularly speaks, moderates and publishes on current affairs in security and defense policy. Meng holds a B.A. in history and management from the University of Mannheim and a Master of public policy from the Hertie School of Governance and Georgetown University in Berlin and Please Welcome Your New Employee! Washington D.C.

Please Welcome Your New Employee!

Mark Matzke, Area Vice President, Department of Defense, ServiceNow •

mark.matzke@servicenow.com

ABSTRACT

We are thrilled to announce the newest team member joining the organization. Effective immediately your teammate will be taking over all daily tasks that each of you have been required to do every day. Do not get nervous, we hired our newest employee so that each of you can focus on the creative, strategic and fulfilling aspects of your roles. No more spreadsheets or getting lost in complex analysis. We want you to innovate, collaborate, connect with our human customers much more frequently, and, most importantly, enjoy your work. Your newest teammate never had a “real” job before, but they have spent their entire existence, which has not been very long, learning and growing in the digital realm. They literally can recall and use as judgement every digital action we as an organization have ever made.

The “welcome letter” above is a little humorous, but absolutely real. Generative artificial intelligence (GenAI) has been overused as a term for the last 12 months, but it is being leveraged everywhere. This presentation will take the audience through the journey of what the current generation of GenAI technology is doing and is able to do. It is meant to be a primer for those who have not been exposed to the real capabilities and use cases.

Audience members will understand how an organization can create exponential capability, with a small investment, while not adding a single new human to their organization. This is a transformational time and we will show the TechNet Trans-Atlantic attendees how to leverage the capabilities.

BIO: With almost two decades of service impacting many parts of the U.S. federal government, Mark Matzke is the area vice president for ServiceNow’s Department of Defense Business. In addition to government experience, Matzke has worked extensively with the Fortune 500 on global initiatives, as well as product line strategy.

Enhancing Next-Gen C2 Systems for Streamlined, Secure Military Operations

Mark Matzke, Area Vice President, Department of Defense, ServiceNow •

mark.matzke@servicenow.com

ABSTRACT

ServiceNow can significantly enhance the efficiency of next-generation command and control (C2) systems in defense agencies by centralizing operations, automating workflows and bolstering decision-making with advanced analytics. Through a unified platform, ServiceNow enables seamless, real-time data sharing across units, reducing delays and enhancing coordination. Automation streamlines repetitive tasks, like resource allocation and personnel tracking, freeing up personnel for mission-critical duties. Artificial intelligence and predictive analytics improve situational awareness and facilitate faster, data-driven decision-making, while incident management ensures swift problem resolution, minimizing downtime. Additionally, integrated cybersecurity measures protect sensitive data and secure the C2 environment, enabling a resilient and responsive operational structure. Together, these capabilities support improved responsiveness, readiness and overall mission effectiveness for defense operations.

BIO: With almost two decades of service impacting many parts of the U.S. federal government, Mark Matzke is the area vice president for ServiceNow's Department of Defense Business. In addition to government experience, Matzke has worked extensively with the Fortune 500 on global initiatives, as well as product line strategy.

Beyond the Device: Quantum Encryption and the Future of Secure Military Communication

Indira Donegan, Chief Technology Evangelist, Red River • indira.donegan@redriver.com

ABSTRACT

As we approach the reality of widespread quantum computing—often referred to as Year 2 Quantum (Y2Q)—the landscape of military encryption is on the brink of transformation. Most military organizations currently depend on physical bulk (Type 1) encryptors, which are rapidly becoming obsolete in the face of emerging quantum technologies. This session will explore the potential of quantum encryption to eliminate the need for traditional hardware TACLAN devices. We will discuss existing industry solutions that facilitate secure communication in a post-Y2Q world, highlighting how these innovations pivot away from physical reliance to enhance availability and support emergent operations.

BIO: Indira Rice Donegan is the chief technology evangelist for Red River Technology, LLC. With nearly \$2 billion in contract support to the DoD/IC and federal civilian agencies, Red River has made a legendary reputation as a trusted mission partner and reseller (VAR) in the U.S. public sector space for close to 30 years. Prior to this role, she was the chief strategy officer and senior strategist and executive business development lead for Data-Centric Hybrid Cloud Solutions at NetApp, U.S.P.S, for the Department of Defense and intel space, where she led strategy development, executive business development and program capture initiatives.

Donegan has a Bachelor of Arts in Spanish and Spanish literature, with extended studies in English, linguistics and organic chemistry from the University of Oregon, a Master of Arts in organizational management from the University of Phoenix, and a fellowship in political science and government affairs from The College of William & Mary, focused on interagency approaches to countering Chinese influence. With more than 20 years of military service as a U.S. Army signal officer, she focused on academic and defense IT/cyber initiatives and communications technologies coupled with a background in acquisition and finance.

Her last assignment on active duty was with the Joint Staff, J6 DD/Cyber Requirements Division, serving as its chief of integration and cyber requirements, cyber/IT budget and legislative affairs, overseeing a \$46 billion cyber/IT portfolio.

Prior to that, Donegan served as the JS J8 representative to the Chairman's Integrated Operations Division (IOD), which developed and advised the Chairman of the Joint Chiefs on strategic dynamic force employment (DFE) and costing for crisis management planning across the Department of Defense's theaters of operation.

Before serving on the Joint Staff, she served as the commander for the 63rd Expeditionary

Signal Battalion, “The Nation’s Signal Battalion” at Fort Stewart, Georgia, where she deployed the Battalion to Puerto Rico in support of Hurricane Maria disaster relief, conducted numerous MEX-MIL missions across the U.S.-Mexico border for counter narco-trafficking and human trafficking missions, and was the primary tactical signal asset to NORTHCOM for Canadian and Arctic TS/SCI support missions. She served as the executive assistant to the director at the Defense Information Systems Agency and Commander of JFHQ- DoDIN at Fort Meade, Maryland. Additional command positions include HHC, NETCOM, Fort Huachuca, Arizona, and Delta Company, 40th Signal Battalion, 11th Signal Brigade, which she deployed to Operation Iraqi Freedom with the 22nd Signal Brigade.

Donegan is a trustee for the U.S. Army’s Command and General Staff College Foundation, serves as on the Executive Board of Directors for AFCEA D.C. Chapter and Rosaries For Heroes 501(c)3, vice president of the Albert J. Meyer Signal Corps Regimental Association for D.C., Virginia and Maryland, president-elect for the Gainesville/Haymarket VA Rotary Club, and is an executive mentor and ambassador for the 501(c)3’s Warrior’s Ethos and FourBlock, which support transitioning military service members from active duty to industry.

Mission Ready: Ensuring Technical Capability and MPE Integration Across U.S. Partners

Indira Donegan, Chief Technology Evangelist, Red River • indira.donegan@redriver.com

ABSTRACT

As the complexities of joint operations increase, ensuring technical capability and availability for all United States mission partners becomes critical. This session will explore how combatant commands can effectively translate lessons learned into actionable strategies for programmatic success. We will discuss methods for fostering sustained inclusion in the mission partner environment (MPE) while ensuring the efficacy and sustainability of collaborative efforts. Attendees will gain insights into best practices and innovative approaches that can enhance operational readiness and resilience across allied forces.

BIO: Indira Rice Donegan is the chief technology evangelist for Red River Technology, LLC. With nearly \$2 billion in contract support to the DoD/IC and federal civilian agencies, Red River has made a legendary reputation as a trusted mission partner and reseller (VAR) in the U.S. public sector space for close to 30 years. Prior to this role, she was the chief strategy officer and senior strategist and executive business development lead for Data-Centric Hybrid Cloud Solutions at NetApp, U.S.P.S, for the Department of Defense and intel space, where she led strategy development, executive business development and program capture initiatives.

Donegan has a Bachelor of Arts in Spanish and Spanish literature, with extended studies in English, linguistics and organic chemistry from the University of Oregon, a Master of Arts in organizational management from the University of Phoenix, and a fellowship in political science and government affairs from The College of William & Mary, focused on interagency approaches to countering Chinese influence. With more than 20 years of military service as a U.S. Army signal officer, she focused on academic and defense IT/cyber initiatives and communications technologies coupled with a background in acquisition and finance.

Her last assignment on active duty was with the Joint Staff, J6 DD/Cyber Requirements Division, serving as its chief of integration and cyber requirements, cyber/IT budget and legislative affairs, overseeing a \$46 billion cyber/IT portfolio.

Prior to that, Donegan served as the JS J8 representative to the Chairman's Integrated Operations Division (IOD), which developed and advised the Chairman of the Joint Chiefs on strategic dynamic force employment (DFE) and costing for crisis management planning across the Department of Defense's theaters of operation.

Before serving on the Joint Staff, she served as the commander for the 63rd Expeditionary Signal Battalion, "The Nation's Signal Battalion" at Fort Stewart, Georgia, where she deployed the Battalion to Puerto Rico in support of Hurricane Maria disaster relief, conducted numerous

MEX-MIL missions across the U.S.-Mexico border for counter narco-trafficking and human trafficking missions, and was the primary tactical signal asset to NORTHCOM for Canadian and Arctic TS/SCI support missions. She served as the executive assistant to the director at the Defense Information Systems Agency and Commander of JFHQ- DoDIN at Fort Meade, Maryland. Additional command positions include HHC, NETCOM, Fort Huachuca, Arizona, and Delta Company, 40th Signal Battalion, 11th Signal Brigade, which she deployed to Operation Iraqi Freedom with the 22nd Signal Brigade.

Donegan is a trustee for the U.S. Army's Command and General Staff College Foundation, serves as on the Executive Board of Directors for AFCEA D.C. Chapter and Rosaries For Heroes 501(c)3, vice president of the Albert J. Meyer Signal Corps Regimental Association for D.C., Virginia and Maryland, president-elect for the Gainesville/Haymarket VA Rotary Club, and is an executive mentor and ambassador for the 501(c)3's Warrior's Ethos and FourBlock, which support transitioning military service members from active duty to industry.

AI in Action: Revolutionizing Military Decision-Making in Real Time Within the European Theater of Operations

Indira Donegan, Chief Technology Evangelist, Red River • indira.donegan@redriver.com

ABSTRACT

Artificial intelligence (AI) holds transformative potential for military communications, particularly in rapidly changing environments. This session will explore how AI is and can be integrated into communication systems to improve situational awareness, optimize resource allocation and enhance decision-making processes. Participants will learn about practical applications of AI that address specific communication challenges faced by the military in Europe.

BIO: Indira Rice Donegan is the chief technology evangelist for Red River Technology, LLC. With nearly \$2 billion in contract support to the DoD/IC and federal civilian agencies, Red River has made a legendary reputation as a trusted mission partner and reseller (VAR) in the U.S. public sector space for close to 30 years. Prior to this role, she was the chief strategy officer and senior strategist and executive business development lead for Data-Centric Hybrid Cloud Solutions at NetApp, U.S.P.S, for the Department of Defense and intel space, where she led strategy development, executive business development and program capture initiatives.

Donegan has a Bachelor of Arts in Spanish and Spanish literature, with extended studies in English, linguistics and organic chemistry from the University of Oregon, a Master of Arts in organizational management from the University of Phoenix, and a fellowship in political science and government affairs from The College of William & Mary, focused on interagency approaches to countering Chinese influence. With more than 20 years of military service as a U.S. Army signal officer, she focused on academic and defense IT/cyber initiatives and communications technologies coupled with a background in acquisition and finance.

Her last assignment on active duty was with the Joint Staff, J6 DD/Cyber Requirements Division, serving as its chief of integration and cyber requirements, cyber/IT budget and legislative affairs, overseeing a \$46 billion cyber/IT portfolio.

Prior to that, Donegan served as the JS J8 representative to the Chairman's Integrated Operations Division (IOD), which developed and advised the Chairman of the Joint Chiefs on strategic dynamic force employment (DFE) and costing for crisis management planning across the Department of Defense's theaters of operation.

Before serving on the Joint Staff, she served as the commander for the 63rd Expeditionary

Signal Battalion, “The Nation’s Signal Battalion” at Fort Stewart, Georgia, where she deployed the Battalion to Puerto Rico in support of Hurricane Maria disaster relief, conducted numerous MEX-MIL missions across the U.S.-Mexico border for counter narco-trafficking and human trafficking missions, and was the primary tactical signal asset to NORTHCOM for Canadian and Arctic TS/SCI support missions. She served as the executive assistant to the director at the Defense Information Systems Agency and Commander of JFHQ- DoDIN at Fort Meade, Maryland. Additional command positions include HHC, NETCOM, Fort Huachuca, Arizona, and Delta Company, 40th Signal Battalion, 11th Signal Brigade, which she deployed to Operation Iraqi Freedom with the 22nd Signal Brigade.

Donegan is a trustee for the U.S. Army’s Command and General Staff College Foundation, serves as on the Executive Board of Directors for AFCEA D.C. Chapter and Rosaries For Heroes 501(c)3, vice president of the Albert J. Meyer Signal Corps Regimental Association for D.C., Virginia and Maryland, president-elect for the Gainesville/Haymarket VA Rotary Club, and is an executive mentor and ambassador for the 501(c)3’s Warrior’s Ethos and FourBlock, which support transitioning military service members from active duty to industry.

Zero-Trust Implementation in Government: A VAR's Perspective on Achieving Cyber Resilience in the Mission Partner Environment

Indira Donegan, Chief Technology Evangelist, Red River • indira.donegan@redriver.com

ABSTRACT

The zero-trust security model is becoming essential in military information technology environments, particularly within the European theater of operations. This session will delve into the principles of zero trust, the challenges in implementation and how it enhances security for mission partners. Attendees will gain insights into creating a robust security posture that aligns with the dynamic needs of the U.S. military and its allies.

BIO: Indira Rice Donegan is the chief technology evangelist for Red River Technology, LLC. With nearly \$2 billion in contract support to the DoD/IC and federal civilian agencies, Red River has made a legendary reputation as a trusted mission partner and reseller (VAR) in the U.S. public sector space for close to 30 years. Prior to this role, she was the chief strategy officer and senior strategist and executive business development lead for Data-Centric Hybrid Cloud Solutions at NetApp, U.S.P.S, for the Department of Defense and intel space, where she led strategy development, executive business development and program capture initiatives.

Donegan has a Bachelor of Arts in Spanish and Spanish literature, with extended studies in English, linguistics and organic chemistry from the University of Oregon, a Master of Arts in organizational management from the University of Phoenix, and a fellowship in political science and government affairs from The College of William & Mary, focused on interagency approaches to countering Chinese influence. With more than 20 years of military service as a U.S. Army signal officer, she focused on academic and defense IT/cyber initiatives and communications technologies coupled with a background in acquisition and finance.

Her last assignment on active duty was with the Joint Staff, J6 DD/Cyber Requirements Division, serving as its chief of integration and cyber requirements, cyber/IT budget and legislative affairs, overseeing a \$46 billion cyber/IT portfolio.

Prior to that, Donegan served as the JS J8 representative to the Chairman's Integrated Operations Division (IOD), which developed and advised the Chairman of the Joint Chiefs on strategic dynamic force employment (DFE) and costing for crisis management planning across the Department of Defense's theaters of operation.

Before serving on the Joint Staff, she served as the commander for the 63rd Expeditionary Signal Battalion, "The Nation's Signal Battalion" at Fort Stewart, Georgia, where she deployed the Battalion to Puerto Rico in support of Hurricane Maria disaster relief, conducted numerous MEX-MIL missions across the U.S.-Mexico border for counter narco-trafficking and human trafficking missions, and was the primary tactical signal asset to NORTHCOM for Canadian

Donegan is a trustee for the U.S. Army's Command and General Staff College Foundation, serves as on the Executive Board of Directors for AFCEA D.C. Chapter and Rosaries For Heroes 501(c)3, vice president of the Albert J. Meyer Signal Corps Regimental Association for D.C., Virginia and Maryland, president-elect for the Gainesville/Haymarket VA Rotary Club, and is an executive mentor and ambassador for the 501(c)3's Warrior's Ethos and FourBlock, which support transitioning military service members from active duty to industry.

Command and Control Redefined: Fostering a Unified Operational Picture with AI

Indira Donegan, Chief Technology Evangelist, Red River • indira.donegan@redriver.com

ABSTRACT

In the complex landscape of modern military operations, the ability to create and maintain a Common Operational Picture (COP) across different branches of the armed forces and civilian services is essential for effective command and control (C2). This session will explore the critical role of artificial intelligence in supporting and enabling COPs, while also addressing the challenges that arise in crossing both digital and organizational divides. Attendees will gain insights into how we can leverage technology to enhance interoperability and collaboration, ultimately contributing to our strategic defense goals (SDD).

BIO: Indira Rice Donegan is the chief technology evangelist for Red River Technology, LLC. With nearly \$2 billion in contract support to the DoD/IC and federal civilian agencies, Red River has made a legendary reputation as a trusted mission partner and reseller (VAR) in the U.S. public sector space for close to 30 years. Prior to this role, she was the chief strategy officer and senior strategist and executive business development lead for Data-Centric Hybrid Cloud Solutions at NetApp, U.S.P.S, for the Department of Defense and intel space, where she led strategy development, executive business development and program capture initiatives.

Donegan has a Bachelor of Arts in Spanish and Spanish literature, with extended studies in English, linguistics and organic chemistry from the University of Oregon, a Master of Arts in organizational management from the University of Phoenix, and a fellowship in political science and government affairs from The College of William & Mary, focused on interagency approaches to countering Chinese influence. With more than 20 years of military service as a U.S. Army signal officer, she focused on academic and defense IT/cyber initiatives and communications technologies coupled with a background in acquisition and finance.

Her last assignment on active duty was with the Joint Staff, J6 DD/Cyber Requirements Division, serving as its chief of integration and cyber requirements, cyber/IT budget and legislative affairs, overseeing a \$46 billion cyber/IT portfolio.

Prior to that, Donegan served as the JS J8 representative to the Chairman's Integrated Operations Division (IOD), which developed and advised the Chairman of the Joint Chiefs on strategic dynamic force employment (DFE) and costing for crisis management planning across the Department of Defense's theaters of operation.

Before serving on the Joint Staff, she served as the commander for the 63rd Expeditionary

Signal Battalion, “The Nation’s Signal Battalion” at Fort Stewart, Georgia, where she deployed the Battalion to Puerto Rico in support of Hurricane Maria disaster relief, conducted numerous MEX-MIL missions across the U.S.-Mexico border for counter narco-trafficking and human trafficking missions, and was the primary tactical signal asset to NORTHCOM for Canadian and Arctic TS/SCI support missions. She served as the executive assistant to the director at the Defense Information Systems Agency and Commander of JFHQ- DoDIN at Fort Meade, Maryland. Additional command positions include HHC, NETCOM, Fort Huachuca, Arizona, and Delta Company, 40th Signal Battalion, 11th Signal Brigade, which she deployed to Operation Iraqi Freedom with the 22nd Signal Brigade.

Donegan is a trustee for the U.S. Army’s Command and General Staff College Foundation, serves as on the Executive Board of Directors for AFCEA D.C. Chapter and Rosaries For Heroes 501(c)3, vice president of the Albert J. Meyer Signal Corps Regimental Association for D.C., Virginia and Maryland, president-elect for the Gainesville/Haymarket VA Rotary Club, and is an executive mentor and ambassador for the 501(c)3’s Warrior’s Ethos and FourBlock, which support transitioning military service members from active duty to industry.

Empowering Government Agency Innovation through ServiceNow's Generative AI

Eric Silverstein, Director, Solution Consulting Architecture, ServiceNow •

eric.silverstein@servicenow.com

ABSTRACT

Generative AI (GenAI) is already transforming traditional workflows. Tools like ChatGPT, Siri and Google Assistant are streamlining processes, boosting productivity and optimizing workflows in the commercial world. The demand and expectation for these capabilities within government agencies is exploding, with stakeholders and constituents who want smarter systems that remove friction and frustration from mundane tasks, fast and accurate answers to questions and personalized experiences to improve user satisfaction.

ServiceNow understands that AI is only as good as the platform it's built on, which is why to maximize probability of a successful GenAI solution, agencies must enable a comprehensive approach that brings data, AI, and automation together on a single platform with the security and scalability required by government agencies. In addition, government agencies must consider the data and workloads in their environment and adopt domain-specific large language models (LLMs) purpose-built for their use cases to increase model accuracy and improve model response times while remaining cost-effective and sustainable.

ServiceNow has gained experience within US Federal agencies by applying the Now Assist Skill Kit, enabling teams to develop skills and create and publish custom prompts that provide relevant, contextual and trusted data to inform decision-making across the enterprise. Through discussion of practical applications of AI, to best practices and strategies for federal technology teams to harness generative AI in support of their mission objectives, we can explore how GenAI is transforming operational efficiency and enhancing decision-making for government agencies.

BIO: Eric Silverstein is a seasoned professional in the field of solution consulting architecture, currently serving as the senior manager for the U.S. federal sector at ServiceNow. With a robust background in the intricacies of solution consulting, Silverstein has played a pivotal role in shaping and implementing innovative solutions to address the unique challenges within the federal domain.

Ensuring Business Continuity with ServiceNow: The Power of Mission Resiliency

Eric Silverstein, Director, Solution Consulting Architecture, ServiceNow •

eric.silverstein@servicenow.com

ABSTRACT

The presentation focuses on the importance of ensuring business continuity through ServiceNow's offerings. It highlights the concept of mission resiliency, which is crucial for modern business operations in an increasingly complex digital landscape. ServiceNow is a leader in this arena, helping organizations manage workflows, automate processes, and maintain continuity even in challenging circumstances.

The presentation delves into the Vault add-on, a premium feature that provides real-time replication of the ServiceNow database to a tertiary site owned by the customer. This ensures that customers have access to their data even during emergencies, allowing them to work with ServiceNow in a self-hosted instance if the SaaS instance is no longer reachable.

Key benefits of mission resiliency include enhanced business continuity, peace of mind for customers and operational efficiency. The Vault add-on supports compliance with industry regulations, reduces the risk of data loss and improves overall security posture. Real-time replication and self-hosted instances provide flexibility and control, ensuring that organizations can respond effectively to disruptions.

ServiceNow's mission resiliency framework, supported by the Vault add-on, offers invaluable benefits to organizations. It ensures business continuity, protects critical data and provides the peace of mind that enables teams to innovate and adapt. The features of real-time replication and self-hosted instances further solidify this framework, allowing businesses to navigate disruptions with confidence.

BIO: Eric Silverstein is a seasoned professional in the field of solution consulting architecture, currently serving as the senior manager for the U.S. federal sector at ServiceNow. With a robust background in the intricacies of solution consulting, Silverstein has played a pivotal role in shaping and implementing innovative solutions to address the unique challenges within the federal domain.

Deploying Software as a Service (SaaS) for Government Agencies with ServiceNow

Eric Silverstein, Director, Solution Consulting Architecture, ServiceNow •

eric.silverstein@servicenow.com

ABSTRACT

SaaS has revolutionized the way government organizations access and utilize software, offering unparalleled flexibility, scalability and cost-efficiency. Federal and civilian agencies have the challenging task of bringing these benefits to the enterprise, its stakeholders and constituents, while effectively securing and protecting matters of national security. Deploying SaaS involves several critical steps with success, ultimately stemming from three key pillars: governance, execution and adoption.

ServiceNow has extensive expertise in providing a platform that enables outsourcing of enterprise-wide information technology functions, and in guiding strategy to enable stakeholder and constituent success. The ServiceNow platform itself has been used to support DoD use cases with 700,000-plus users, while enabling scalability and security of data, processes, and integrations at all classification levels. Our experts have conducted comprehensive assessments of organizational needs to ensure success in deploying SaaS solutions, and guided executive leadership teams, delivery teams and organizational change management to enable success for governments globally.

Recent use cases include the deployment of ServiceNow as the enterprise IT platform for Air Force Service Management, through the Department of the Air Force Enterprise IT as a Service effort (DAF EITaaS). Other use cases include the Army Enterprise Service Management Platform, and lessons learned from across Federal DoD, Civilian, and Intelligence agencies. Deploying SaaS at ServiceNow involves a strategic, user-focused approach that prioritizes scalability, security, integration, and ongoing support. By leveraging the power of SaaS, government agencies can achieve their digital transformation goals and drive operational excellence.

BIO: Eric Silverstein is a seasoned professional in the field of solution consulting architecture, currently serving as the senior manager for the U.S. federal sector at ServiceNow. With a robust background in the intricacies of solution consulting, Silverstein has played a pivotal role in shaping and implementing innovative solutions to address the unique challenges within the federal domain.

Zero-Trust Architecture With the Now Platform—Systematically Harden the Digital Attack Surface

Scott Flynn, Advisory Solution Consultant, ServiceNow • scott.flynn@servicenow.com

ABSTRACT

European mission partners face significant challenges in implementing zero-trust architecture (ZTA) across federated networks. Diverse identity sources and distinct security boundaries create obstacles to secure, data-centric collaboration. ServiceNow addresses all zero-trust pillars—user, devices, application and workload, data, network and environment, automation and orchestration, visibility and analytics —through integrated workflows.

Anchored by the Configuration Management Database (CMDB), ServiceNow's platform provides mission partners with full visibility into information technology, software, hardware and enterprise assets, enabling comprehensive monitoring, security, and compliance across complex environments. Integrated security workflows support automated security incident handling and prioritized remediation based on threat intelligence, while risk-based vulnerability management streamlines detection and response across expanding attack surfaces.

ServiceNow's Zero Trust Access improves security by enforcing multi-factor authentication, policy-based session controls, and contextual access policies to maintain least-privilege access. Integrations with 19 of 24 NIST Zero Trust Architecture vendors facilitate cross-boundary interoperability, enabling secure identity federation and data sharing across disparate environments. Additionally, ServiceNow Vault safeguards sensitive data to meet regulatory mandates, reducing exposure and protecting against insider threats.

This session will demonstrate how ServiceNow's comprehensive approach to Zero Trust empowers mission partners to achieve resilient, secure, and collaborative operations across federated networks, supporting a data-centric approach to shared security.

BIO: Scott Flynn began his career enlisting in the U.S. Army in 1991 at the age of 17. He entered the Signal Corp as a 29V. Supporting secure, global IT operations in South Korea and at the Pentagon Army Tech Control and Army Operation's Center, Flynn was honorably discharged in 1996. For more than 30 years, Flynn has supported the secure global communications of the Department of State, U.S. Navy, U.S. Marine Corps, U.S. Air Force, White House Communications Agency, and several other U.S. intelligence agencies focusing specifically on cybersecurity and RMF via ICD-503. Flynn has a bachelor's degree in information technology and a master's degree in cybersecurity. Certified in several network disciplines, Flynn also holds a CISSP certification as well as ServiceNow's CSA.

Empowering the Cyber Workforce with Automation and Orchestration within ServiceNow

Scott Flynn, Advisory Solution Consultant, ServiceNow • scott.flynn@servicenow.com

ABSTRACT

The evolving threat landscape demands a resilient cyber workforce capable of implementing and maintaining zero-trust security across federated networks. ServiceNow equips organizations to meet this need by providing a unified platform through centralized case management that supports the entire cyber workforce lifecycle—from recruitment and training to operations and career development.

ServiceNow's automated workflows and context-based vulnerability management prioritize and optimize the cybersecurity workforce response to risks and threats.

Security operations and integrated risk management workflows collaborate to ensure policy and governance are leveraged within risk and compliance. ServiceNow's adaptive Zero Trust Access platform controls and seamless integrations with industry-standard tools enable cyber teams to enforce least-privilege access and protect sensitive data, ensuring compliance with policy and regulatory standards.

This session will explore how ServiceNow strengthens cyber workforce resilience, providing security professionals with the resources and support they need to thrive within a Zero Trust framework.

BIO: Scott Flynn began his career enlisting in the U.S. Army in 1991 at the age of 17. He entered the Signal Corp as a 29V. Supporting secure, global IT operations in South Korea and at the Pentagon Army Tech Control and Army Operation's Center, Flynn was honorably discharged in 1996. For more than 30 years, Flynn has supported the secure global communications of the Department of State, U.S. Navy, U.S. Marine Corps, U.S. Air Force, White House Communications Agency, and several other U.S. intelligence agencies focusing specifically on cybersecurity and RMF via ICD-503. Flynn has a bachelor's degree in information technology and a master's degree in cybersecurity. Certified in several network disciplines, Flynn also holds a CISSP certification as well as ServiceNow's CSA.

Leading at Flank Speed: How Digital Champions Secure Zero Trust Advantage

Steven Kyle Denton, N-MRO Resource Sponsor, OPNAV N4 •

steven.k.denton4.civ@us.navy.mil

ABSTRACT

In 1966, Adm. H. G. Rickover succinctly captured the essence of the technological age: “By boring into the secrets of nature, scientists have discovered keys that will unlock powerful forces which are then put to practical use by technology.” As technological change accelerates, a revolution in global dynamics is unfolding, presenting both opportunities and challenges. This is particularly evident in the U.S. Navy, where emerging technologies such as artificial intelligence intersect with the forces of Great Power Competition and rapidly evolving societal trends. This research focuses on the Navy’s ‘digital champions’—leaders driving the integration of zero-trust security and digital innovation within this complex global framework.

This approach aligns with Rickover’s advocacy for a human-centric view of technology. He asserted a fundamental truth about technological change: “The threat does not inhere in the apparatus itself; technology is neutral. It lies in ourselves, in the way we look at technology, for this determines what we do with it.” In this vein, we present proven methods for military organizations to cultivate and accelerate digital transformation through the leadership and influence of digital champions.

BIO: Steven Kyle Denton, PhD[c], has served 20 years across government, industry and academia in various leadership roles. Currently stationed in Washington, D.C., Denton supports the Navy as an industrial depot maintenance expert, bolstered by his academic research areas focused on strategy, transformation and leadership in the role of technological change.

Creating Order out of Chaos— Understanding Your Cyber Adversary and How to Defeat Them by Modernizing Technology and Increasing Warfighter Productivity

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

ABSTRACT

U.S. and ally cyber and IT operators are on the frontline of protecting our nations' most sensitive cyber terrain. Threats are increasingly complex, speedy and relentless; creating opportunities in the shadows and complexity of our networks. Adversaries act to disrupt, deny and degrade the capabilities and lethality of our formations. Current point solutions, bifurcated security and information technology teams and lack of intelligence across the cyber domain create gaps and seams easily exploited by the enemy. Couple these facts with the lack of human resources in skilled cybersecurity positions and you have a recipe for disaster. Today, our focus will be on understanding our adversary; their motives, tactics, techniques and procedures while simultaneously leveraging that information to protect and defend our critical infrastructure at speed and scale. Speed is the key word—today's next-generation tools reduce mean time to defend cyber incidents, reduce alert fatigue and allow defense teams to critically and efficiently analyze data to stop breaches—technology becomes a force multiplier. Leveraging next-generation capabilities and enabling zero trust principles enables decision dominance and empowers teams to dominate through greater understanding, speed and resilience.

Sun Tzu wrote: "If you know the enemy and know yourself, you need not fear the result of a hundred battles."

Modern EDR solutions that take advantage of next-generation technologies such as AI/ML, integrated threat intelligence and vulnerability and patch management provide the necessary visibility into endpoint activities, allowing for real-time detection of malicious behavior and enabling swift responses to potential breaches. More time can be spent threat hunting vs. threat identification and verification. In essence, Next Gen EDR transforms endpoints from vulnerable targets into active lines of defense leveraging the single source of data and truth that supports exactly what Sun Tzu wrote about.

- We will dive into the current and emerging threat landscape affecting our warfighting formations and governments.

- We will explore why a platform-approach to security eliminates blind spots, reduces overhead, streamlines operations and empowers teams to provide actionable results.
- And, most importantly, we will address those tactics, techniques and procedures each of our operators face every day in defending these critical systems.

CrowdStrike, a leader in cybersecurity, offers advanced EDR capabilities through its Falcon platform, which is tailored to meet the unique needs of defense agencies. CrowdStrike's cloud-native architecture, powered by AI and machine learning, delivers unparalleled speed, scalability, and accuracy in threat detection and response. Harnessing AI and machine learning empowers our soldiers to do more with less. This makes it an ideal partner for defense agencies seeking to bolster their defenses.

BIO: Jeff Worthington, executive strategist, sits on the Executive Strategist Team at CrowdStrike, where he provides strategic advisory services related to enterprise cybersecurity solutions for all industry verticals, including government, education and health care. Prior to joining CrowdStrike, he served as the chief information officer for the Joint Special Operations Command capping a career of uniformed federal service spanning 30 years installing, operating, maintaining and defending the United States' most vital information network across the globe. He has served in positions from the foxhole to the White House in both conventional and airborne special operations units.

Layered PACE Model for C2 Planning

Chief Warrant Officer 3 William Holden, Network Operations Warrant Officer, Joint Multinational Readiness Center • william.j.holden.mil@army.mil

ABSTRACT

Army Signal planners have used the Primary, Alternate, Contingency and Emergency (PACE) model for many years, but our observation at the Joint Multinational Readiness Center (JMRC) is that PACE plans are too simple and limited for the modern brigade and division. Inspired by the graph structure of a neural network, we propose a layered PACE model, which has a transport layer, a network layer and an application layer. Signal planners can easily visualize the layered PACE plan using tools such as GraphViz, and one may apply matrix multiplication to assess the efficacy and survivability of the plan. The application layer aids senior leaders form decisions about their Command-and-Control architecture independent of the communications infrastructure.

BIO: Chief Warrant Officer 3 William John Holden is a network operations warrant officer and an observer-coach/trainer at the Joint Multinational Readiness Center (JMRC) at Hohenfels, Germany. In his current role, Holden has coached brigade S6s from American, German and Ukrainian units. He has a master's degree in computer science from the University of Louisville. His recent assignments include Allied Command Counterintelligence, Regional Cyber Center-Korea and Special Operations Joint Task Force-Operational Inherent Resolve.

The Software Defined Enterprise & Autonomic Networking

Ken Camp, Network Capabilities Leader - Office of CTO, Tyto Athene •

ken.camp@gotyto.com

ABSTRACT

In an era where mission-critical operations across diverse geographical regions increasingly hinge on the robustness and responsiveness of network infrastructures, there is a compelling need to enhance network systems to achieve greater intelligence and resilience. This discussion outlines a comprehensive approach for developing a software defined enterprise infrastructure utilizing cutting-edge technologies such as artificial intelligence (AI)-driven analytics, automated network management, real-time adaptability and enhanced security measures. The recommended approach provides the groundwork for the fully autonomic network. For the EUCOM and coalition partners, where emerging technology integration, interoperability with allies and partners, cybersecurity and threat resilience are paramount, this reliance is magnified. The demand for advanced network solutions is driven by the need for superior performance, resilience and security to meet the challenges of modern warfare and strategic operations.

Autonomic network systems aim to manage technology resources with nominal human intervention. These systems are characterized by several self-managing properties:

- Self-Configuration
- Self-Optimization
- Self-Healing
- Self-Protection

Management is no longer about controlling “a device” but managing the optimized performance of the entire enterprise technology stack.

Autonomic network systems are transforming the way IT infrastructures are managed by introducing self-managing capabilities that reduce human intervention, enhance efficiency, integrate Zero Trust security enablement, and improve reliability, paving the way for smarter and more resilient networks, application services, and data centers.

BIO: Ken Camp leads the network capabilities development for Tyto Athene, LLC, a federal systems integrator based in Herndon, Virginia. Camp is focused on IT strategies around

service delivery, enterprise architecture, cybersecurity and emerging technologies. He has extensive experience in the networking and communications industries managing global teams of engineers, architects and sales executives in direct and matrix managed organizations. His portfolio of work includes global telecommunications and IT implementations, including major redesigns for security, continuity of operations/disaster recovery, cost recovery and performance improvement programs.

He has delivered architecture development of solutions for the enterprise and workforce of 2025 and beyond in SDWAN, cloud computing, Internet of Things and big data technologies. Camp regularly led M&A due diligence, integration, spinoffs and enterprise reorganization. He brings deep experience developing and deploying strategies that solve complex business issues with integrated, innovative IT solutions, with demonstrable history in networking/internet/telecommunications, pharmaceutical, financial services, engineering, publishing, education and government (defense and civilian) sectors translating architecture strategies into measurable, successful deliverables.

A Practical and Scalable Implementation of the Vernam Cipher, under Shannon Conditions, Using Quantum Noise

Adrian Neal, Senior Director and Global Lead for Post-Quantum Cryptography, Oxford Scientifica • adrian.neal@oxfordscientific.com

ABSTRACT

The one-time pad cipher is renowned for its theoretical perfect security, yet its practical deployment is primarily hindered by the key size and distribution challenge. This paper introduces a novel approach to key distribution, designed to make symmetric-key cryptography, and the one-time pad cipher in particular, a viable option for contemporary secure communications, and specifically, post-quantum cryptography, leveraging quantum noise and combinatorics to ensure secure and efficient key-distribution between communicating parties. We demonstrate that our key-distribution mechanism has a variable, yet quantifiable hardness of at least 504 bits, established from immutable mathematical laws, rather than conjectured-intractability that is common to many cryptographic key encapsulation or exchange mechanisms, and how we overcome the key-size issue with a quantum-noise seeded key-generation function, having a system hardness of at least 2304 bits, while introducing sender authentication and message integrity. While the proposed solution has potential applications in fields requiring very high levels of security, such as military communications and large financial transactions, it is sufficiently practical and scaleable for use in common browser-based web-applications, on both personal computers and mobile devices.

BIO: Adrian Neal, a two-time winner of the NATO Defence Innovation Challenge, is an internationally recognised cybersecurity & cryptographics expert and currently holds the position of Senior Director and Global Lead for Post-Quantum Cryptography at Capgemini.

GitOps for Edge Applications in Denied, Disrupted, Intermittent and Limited (DDIL) Environments

Zachary Yates, Sr. Solution Architect, GitLab • zyates@gitlab.com

ABSTRACT

Learn how to leverage a GitOps methodology to rapidly configure edge computing hardware, sensors and applications for a range of mission profiles. With use cases spanning Tactical Awareness Kits (TAK/ATAK), Fly Away Kits (FAK), vehicles and airframes, operators can apply well understood modern software deployment techniques such as Infrastructure as Code (IaC) and Continuous Integration/Deployment (CI/CD) to create a robust and flexible infrastructure capable of operating in denied, disrupted, intermittent, and limited (DDIL) environments. The presentation will focus on concepts that can be applied to any set of technologies, while the demo will provide a targeted solution based on GitLab and container networking technologies.

BIO: Zachary Yates has served in many public sector roles over the past 15 years, ranging from building DevOps teams to serving as chief architect for a CBP program.

Is Your Acquisition and Zero-Trust Plans Set Up to be Cyber Survivable?

Steve Pitcher, Senior Cyber Survivability Analyst, Joint Staff J6 •

steve.e.pitcher.civ@mail.mil

ABSTRACT

The Department of Defense (DoD) has a challenging situation fielding and sustaining warfighting capabilities, due to the threats targeting survivability of its weapon systems. However, the DoD's cyber vulnerability risk is not due to a lack of cybersecurity strategies, policies or minimum standards to counter these threats. Instead, the DoD's cyber survivability efforts have highlighted the lack of cybersecurity and cyber resilience performance requirements considered during cost, schedule and performance risk trade space decisions.

Cybersecurity doesn't have to cost more, and the DoD should demand more for the resources expended. Relying on standards compliance alone has not worked and Defense Systems Management College studies have shown:

- 70% of defects were introduced before coding began
- 80% of defects were found after 95% of funds were committed
- 97% of rework costs were identified too late and were too costly to influence design
- Sponsors were left with the untenable choice of cancelling the program or accepting system risk

The Cyber Survivability Endorsement helps requirement sponsors (senior non-cybersecurity professionals) define plain language, mission focused, threat informed and system specific cyber survivability performance requirements. Once these cybersecurity and cyber resilience requirements are defined as performance attributes, they can be considered during an alternatives analysis and contract source selection to prevent pursuit of inherently flawed capabilities, with no reasoned expectation the vulnerability risks could be cost effectively mitigated to an operationally acceptable risk posture. They can also guide system security engineers to flow zero trust and MPE requirements into system specifications to ensure systems are secure by design.

BIO: Steve Pitcher is the senior cyber survivability analyst for the Joint Staff J6. During his 20 years in the Air Force, and 20 years as a government civilian with the Missile Defense Agency and Joint Staff, he has held several cybersecurity, command and control, modeling and simulation, information sharing, joint/coalition operations, and cyber survivability positions. As part of the Joint Staff, Pitcher focused on developing cybersecurity approaches to enable coalition interoperability, with authoritative data services and web-based presentation applications to rapidly deploy a hybrid mission planning and execution network. More recently, he has worked to define how properly articulated cyber survivability threshold performance requirements can reduce resource and mission risk for the acquisition of warfighter systems, by ensuring cybersecurity and cyber resilience performance requirements are included in a program managers

cost, schedule and performance risk trade space. This has been transformational in driving cybersecurity and cyber resilience consideration within DevOps, and validation of the effectiveness of implementation during DevSecOps—helping to ensure warfighting capabilities are secure and resilient by design.

Future-Ready Defense Networks: Leveraging Zero-Trust Architecture for Secure, Real-Time Military Collaboration

Rob Bair, CISO in Residence, Zscaler • rbair@zscaler.com

ABSTRACT

In today's rapidly evolving defense landscape, the ability to securely share information with mission partners is paramount. NATO and international defense organizations rely on advanced collaborative environments to facilitate seamless cooperation and ensure that the right information reaches the right people at the right time.

This session will explore how a zero-trust architecture empowers these critical partnerships by providing robust security solutions tailored for mission partner environments with a special focus on CJADC2 (Combined Joint All-Domain Command and Control) and operations at the Tactical Edge including:

- **Enhanced Security for Mission Partner Environments:** Discover how a zero-trust architecture fortifies collaborative platforms, enabling secure information sharing across all domains for NATO and international defense partners.
- **Optimizing CJADC2:** Learn about Zscaler's role in enhancing CJADC2, ensuring real-time, secure communication and decision-making capabilities for multinational operations.
- **Tactical Edge Excellence:** Understand how zero trust supports operations at the tactical edge, ensuring that frontline personnel have secure, reliable access to critical information wherever they are.

This session is designed for defense and security professionals across NATO and international partner nations who are keen on enhancing their collaborative capabilities in a secure and efficient manner.

BIO: Robert (Rob) Bair is chief information security officer (CISO) Americas for Zscaler. Prior to joining Zscaler he served as executive director at Team Cymru, a cybersecurity and threat intelligence firm providing comprehensive visibility into global cyber threats. He served 20 years as an officer in the

United States Navy. His most recent military assignment was as the director for cybersecurity and operations policy at the National Security Council. He previously served as a director for intelligence programs at the National Security Council. Bair completed multiple tours at the National Security Agency, U.S. Cyber Command and Fleet Cyber Command/TENTH Fleet with experience in both offensive and defensive cyber operations. He served in several intelligence and counterterrorism assignments, including the national counter-narcotics detection and monitoring task force, and deploying to Afghanistan with a Joint Special Operations Task Force. He

began his naval career as a submarine officer serving aboard the USS Tennessee (SSBN 734 Blue). Bair served as the military aide to the Deputy Chief of Naval Operations

for Fleet Readiness and Logistics (N4) and Deputy Chief of Naval Operations for Warfare Systems (N9) and was the executive assistant to the commander, Fleet Cyber Command/TENTH Fleet.

Achieving Performance-Based Outcomes and Innovation When Outsourcing ICT Services With GSA AAS

Michael Baumann, Division Director, Assisted Acquisition Services Army, U.S. General Services Administration • michael.baumann@gsa.gov

ABSTRACT

Use of performance-based contracts when outsourcing IT services with GSA Assisted Acquisition Services Army (AAS Army) streamlined acquisition processes enables stakeholders to achieve their objectives and drive performance results in IT Service Management, whether that is through a managed service like SAAS or traditional enterprise IT services. There are several key factors that establish the framework for success: Awarding contracts on a best-value-trade-off (BVTO) basis, structuring contracts with incentives aligned to IT Service Level Agreements (SLAs), and ensuring the Government executes proper Quality Management.

- Using BVTO as an evaluation methodology focuses the award decision on what an IT contractor brings to the table. The focus of selecting an industry partner is on the merits of their understanding, effectiveness, and innovation with emerging concepts like AI, ZTA or DevSecOps proposed by an offeror, and not on the price of an offeror.
- When outsourcing IT, whether it is SAAS or traditional services model, it is advantageous to the government to use a performance-based approach to incentivize positive performance. This means writing a contract where the industry partner receives a financial incentive for meeting or exceeding performance thresholds.
- Oftentimes, when outsourcing a service, the government focuses on the execution of the contract. While this is important, it is only part of the equation. The more important part is building a partnership with the industry partner and ensuring the Government entity is trained and vested in quality management for the life of the contract. Building a proper surveillance structure and QASP is imperative to drive performance in outsourced efforts.

BIO: Michael Baumann currently serves as a division director for GSA FAS, Assisted Acquisition Services Army (AAS). In his role, he oversees the technical solution and project delivery of an \$8 billion portfolio of large and complex acquisitions throughout the Mid-Atlantic and Europe, Middle East and Africa (EMEA) Regions.

Baumann has more than 15 years of federal service leading large and complex IT and ISR acquisitions with the General Services Administration, primarily servicing the U.S. DoD, intelligence community and NATO. Prior to his current role, he served as the operations manager for GSA Region 3, AAS. In addition, he also served as the EMEA branch chief for GSA Region 3, AAS

in Wiesbaden, Germany, embedded with the U.S. Army Europe and Africa (USAREUR-AF); and served as a senior project manager for Region 3, AAS in Philadelphia and Germany, and is a graduate of the Federal Career Intern Program.

His awards include AFCEA Distinguished Young Professional Award, AFCEA Albert J. Myer Award, Civilian Service Commendation Medal - Department of Army, multiple GSA FAS Commissioner Spotlight on Success Awards, FEB Philadelphia - Collaborations Champion Gold Medalist, Samuel J Heymen Service to America Medals - Emerging Leaders Nominee, GEARS Team Agency Nominee - Accountable Stewardship, and FEB Philadelphia - Excellence in Government.

Baumann holds a Master of Science in major programme Management from the University of Oxford, Leadership for a Democratic Society Diploma from Federal Executive Institute, Certificate in Leading Teams for Emerging Leaders from London Business School, and a Bachelor of Science in business administration from Villanova University.

Cyber Threats and Mitigations for Briefing Rooms

Zohar Vered, Vice President, Marketing & Sales, High Sec Labs •

Zohar@highseclabs.com

ABSTRACT

Briefing rooms are an indispensable tool in reaching complex decisions. A briefing room will typically have access to multiple network domains, large display screens and video and teleconferencing capabilities. Securing the briefing room from cyber-attacks is an essential component in the overall security plan used to protect the occupants and the contents of the briefings. This session will cover the different types of attacks targeted at exfiltrating information or injecting malicious code into secure network domains. Topics covered will describe hacks that repurpose conferencing speakers to become microphones or high-frequency data modems, exploitation of display screens and other peripheral devices as intermediaries for unauthorized exchange of information between network domains, threats from inadvertent transmission of sensitive conversations through communication devices assumed to be off-line, and the inherent threats of data leakages from peripheral sharing devices such as KVM switches. Risk mitigations to these threats will be described. The leading cyber-security standards applicable to the briefing room / commander offices will be covered.

BIO: Zohar Vered has more than 20 years of experience in global high-tech product definition, information technology and systems analysis. For the past 12 years, Vered has been serving as the chief marketing officer at High Sec Labs, defining product lines for NIAP and TEMPEST certified peripheral sharing switching devices including KVMoIP networks, KVM switches, matrix solutions, cross-domain solutions and multiviewer and video scaling products. Vered has served in the Israel Defense Forces and holds a Bachelor of Arts degree from Tel Aviv University.

Cybersecurity Methods for Command and Control Centers

Zohar Vered, Vice President, Marketing & Sales, High Sec Labs •

Zohar@highseclabs.com

ABSTRACT

Today's battlefield leverages multiple sensors and intelligence systems along with unclassified feeds such as news reports to gain the best possible understanding of the environment in which warfighters will be engaging the enemy. This scenario, in which multiple network domains of different classification levels are accessed and displayed side-by-side on the same monitor, poses threats of data leakage from higher classification to lower classification networks, along with the insertion of malicious code from a lower classification to a higher classification domain. The session will review the topology and architecture of a secure command and control room, allowing operators to work with and interact with different networks having different certifications. Common threats will be presented, and mitigation plans will be suggested. The session will look at components from workstations and KVM over IP to video wall controllers and will suggest functionality and cybersecurity safeguards. The security threats of both topologies will be addressed. Hardware- and software-based solutions to these threats will be discussed along with accepted Industry protection profiles and certifications.

BIO: Zohar Vered has more than 20 years of experience in global high-tech product definition, information technology and systems analysis. For the past 12 years, Vered has been serving as the chief marketing officer at High Sec Labs, defining product lines for NIAP and TEMPEST certified peripheral sharing switching devices including KVMoIP networks, KVM switches, matrix solutions, cross-domain solutions and multiviewer and video scaling products. Vered has served in the Israel Defense Forces and holds a Bachelor of Arts degree from Tel Aviv University.

Empowering Battlefield Commanders in Contested Environments: Leveraging Software-Defined Wide Area Networking (SD-WAN) for Mission-Critical Application Delivery

Michael Maice, Sr. Technical Advisor, Juniper Networks • mmaice@juniper.net

ABSTRACT

In modern warfare, battlefield commanders rely on real-time access to mission-critical applications for effective decision-making and force employment. However, near-peer adversaries maintain advanced electronic warfare (EW) capabilities that threaten to disrupt critical info flows. Software-Defined Wide Area Networking (SD-WAN) can safeguard delivery of essential applications for battlefield commanders and their mission partners, even in the face of sophisticated EW attacks.

SD-WAN goes beyond traditional routing by enabling granular application identification and incorporating telemetry data with service level agreement (SLA). Adversary electronic warfare (EW) attacks, such as jamming and GPS spoofing, manifest on the network as degraded performance, including increased packet loss, jitter, latency and errors. SD-WAN allows the network to dynamically adapt to these conditions, prioritizing mission-critical applications and ensuring commanders maintain access to vital information

Drawing upon real-world examples observed in the Ukraine conflict, this presentation will demonstrate how SSR can mitigate the impact of adversary EW activities on critical applications, such as:

- Command and Control (C2) systems: SSR ensures reliable communication and data exchange for commanders to direct forces and coordinate operations effectively.
- Intelligence feeds: SSR prioritizes the delivery of real-time intelligence data, enabling commanders to maintain situational awareness and make informed decisions.
- Improve decision-making: By ensuring reliable delivery of critical information, SSR supports informed decision-making at all levels of command.
- Increase operational tempo: SSR helps maintain a high operational tempo by ensuring commanders have the tools they need to execute missions effectively.

BIO: Michael Maice is a retired Army warrant officer and seasoned technology leader who

brings a unique perspective to battlefield communications. With experience spanning both military deployments to the Middle East and private-sector leadership at Juniper Networks, Archon (a CACI company), and Klas, he understands the challenges of delivering mission-critical applications in contested environments.

During his military career, Maice held key positions with 18th Airborne Corps, the Joint Communications Unit and the Joint Communications Support Element, gaining firsthand knowledge of tactical networking needs. He is a recognized thought leader with publications and podcast appearances covering CSfC and military technology.

In this presentation, Maice will draw on his expertise with Juniper's SSR product and real-world experience to discuss how application-aware networks can provide autonomous resilience and support distributed Command and Control in an era of electronic warfare.

Maintaining Mission Readiness and Protecting COP Collaboration with Physics not Software

Christian Hager, VP of Sales & Business Development, Fend Inc. • chager@fend.tech

ABSTRACT

With increasing threats in cyberspace, allies across Europe are being drawn into “cyberconflict” operations in C4ISR and cyber.

One can argue that without a secure, efficiently operating base, enhanced partner force integration could be flawed or jeopardized. And if operational data from critical field systems cannot be monitored remotely and securely in real time, the common operational picture COP itself may be called into question.

It is necessary to maintain mission readiness on base and uphold quality of life for personnel by enabling real-time operational visibility of all base-critical infrastructure and facilities-related control systems (FRCS). This also includes managing energy efficiency standards, collaboration with local utilities to maintain energy and water provisioning, ensuring minimal operational downtime through predictive maintenance.

The use of small form factor one-way data diode technology as a protective filter for edge devices, legacy assets, microgrids or COPs, enables the sharing of operational data and telemetry with third parties, as recommended in the Unified Facilities Criteria UFC 6-010-04, 3-550-04 and NIST SP 800-82 r3.

The data diodes allow data to be transported from a secure network while physically preventing external traffic from passing through the same channel in the opposite direction (optical isolation). This unidirectional data comms capability can also support the readiness monitoring of mission critical COP systems without the threat of unauthorized access.

This technology is currently in use by AFCEC, NAVFAC and the USACE. It is widely used in the intelligence community, nuclear power facilities and energy/manufacturing operations in the United States and Europe.

BIO: Christian Hager is vice president of sales & business development at Fend Inc., a rapidly growing manufacturer of one-way communication diodes, where he heads up the commercial activities (sales and business development) for government and private sector applications.

Preparing Defenders and Defenses in the Age of Cyberwarfare

Lee Rossey, Co-Founder & CTO, SimSpace • lee@simspace.com

ABSTRACT

As cyberwarfare intensifies, defending critical infrastructure and ensuring the readiness of both defenders and defenses has become more urgent than ever. At SimSpace, we understand that the complexity and sophistication of cyberattacks today demand more than traditional training methods and static security controls. To stay ahead of adversaries, organizations must adopt a proactive, continuous approach to threat exposure management, validation and training.

In this session, we will explore how modern-day cyber range technology helps organizations prepare their teams and systems for real-world cyber threats. By leveraging live-fire exercises and high-fidelity simulations that emulate adversary tactics, techniques and procedures (TTPs), cyber ranges enable security teams to train in realistic scenarios. These exercises allow defenders to refine their skills, assess their detection capabilities, and test security stack configurations, ensuring that defenses are not only operational but fully optimized to withstand sophisticated attacks.

The session will also emphasize the importance of continuous validation—testing the readiness of people and technology in a controlled environment before a real attack occurs. Participants will gain insights into how cyber ranges can help improve incident response times, reduce risk, and ensure ongoing preparedness against evolving cyber threats.

BIO: Lee Rossey is the co-founder and chief technology officer at SimSpace, where he leads the development of advanced cyber ranges. With extensive experience at MIT Lincoln Laboratory, Rossey has worked on critical projects involving cyber defense, threat emulation and advanced persistent threat (APT) simulations. His expertise in creating high-fidelity cyber environments has been instrumental in equipping organizations and government agencies with the tools they need to enhance their cybersecurity readiness. Rossey is dedicated to pushing the boundaries of cybersecurity training and building resilient cyber defenses.

The “War Phone”—Eliminating the Signature Management and Active Espionage Risks of Commercial Mobile Devices in Military Operations

Michael Campbell, President and General Manager, Privoro Government Solutions •

michael.campbell@privoro.com

ABSTRACT

Military commanders face a decision for how to equip themselves for the future: stop using the incredible power of the commercial EUD for missions or take accept the risk. Signature management is a growing requirement that should include the signature of the commercial mobile device. Mobile devices—commercial smartphones and tablets — are an increasingly common tool used for everything from infantry squad operations to brigade-level command post operations, but they come with a signature and active espionage risk that must be mitigated.

Lessons learned from recent conflicts indicate the use of commercial mobile devices and mobile technologies will feature more, not less, in and near future areas of conflict. Signature management’s focus has sometimes been more on tactical radios than on the commercial mobile devices increasingly used today.

Today’s reality is less about the old single channel voice radio and more the squelching of commercial smartphone and tablet radios that are designed to reach out and look for the commercial infrastructure they were intended to normally use for communication.

In addition to having a cell radio signature management risk, commercial mobile devices have multiple cameras and microphones. This creates an active espionage risk or the ability to actively record audio and imagery, and the presence of mobile devices near classified matter creates the need for physical controls.

Good news. Solutions exist that mitigate or even eliminate the risks of the commercial mobile device, smartphone or tablet, EUD—allowing full trusted use throughout all phases of operational deployment needs.

BIO: Michael Campbell is based in Washington, D.C., and leads Privoro’s government business. Prior to joining Privoro, Campbell spent almost 10 years with Cisco helping create and run Cisco’s largest government partnerships, first the Army Enterprise Services Agreement and later the Department of Defense Joint Enterprise Level Agreement. Combined, these two agreements represent multi-billion-dollar efforts to better leverage industry expertise to improve communications for U.S. Department of Defense missions globally. Prior to joining

Cisco, Campbell served as an Army officer in Special Operations for 13 years with deployments to more than 20 countries, including Afghanistan and Iraq. Campbell also served as chief of staff for the U.S. Army Chief Information Officer (CIO) and helped author the Army's Global Network Enterprise vision and strategy. He concluded his active military career serving as a military legislative assistant for Sen. Conrad Burns (R-MT). Campbell served as deputy director of instruction and quality assurance officer for Reserve Component Command and General Staff Officers College, until his retirement in 2017. In 2020, Campbell, on behalf of Privoro, was awarded one of eight strategic small business innovation and research awards from the Air Force's innovation cell, AFWERX, to help bring secure mobile solutions to the Air Force and the DoD. He is an entrepreneur who owns two businesses in Washington D.C.'s Capitol Hill. He holds a Master's in public policy from Georgetown University and a Bachelor's in electrical engineering/computer science from Gonzaga University.

Building Next-Gen Secure Remote Capabilities and Enhanced Interoperability with Global Partners

Brian Kovalski, Senior Vice President, Federal, Hypori • brian.kovalski@hypori.com

ABSTRACT

In today's fast-paced digital world, secure military communications and data are crucial, especially for personnel working globally or on temporary duty (TDY). Zero-trust virtual mobility solutions offer the flexibility needed to support Department of Defense (DoD) operations anywhere, anytime.

This session explores how cutting-edge virtual mobility solutions ensure secure collaboration with global allies, protecting sensitive data even when personnel are outside the Continental United States (OCONUS). By processing data in the cloud, security risks, such as device confiscation or reliance on local networks, are minimized.

Mission partner environments (MPEs) allow the military and allies to securely share classified information in real time. As technology advances, building and maintaining MPEs becomes increasingly complex. Virtual mobility solutions play a key role in enabling this interoperability, supporting the DoD's hundreds of mission command applications that must seamlessly collaborate with global partners.

Join us to learn how next-generation MPEs enhance secure data sharing, empowering warfighters to act swiftly and decisively.

BIO: Brian Kovalski has more than 20 years of experience as an information technology and intelligence professional and more than a decade of successful business management experience culminating as the CEO of Ski Systems, Inc. He began his career in the U.S. Army Signal Corps, where he served for 10 years. As part of L-3 STRATIS (now a CACI), Kovalski continued to support military intelligence and Special Forces activities after an honorable discharge. He helped create a highly advanced cyber perimeter protection program for the intelligence community. Brian has held positions from senior engineer, program manager to CEO, and has a proven track record of sustainable growth. Kovalski has a Bachelor of Science degree in information technology from the University of Phoenix.

Data Interoperability for Decision Dominance: Strategies as Executed at U.S. EUCOM and U.S. AFRICOM

Dominic Critchlow, Chief Scientist, Booz Allen Hamilton • critchlow_dominic@bah.com

ABSTRACT

As data becomes a critical asset in modern military operations, achieving decision dominance hinges on seamless data interoperability across complex, multi-domain environments. EUCOM and AFRICOM rely heavily on enterprise data to inform their headquarters and mission systems while also having unique challenges in their respective areas of operation (AOR) that require custom solutions to most effectively integrate data.

At Booz Allen, we leverage our expertise across all Department of Defense and intelligence community organizations and here with a focus on our work supporting U.S. EUCOM and U.S. AFRICOM. We will discuss practical strategies for implementing interoperable enterprise systems. These systems not only drive collaboration across diverse workstreams but also empower action officers to deliver critical, timely information to decision-makers. Our approach emphasizes collaboration and leadership to ensure data can be transformed into actionable intelligence and enhance operational efficiency for strategic outcomes.

BIO: Dominic Critchlow is a chief scientist at Booz Allen Hamilton, focusing on the technical development and implementation of artificial intelligence solutions to government processes. He has been working across all echelons of the Department of Defense, as a civil servant at the Chief Digital and Artificial Intelligence Office, the U.S. Army as an intelligence officer and in the private sector. Critchlow has a background in physics and computer science.

The Path to C2 and an AI-Enabled COP

Nathan Keegan, CTO, Booz Allen Hamilton • Keegan_Nathan@bah.com

ABSTRACT

As the defense community prioritizes enhanced command and control (C2) capabilities, focus is increasingly being placed on the role of artificial intelligence (AI) in providing true situational awareness, facilitate informed decision-making and maintain battlefield advantage. The path to a seamlessly integrated and AI-enabled COP across theaters, however, is obstructed by siloed data processes and fragmented information collection. Booz Allen is leading efforts to address this challenge by facilitating data integration across multiple data platforms, laying the foundation for Strategic Decision Dominance (SDD).

While AI is often seen as the key to real-time decision-making, its true potential relies on robust data engineering and agile governance practices. Before AI can effectively weave together disparate data sources and deliver actionable insights, we must first standardize and harmonize data, breaking down organizational silos and ensuring consistency. Equally important is a flexible governance model that can adapt as the data environment grows, fostering the rapid integration and management of diverse data sources. Only with this foundation can AI serve as the intelligence layer that transforms fragmented common operational pictures (COPs) into cohesive, dynamic and predictive tools.

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 more than 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, kinetic motion capture, and integrated lakehouses.

Before Booz Allen, Keegan worked as a Spanish translator and speechwriter at the Mexican Embassy in Washington, D.C., and as a music teacher at Kosrae High School, where he taught guitar, piano, and ukulele. He has dual Masters in computer science and Latin American studies.

Leveraging the Pentaho DataOps Platform for Enhanced Leadership and Collaboration in C4ISR and Cyber Domains: A Data Analytics Use Case from the Ukraine-Russia Conflict

Pragyansmita Nayak, Chief Data Scientist, Hitachi Vantara Federal •

pragyan.nayak@hitachivantarafederal.com

ABSTRACT

In this era of information-centric warfare, integrating and analyzing vast quantities of data in real time is critical for operational effectiveness. Throughout the war, the Ukrainian military and its allies have had to integrate diverse data sources, from satellite imagery and signals intelligence to social media and cyber threat indicators. The Pentaho platform can streamline these processes by enabling the extraction, transformation and loading (ETL) of data from multiple intelligence streams into a single, unified system. This data is then made accessible for real-time analysis, ensuring that decision-makers at various levels—from tactical commanders to strategic leaders—can collaborate based on accurate and timely information.

For instance, during cyber operations and electronic warfare, the ability to correlate signals intelligence (SIGINT) with cyber threat data can be crucial in identifying and mitigating Russian cyberattacks targeting critical infrastructure or battlefield communications. By bringing together cyber and traditional C4ISR data, military leaders can make more informed decisions, rapidly adjusting strategies and coordinating defensive and offensive operations. The open architecture of the product easily integrates with an existing solution architecture.

This fosters a shared operational picture (SOP), critical for both offensive and defensive operations in hybrid warfare environments like the Ukraine-Russia conflict, where the lines between conventional and cyber warfare are blurred. In conclusion, the Pentaho DataOps Platform is an essential tool for modern warfare, enhancing leadership and collaboration through optimized data integration and analytics. Future applications in defense operations will evolve refining its role in transforming the nature of military leadership and collaboration.

BIO: Pragyansmita Nayak, PhD, is the chief data scientist at Hitachi Vantara Federal (HVF). She explores the “Art to the Science” of solution architectures orchestrating data, APIs, algorithms and applications. She has more than 25 years of experience in software development and data science (analytics, machine learning and deep learning). She has led multiple projects for different federal government agencies (DoD/civilian) in the domain of federal accounting, operational analytics, data mesh, object storage, metadata management, records management and data governance.

She holds a PhD in computational sciences and informatics from George Mason University (GMU) (Fairfax, VA) and Bachelors of Science in computer science from BITS Pilani (India). She has published and presented at numerous AI-focused conferences including WEST, AFCEA TechNet Cyber, NLIT, BrightTalk summits, guest lecture at GMU, George Washington University and National Defense University among others.

For more information on Pragyan’s professional experience, please visit her LinkedIn profile at <https://www.linkedin.com/in/pragyansmita>.

Interoperable Experimentation is Key to Warfighter Readiness Across European Allies

Nick Woodruff, Chief Growth Officer, Research Innovations Inc. •

nwoodruff@researchinnovations.com

ABSTRACT

Experimentation is the lifeblood of progress. For exercise Valiant Shield (VS24), which took place in June 2024, experimentation means the vital acceleration of threat detection and interoperability critical to warfighter readiness.

Exercises such as VS24 allow forces across the Indo-Pacific region the opportunity to integrate multi-domain forces and partner nations to train in various environments that demonstrate the strength and versatility of the joint and combined force. With this year's new inclusion of the U.S. Space Command and U.S. Transportation Command, VS24 achieved data interoperability at a magnitude never seen before.

While the United States invests heavily in state-of-the-art technology, it is wise to urge other European allied nations to refrain from automatically investing in the same technology. One of the most exciting prospects of these experimentations is getting a closer look at smaller nations' independent experimentations. Nations such as the United Kingdom and France do not have as expansive defense budgets as the United States, forcing them to be more agile, fail faster and identify new ways to solve emerging mission challenges. Leveraging allies' unique perspectives and differing solutions can help our defense experimentation and better promote healthy competition and innovation.

In this session, Chief Growth Officer Nick Woodruff will provide a deep dive into the benefits of varying experimentation areas, including enhanced interoperability and competition. Furthermore, he can shed light on the dangers of vendor lock-in and how the DoD can best diversify their partnerships to ensure a robust and adaptable technological ecosystem.

BIO: Nick Woodruff is the chief growth officer of Research Innovations Inc. (RII), charged with the development of partnerships, domestic and internationally, and the leadership of select strategic initiatives in pursuit of global impact. Through his growing network, Woodruff is helping to evolve RII's ability to quickly engage and fundamentally change the decision-making processes of the American and allied defense infrastructures through rapidly developed and fielded technical capabilities. Prior to his tenure at RII, he served in uniform for 14 years in various organizations within U.S. Special Operations Command, including deployments across the globe. The vast majority of his time in Special Operations was spent as a professional in information and unconventional warfare. He holds a degree in business administration and organizational change and has undergone executive leadership training at Stanford, the Uni-

versity of Charleston and Joint Special Operations University.

Serving Defence's Need for Information From a Data Soup

Richard Goodman, EMEA Defence Lead, Hexagon • richard.goodman@hexagon.com

ABSTRACT

There is no shortage of inputs and sources into today's defence ecosystems, from whichever particularly 'INT' you choose. However, these inputs and sources are often not intelligence but are 'data' that needs transforming to information to feed knowledge to help make decisions (and raise more questions). To do this, data needs to be exposed to those defence analysts and systems who will use it, often in conjunction with other data to answer their questions. Data needs to be findable, accessible, interoperable and reusable (FAIR). As NATO adopts the principle of need to share, rather than need know, users should have easier access to data, if they know where and how to look.

This talk will look at aspects to consider when sharing data, in terms of making it FAIR. Working across data meshes and fabrics, or data silos and lakes, a catalogue will need to capture all aspects of data that makes it usable and findable for users. This metadata will include the source, dates, classification, etc. and give the details against which the data can be discovered. Having standards for metadata, as well as for transfer formats of data, access controls, storage and distribution will ease the interoperability of data across domains. Also, we will look at sharing data processing capabilities allowing non experts to analyse and benefit from the data.

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 defence, setting strategy, gaining market recognition within defence agencies and supporting the wider sales team and partners.

Speaking the Same Language: Creating Conditions for MPE Success

James Stanger, Chief Technology Evangelist, CompTIA • jstanger@comptia.org

ABSTRACT

Over the past year, James Stanger has been lucky enough to work closely with IT leaders from the United States, the United Kingdom, Australia, Japan, Thailand and various other countries around the world. Even those who don't use the term, "mission partner environment (MPE)" are deeply engaged in finding better ways for organizations to communicate.

He proposes to discuss how militaries around the world are upskilling their workers to ensure that they speak the same technical language as they cooperate. He will discuss insights about how militaries are transforming signaling tech workers worldwide to focus on enhanced security analytics, monitoring and micro-segmentation. He will further discuss how organizations are borrowing from enterprise and private-industry leaders about modularizing their approach to consider various architectures. These architectures don't specifically involve one approach, such as zero trust. Instead, they focus on the "business" architecture, as well as architectural approaches having to do with application, data, and technology.

If militaries wish to engage in more productive MPE environments, then it's important to avoid getting lost in the technologies. He will discuss ways the most progressive militaries seem to be adopting to put the mission first, and then let the technology fall into place as appropriate. Therefore, workers need unique combinations of soft and technical skills to identify and even proactively avoid toxic combinations that affect MPE and military environments.

BIO: James Stanger, PhD, has consulted with corporations, governments and academic institutions on cybersecurity, emerging technologies, and information technology for more than 25 years. Organizations include Microsoft, Coca-Cola, AWS, Tesco, AstraZeneca, the University of Cambridge, Nissan and the U.S. Department of Defense. Stanger is a working IT professional, as well as an award-winning blogger and educator. He is a member of various advisory councils, including the Forbes Technology Council, the AFCEA International Cyber Committee, and the ATARC Future of Secure Work and Zero Trust committees. As President of the C3, Stanger leads the consortium of leading global cybersecurity certification bodies, which include GIAC, ISC2, ISACA, CompTIA, the IAPP, FITSI, and CertNexus. He is currently CompTIA's chief technology evangelist.

NATO SPS Cube4EnvSec: Federated, Interoperable AI-Cubes for ISR and Tactical Data Availability at Scale

Peter Baumann, Professor | CEO, Constructor University | rasdaman GmbH •

pbaumann@constructor.university

ABSTRACT

Modern ISR as well as tactical missions have to “operate off the same map” and “get the right data at the right time, in the right format.” This poses high challenges as data of substantial variety have to be gathered, homogenized, and distributed in near real time, including static, large scale data centers and moving edge devices as heterogeneous sources and sinks. Further, different players, ranging from human analysts to automated effectors, have different needs.

The Cube4EnvSec project, supported by the NATO Science for Peace and Security (SPS) program, has shown how a combination of space/time datacubes, AI, cloud/edge federation, and interoperability can substantially enhance the information availability for GEOINT, ISR, and the NATO Federated Mission Network (FMN). Finished this October, Cube4EnvSec has generated a series of federated services for the use cases aviation safety and arctic environmental monitoring.

We present the project, its technology and use cases. Under the lead of Constructor University, the project united Germany, Israel, Turkiye, Greenland, and the United States. Through live demos, many of which the audience can recapitulate, we show hands-on how to access, extract, analyze, and reformat data from datacubes. Particular emphasis is on federation and interoperability aspects.

The presenter is Cube4EnvSec PI and editor of the datacube standards in OGC and ISO and member, EOSC.

This research has been supported by NATO SPS, which is gratefully acknowledged.

BIO: Peter Baumann, PhD, is professor of computer science and an entrepreneur. At Constructor University, he researches flexible, scalable datacube services and their application in science and engineering. With the rasdaman engine, he and his team have pioneered datacubes and Array Databases and have set the de-facto standard for datacube services, documented by 200+ scientific publications, international patents and numerous high-ranking innovation awards.

As founder and CEO, he leads the successful international commercialization of rasdaman. For many years, Baumann has been leading datacube standardization in ISO, OGC, and EU INSPIRE.

Baumann is board member, UNGGIM PSN; chair, IEEE GRSS Earth Science Informatics Technical Committee; co-chair, OGC Coverages.SWG and Coverages.DWG and BigData.DWG; German delegate, INSPIRE; editor, ISO 19123 suite.

See details on <https://peter-baumann.org>.

Networking: The Superpower Fueling Success in Technology and Cyber Operations

Seni Aguiar, COO, Digital Charter • seniaguiar@gmail.com

ABSTRACT

In a rapidly evolving world where technology professionals play a pivotal role in shaping the future, the ability to build and nurture relationships has become a superpower that transcends industries and sectors.

Whether you are an engineer, a business leader or an innovator, your network can be the catalyst for achieving professional success. Drawing on over a decade of experience, Seni Aguiar shares how networking has helped secure executive-level positions and navigate complex career paths—without traditional job interviews.

In this session, you'll learn actionable strategies for expanding your network, overcoming common challenges and making lasting connections that go beyond job titles. Discover how networking is not just an asset for personal growth, but a tool to enhance collaboration, spur innovation, and lead technology teams through today's dynamic challenges.

Join Aguiar for an engaging exploration of how staying connected can empower your career in the fast-moving world of technology, defense, and cybersecurity, with key takeaways that apply across all domains—from C4ISR to AI and cyber operations.

BIO: Seni Aguiar is an experienced leader with more than a decade in DevOps serving government and commercial customers.

With a background in strategic development and business operations, Aguiar is the driving force behind Digital Charter (DCIT), where she is the chief operations officer (COO).

WHAT IS AFCEA?

AFCEA is a member-based, nonprofit association for professionals that provides highly sought-after thought leadership, engagement and networking opportunities. We focus on cyber, command, control, communications, computers and intelligence to address national and international security challenges. The association has more than 30,000 individual members, 138 chapters and 1,600 corporate members. For more information, visit afcea.org.

