



TechNet Augusta

August 20–23, 2018 | Augusta Marriott at the Convention Center | Augusta, GA



2018 SOLUTIONS SHOWCASE

AFCEA TechNet Augusta Solutions Reviews

AFCEA International is pleased to host TechNet Augusta to assist the military as it faces the intricate challenges the cyber domain pose. One of these challenges is the theme of the event: Cyber Electromagnetic Activities (CEMA) for Unified Land Operations. CEMA aims to exploit an advantage over enemies in both cyberspace and the electromagnetic spectrum while denying adversaries use of these arenas and protecting the mission command system.

Earlier this year, AFCEA International hosted the 2018 Army Signal Conference. During the presentations, Army leaders described how the service is overhauling its relationship with technology providers to incorporate a new class of capabilities.

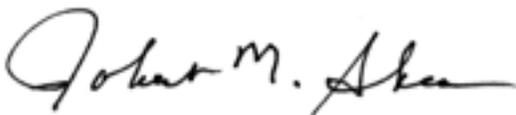
To bring industry into the discussion prior to TechNet Augusta 2018, the service identified the following areas as opportunities for the commercial sector to offer potential solutions for the best ways to achieve this goal. Companies were invited to offer their ideas about:

- **Artificial intelligence** to support the planning, execution and training of offensive and defensive cyberspace operations.
- **Cyberspace modeling and simulation** to support cyber mission planning, proficiency training, cyber situational understanding and exercise support.
- **Advanced analytics** enabling cyber situational understanding with mission context; and planning and offensive/defensive cyber operations.
- **Cyber stealth technology** enabling signature masking/reduction and obfuscation.
- **Tactical communication network** that can transport voice and data through integrated multiple transport paths using automatic routing and reconfiguration.
- **Radios that are spectrum aware and can adapt to different frequency bands** if needed.
- **Range extension to existing radios and other communication equipment** without relying on satellites exclusively.
- **Radios with reduced RF signatures** that are less susceptible to electronic attacks.
- **Electronic warfare systems** capable of conducting simultaneous electronic attack and electronic warfare support from the same platform.
- **Small form factor and ruggedized antennas** and tactical EW systems capable of survival in harsh environments while transmitting and receiving.
- **EW systems that can generate increased power** from both batteries and high-power amplifiers without adding additional weight and size.

AFCEA International received more than 40 potential solutions to some of these problem areas from a range of industry partners and conference participants. The AFCEA Technical Committee reviewed the submissions and evaluated them on criteria such as innovation, potential effectiveness and maturity of solution. It selected several solutions to be presented at the conference in a Solution Reviews format.

All submissions are valuable and offer some innovative approaches to difficult problems. We encourage you take the opportunity to review them.

Sincerely,



Lt.Gen. Robert M. Shea, USMC (Ret.)
President and Chief Executive Officer,
AFCEA International

Problem Statements

Artificial Intelligence

Problem Statement: The Army requires Artificial Intelligence (AI) to support the planning, execution and training of offensive and defensive cyberspace operations.

Why it is important: Army networks and network defenders encounter high volume and velocity of a constantly evolving threat. Threat identification and isolation requires a complex combination of machine learning, AI and human interface to reduce the time to reconfigure, react to an adversary or change techniques and/or tools to support a mission. This would reduce the time gap between human reaction and dynamic threat response and enable autonomous active cyber operations.

Cyberspace Modeling and Simulation (M&S)

Problem Statement: The Army requires cyberspace modeling and simulation (M&S) to support cyber mission planning, proficiency training, cyber situational understanding (SU) and exercise support.

Why it is important: Cyberspace M&S is required for cyberspace mission and support personnel at all levels. For mission planning, it must be intuitive and include a level of artificial intelligence that identifies likely challenges, viable courses of action and potential impacts to mission. For proficiency training and exercises, M&S must be able to emulate an array of realistic mission-specific logical environments. It must include a high fidelity of user activity and system interactions, both commercial and military, and generate realistic traffic. This traffic should include adversary cyberspace effects, anomalous network activity and insider threat. M&S also is necessary for cyber SU to blend seamlessly with mission/maneuver command for the military decision-making process driving the course of action (COA) analysis development. This is a time-dependent requirement for available staff planning and COA validation through modeling and simulation. There are currently ongoing M&S environments being created concurrently at different classification levels. The effects implemented in one conventional warfare scenario on one M&S must be synchronized with a cyber training scenario on another platform. This is an inherent factor to be resolved for persistent cyber training environment in regards to M&S.

Advanced Analytics

Problem Statement: The Army requires advanced analytics enabling cyber situational understanding (SU) with mission context and planning and offensive/defensive cyber operations (OCO/DCO).

Why it is important: Analytics of multi-source, multi-time, large-scale data in unstructured and structured formats will enable operational Army commanders and staffs in planning and execution of unified land objectives (ULO) in the conduct of multi-domain battles. Analytics will enable integrated course of action analysis across all domains fed by local network sensors and data as well as national, joint, coalition and commercial data sources through secure bi-directional cross-domain layers. Such advanced analytics will create alternatives in planning scenarios assisting the military decision-making process and simulating effects/mission impacts for base planning options, branches and sequels.

Cyber Stealth Technology

Problem Statement: The Army requires cyber stealth technology enabling signature masking/reduction and obfuscation.

Why it is important: Force protection of Tactical Cyber Mission Forces (CMF) is required in a peer/near-peer fight in multi-domain battles and to ensure mission success. CMF protection capabilities will enable the CMF to screen/guard against adversary network defenders. CMF capabilities are enhanced with an automated identification of friend/foe that can protect CMF actions in and through cyberspace to counter the cyber threat out front of friendly network boundaries. They will minimize detection; improve low probability of intercept and low probability of detection; and enable deception and masquerade techniques.

Voice and Data Transport Through Multiple Transport Paths

Problem Statement: The Army needs a tactical communication network capable of transporting voice and data through integrated multiple transport paths using automatic routing and reconfiguration.

Why it is important: The Army needs to ensure communications while operating under disconnected, intermittent and limited conditions. The Army's operating environments are becoming increasingly congested and contested with unfriendly RF sources, and it needs to maintain network resiliency in these conditions.

Spectrum Aware and Adaptive Radios

Problem Statement: The Army needs radios that are spectrum aware and can adapt to different frequency bands if needed. Advanced antenna technologies capable of supporting a wide band of spectrum are desired.

Why it is important: The Army's existing radios are challenged by terrain and spectrum efficiency, and there is an increasing threat of electronic attack, which reduces throughput and effectiveness of the radios.

Range Extension for Radios and Communication Equipment

Problem Statement: The Army needs to provide range extension to existing radios and other communication equipment without relying on satellites exclusively. The capability must be expeditionary and must support units moving across the battlefield.

Why it is important: Ground-based radios are severely limited by terrain and atmospheric conditions. Maintaining network fidelity in such environments is a challenge. Satellite-based range extension methods have high costs and do not have sufficient bandwidth to support all users. Additionally, satellites can be easily jammed. Warfighters need the ability to establish range extension at lower echelons without depending on higher HQ.

Radios with Reduced RF Signatures

Problem Statement: The Army needs radios that have reduced RF signatures so they are less susceptible to electronic attacks.

Why it is important: The Army's current radio RF signatures are easily detectable and vulnerable to adversaries' direction-finding and interception efforts. Networked radios also need to constantly beacon to maintain network awareness, creating a significant electronic warfare liability.

Simultaneous Electronic Attack and Electronic Warfare Support

Problem Statement: The Army requires electronic warfare systems that can conduct simultaneous electronic attack and electronic warfare support from the same platform.

Why it is important: EW systems need to be able to continue sensing and collecting electromagnetic emissions while conducting EA missions to maintain direction finding and continue to geolocate the adversary for situational awareness and further targeting.

Small, Ruggedized Antennas and Tactical EW Systems

Problem Statement: The Army requires small form factor and ruggedized antennas and tactical EW systems that can survive in harsh environments while transmitting and receiving.

Why it is important: EW systems need antennas that are as small as possible and can withstand impacts while continuing to fully function.

Light, Small EW Systems With Power-Generating Capabilities

Problem Statement: The Army requires EW systems capable of generating increased power from both batteries and high-power amplifiers without adding to the weight and size. Improved antenna technology, such as directional and beam forming, also would be helpful.

Why it is important: EW systems need to be able to provide increased effects without increasing the size and weight of the systems.

Table of Contents

Highlighted abstracts selected as presenters at conference as of August 14.

Advanced Analytics

Evolving the Modern Enterprise with AI and Machine Learning

Bill Babilon, Public Sector Chief IT Operations Solution Architect, Splunk 10

Dynamic Data Protection

Jack DeGennaro, Senior Cyber Engineer, Forcepoint..... 12

Providing Combatant Commanders with Real-Time Advanced Analytics Against Offensive Adversarial Cyber Tactics, Techniques and Procedures

Jay Grant, Senior Systems Engineer, Federal, Symantec Corporation..... 14

Building CyberSU into SitaWare

Daniel Lacks, Chief Scientist, Cole Engineering Services Inc..... 16

Achieving Instant Situational Awareness in Secure Command and Control Environments

Jillian Little, Vice President, Federal Solutions, Thinklogical, A Belden Brand 18

Avoiding The Artificial Conclusion: Systems and Methods That Obtain Tactical and Strategic Clarity

Chris Mac-Stoker, Distinguished Engineer, NIKSUN..... 20

Cyber Common Operating Picture Solution — MI:COP

Jamie Miller, CEO, Mission Multiplier 21

Take Back Control of Your Security Operations

George Nazarey, Consulting System Engineer, FireEye 23

Operational Analytics for the Warfighter

Andrew Ratzlaff, Business Development Director, i3solutions..... 24

Situational Understanding Through the Machine Data Fabric

Ashok Sankar, Director of Solutions Strategy, Splunk 25

Enterprise Performance Management with AIOps (Advanced Analytics)

Robert Schofield, Senior Solutions Architect, NetCentrics Corporation..... 27

Learning from Today's Tech Giants: Modernized Advanced Analytics at Mission-Scale — Lessons from Industry Disruptors

Brian Shealey, Enterprise Sales Manager - DoD, DataStax 29

Artificial Intelligence

Operational AI for Battlespace Mission Command Allen Badeau, CTO, NCI.....	30
Combat AI with AI to Secure Your Agency Craig Bowman, Vice President, Advanced Solutions, Verizon.....	31
Cyber Cognitive Operator Jacob Cox, Research Scientist, Soar Technology Inc.	32
aiWARE Biney Dhillon, Chief Executive Officer, NexTech Solutions	34
AI and Moving Up the Attack Chain Larry Gloss, Managing Director, BluVector Inc.....	35
Understanding the Cyber Terrain — Network Topology, Endpoint Characterization, Cybersecurity Posture – As the First Step to Active Cyber Defense Dean Hullings, Senior Solutions Strategist, ForeScout Technologies Inc.....	36
Automated Secure and Optimal Cyber Configurations Using SOCCER William Liu, Technical Director, LGS Innovations	37
Automated and Scalable Sensitive Document Classification Malek Ben Salem, Senior R&D Manager, Accenture.....	39
Implementing Self-Healing, Self-Defending AI Systems Nicola Whiting, CSO, Titania Ltd.....	40
Portable Fiber Optics on the Battlefield Larry Widgeon, Ground Tactical Product SME, KITCO Fiber Optics	42
AI and Machine Learning Jeff Winterich, DoD Account Chief Technologist, Hewlett Packard Enterprise.....	43

Cyber Modeling and Simulation

In Depth Security From a Hacker's Point of View

Craig Bowman, Vice President, Advanced Solutions, Verizon..... 44

Cyber Integration with Warfighter Training Platforms

Kevin Hofstra, Chief Technology Officer, Metova CyberCENTS 45

High Fidelity Modeling and Simulation for Commercial Mobile Networks and Mobile Apps Using an Innovative Live, Virtual and Constructive (LVC) Testbed

Steven Kropac, Chief Technology Officer - Cyber, LGS Innovations 47

CyberSAF Simulator

Daniel Lacks, Chief Scientist, Cole Engineering Services Inc..... 49

Cyber Stealth Technology

Muddler

Accenture Federal Services Adversary Research and Recon Team,
AFS ARRT, Accenture Federal Services..... 51

On-Demand, Secure and Traceless Cloud Networks

Jason Crowley, Business Development, Dexter Edward 52

Establishment of Secure Networks on Untrusted or Hostile Infrastructure

Jonathan Roy, Principal Security Architect, Unisys Corporation 54

Operation Pigtail

Larry Widgeon, National Sales and Marketing Manager, KITCO Fiber Optics..... 56

Increased Power Without Increasing Weight and Size

SWaP Improvements in RF High Power Amplifiers

Steve Richeson, Vice President, Sales and Marketing, Mission Microwave..... 57

Multi-Path Transport

Unified Heterogeneous Network (HetNet) Transport Denis Couillard, Director, Government Strategy, Ultra Electronics TCS	58
The NTS Tactical Edge Biney Dhillon, Chief Executive Officer, NexTech Solutions	59
Do You Want Good Network Resiliency Today or to Wait for Unknown Routing Tomorrow? COTS Multipath Is Here Today David Howgill, President, Huckworthy	60
Increase Integrated Resilience at the Tactical Edge with Software-Defined WAN (SD-WAN) Martin Isaksen, Senior Architect, Cisco	61
Core Level Security Extended to the Tactical Edge SafeNet AT	62
Network Automation — Rapid Response to Enterprise Threats Chuck Swan, Solutions Architect, Force 3	63
Enabling IoT at the Edge Jeff Winterich, DoD Account Chief Technologist, Hewlett Packard Enterprise.....	64

RF Signature

A “Future Tactical Waveform” (FTW) Process for Accurate Position, Navigation and Timing Timothy Allen, Senior Principal Software Engineer, CERDEC S&TCD	65
Adaptive and Efficient Frequency Band Reuse for Reduced RF Signatures Ronald Connelly, Program Manager, Alion Science and Technology.....	66

Spectrum Awareness and Agility

Multilayer Network Diversity and Adaptation Denis Couillard, Director, Government Strategy, Ultra Electronics TCS	68
Leveraging COTS Wireless for Secure Spectrum Agile Multipath Communications Today David Howgill, President, Huckworthy	70

Evolving the Modern Enterprise With AI and Machine Learning

Bill Babilon, Public Sector Chief IT Operations Solution Architect, Splunk •

bbabilon@splunk.com

ABSTRACT

Splunk is the foundation for an organization's machine data fabric. Thousands of customers are using Splunk across a wide variety of use cases, including cybersecurity, IT operations, SCADA/ICS, Internet of Things (IoT) and business analytics. Splunk natively and reliably collects, indexes, prepares and stores data from tens of thousands of sources, including network traffic or wire data, firewalls, intrusion detection and prevention systems, web and application servers, custom applications, hypervisors, GPS systems, social media, sensors and preexisting structured databases in real time. This includes any ASCII text-based data from any location with no predefined schema, enabling the collection and indexing of petabytes of information.

Splunk has a full complement of data ingest wizards and technology add-ons that can help further reduce the time to integrate additional, more exotic, novel or Army-specific data streams. Splunk was designed to make it easy for the platform to integrate with other commercial and open source tools. With its strong focus on research and development, it continues to provide support for emerging technologies.

As agencies look to improve their IT operations, resource and budget constraints are increasingly turning them toward automation. The anticipated benefits of modernization—the ability to adapt rapidly to meet citizen expectations, performance requirements and security—cannot be fully realized using old-school IT management tools and tactics. “Automation is a critical tool to maintain agility in system design and to make the best use of finite human resources,” according to the Report on Federal IT Modernization.

Automation begins with data—specifically, the machine data generated by the constellation of hardware, software and management tools that make up the existing IT infrastructure and services, as well as the new devices and technologies that are ushering in digital transformation. By automating repetitive tasks and employing innovative machine learning and artificial intelligence techniques, agencies not only can overcome resource challenges but also gain new insights that can help them achieve better outcomes, drive agency efficiencies and enhance security posture.

As agencies begin to explore innovative ways to transform themselves and deliver services, they are increasingly turning to data-driven decision-making strategies. But the variety, volume and velocity of data can be daunting, including harnessing them to derive intelligence to solve problems—be it a security threat, performance issues or possible service outages.

AI and machine learning are helping agencies rethink their approach and look beyond their resource constraints to advance their mission outcomes.

BIO: Bill Babilon leads Splunk's U.S. public sector practice for IT operational analytics as the chief IT operations solution architect. He has been a consumer of Splunk Enterprise since 2010 as a systems integrator and consultant to the U.S. federal government. Babilon has more than 25 years of expertise in application development, IT operations and enterprise architecture. He works with customers across the commercial, federal civilian, defense and intelligence communities in the areas of information technology, operations and machine learning. He has a BS in aerospace engineering from the University of Virginia and an MS in software engineering from George Mason University.

Dynamic Data Protection

Jack DeGennaro, Senior Cyber Engineer, Forcepoint • jdegennaro@forcepoint.com

ABSTRACT

Data protection can halt a security organization and productive work. As indicated in the 2018 Verizon Data Breach Investigation Report, 68 percent of data breaches take months to discover. Learning about a breach after the fact does not prevent an event from occurring. The same report revealed 73 percent of cyber attacks occur with lost or stolen credentials. Bad actors can come from anywhere—it's not just malicious insiders organizations need to watch out for to protect data and personnel. According to a 2017 Ponemon Institute study, companies experienced between 2,600 and 10,000 records containing sensitive and/or confidential information had been compromised per breach. This resulted in an average data breach cost of \$3.62 million per incident.

Security analysts are sick of managing exceptions that can create holes in security defenses. Unbalanced strategies with over-restrictive policies cause headaches and roadblocks to mission success while under-restrictive policies leave an organization exposed from all sides.

Today, IT security protects data in different ways, using a variety of different tools. These tools are designed to do the same thing: stop data exfiltration. However, none of them is really all that effective because they are static, threat-centric policies that either block or allow access to data. That was acceptable when everyone worked within a perimeter.

However, today people access data from just about anywhere; cloud applications enable a boost in productivity. For example, a user tries to save a presentation file to a flash drive. When threat-centric solutions see this activity, they are not sure if it's good or bad and are forced to block the action to protect the data. There is no insight into the broader context. The result is a disproportionate number of flagged activities, which overwhelms security teams who have no way to understand the activities most worthy of investigation. Legitimate threats are more hidden and can more easily infiltrate the enterprise.

An effective data security solution should cut through the noise of alerts and provide early warning signals to prevent the loss of important data. It is one that truly understands how users interact with data and where it lives.

Dynamic data protection vigorously applies monitoring and enforcement controls that adapt to changes in human behavior. Powered by a behavior-centric analytics engine, dynamic data protection correlates data to compile a risk score for each user in the organization. Risk levels are driven up and down by human behavior. Changes in risk levels drive different outcomes such as allowing, auditing or blocking. All outcomes

should be able to be customized or tuned to an organization's unique needs. Dynamic data protection can customize these responses at an organizational, group or individual user level, resulting in automated policy enforcement in near-real time based on the nuances of individuals' behavior and the context of their activity.

Dynamic data protection helps organizations now, which results in triaging fewer alarms, reducing investigation time, reducing dwell time and deterring data loss events.

BIO: Jack DeGennaro is a senior cyber engineer at Forcepoint. After attending Clemson University, DeGennaro began a career in law enforcement with the City of Clemson Police Department. Over the next 15 years, he was detailed with a variety of assignments, which included working undercover for seven years. During that time, DeGennaro worked within the leadership for six years, including management of the department's IT network, criminal investigations, jail operations and police records management.

DeGennaro also worked for a computer mapping firm to provide automated vehicle location services for public safety. In 2008, he joined Visual Analytics and was assigned to the architecture, deployment and management of the company's data sharing and crime analysis tools at 14 crime analysis centers within New York state.

Upon Raytheon Cyber Products' acquisition of Visual Analytics and the subsequent joint venture to become Forcepoint, DeGennaro moved out of the services group and currently serves as a solutions architect supporting the U.S. Defense Department in insider threat and analytics.

Providing Combatant Commanders With Real-Time Advanced Analytics Against Offensive Adversarial Cyber Tactics, Techniques and Procedures

Jay Grant, Senior Systems Engineer, Federal, Symantec Corporation •

jay_grant@symantec.com

ABSTRACT

In addition to hostile enemy fire from kinetic weapons system platforms, future U.S. Defense Department battlefield engagements will include aggressive, well-coordinated, mature, cascading cyber attacks from advanced nation-state adversaries. These technically competent enemy combatants will attempt to deny, destroy or disrupt U.S. military IT systems across the full spectrum of operations. Therefore, a critical component to further along U.S. cyber defenses will be to develop a marked increase in the nation's ability to conduct advanced analytics against offensive adversarial cyber tactics, techniques and procedures. To do so, Symantec Security Analytics can provide the Defense Department with an automated capability that captures, indexes, classifies and enriches all network traffic, including full packets. For the department, Symantec Security Analytics can consistently and accurately enable full retrospective analysis and provide combatant commanders with real-time situational awareness that is presented via clear, concise, actionable intelligence about cyber threats to warfighter applications, mission data and data-in-motion content via:

Layer 2 through 7 Advanced Analytics: Symantec Security Analytics provides a variety of analytics tools such as complete session reconstruction, data visualization, Root Cause Explorer, timeline analysis, file and object reconstruction, IP geolocation, trend analysis and anomaly detection.

Tight Integration Across Existing and Future Deployed Cybersecurity Infrastructure: Symantec Security Analytics integrates tightly with best-of-breed security technologies (Symantec as well as non-Symantec tools), including security information and event management (SIEM) systems, next-generation firewalls (NGFW), intrusion prevention devices (IPD), malware sandboxing and endpoint forensics that can immensely assist the Defense Department in leveraging its existing security investments and improve the effectiveness of established department cyber defense processes.

Context-Aware Security: Symantec Security Analytics provides rich context for all security alerts, thus providing the Defense Department with the details of what happened before, during and after an attack. The department will then be able to pivot directly from any alert or log in and obtain the full-payload details to support quick incident resolution and ongoing forensics activities.

Symantec Security Analytics can provide the Defense Department with the deep insights necessary to understand the context of security events across even the most extreme operating environments so cyber defenders can quickly contain and remediate the full extent of a security incident and support post-event forensics activities.

Architecturally, Symantec Security Analytics data is stored in an optimized file system for rapid analysis, instant retrieval and complete reconstruction that can support all Defense Department incident response activities. Symantec Security Analytics can be deployed anywhere in the network: at the perimeter, in the core, in a 10 GbE backbone or at a remote link in theater to deliver clear, actionable intelligence for swift incident response and resolution and real-time network forensics.

In short, Symantec Security Analytics can provide U.S. cyber defenders with an ability to quickly contain and remediate the full extent of a security incident as well as support post-event forensics activities. The high-performance analytics, massive scalability and centralized management capabilities of Symantec Security Analytics can provide the Defense Department with a dominant cyber position for mission success at the tactical edge and concomitant technical systems combat survivability.

BIO: Jay Grant has more than 15 years of systems security engineering and technical program management experience across the full spectrum of U.S. Defense Department cybersecurity operations.

Building CyberSU into SitaWare

Daniel Lacks, Chief Scientist, Cole Engineering Services Inc. •

daniel.lacks@cesicorp.com

ABSTRACT

The Army requires advanced analytics enabling cyber situational understanding (CyberSU) with mission context; and planning and offensive/defensive cyber operations. Currently, the Army is developing the SitaWare Mission Command system to replace legacy systems with a focus on providing command and control capability for conventional warfare. SitaWare is built with an open architecture that allows other developers to extend its capabilities.

For example, Cole Engineering Services Inc. has built a prototype course of action (COA) analysis SitaWare plugin that embeds OneSAF and Marine Air-Ground Task Force Tactical Warfare Simulation into the mission command stack. This hides the details of the simulation from the commander and enables him to seamlessly import his existing SitaWare plans, equipment and scenarios for expedient cloud-based COA analysis aiding the commander with a variety of information, charts and graphs.

CyberSU may support any echelon that SitaWare supports, but it is envisioned to operate mainly at the brigade, battalion and company levels by military commanders and their staffs. CyberSU will be employed to support the displaying of simulated or operational cyber effects to military commanders to plan COAs, assess the real-time progress of a mission or calculate battle damage assessment. The cloud-based approach to developing SitaWare will assist the military decision-making process and simulating effects/mission impacts for base planning options, branches and sequels because multiple simultaneous simulations may be executed.

This presentation explores building CyberSU as a SitaWare plug-in designed to visualize analytics in a manner that is understandable by military commanders who operate both inside and outside the cyber domain. CyberSU will reside within SitaWare on the mission command server stack and leverage any communications infrastructure available. CyberSU will be able to leverage the rich capabilities and information in real-world databases providing multisource, multitime, large scale data in unstructured and structured formats for unified land objectives defined when conducting a multidomain battle. By integrating into the SitaWare platform, CyberSU will be available on future mission command server stacks deployed worldwide. SitaWare currently is used by 40 nations, which will give CyberSU the potential for exposure to coalition forces should the capability expand for international releasability.

While the CyberSU capability is not yet developed, examples of the existing COA analysis plugin are built to present the look and feel of CyberSU integrated into SitaWare. Cyber capabilities may be built using this similar approach

across all domains fed by local network sensors and data and national, joint, coalition and commercial data sources through secure bidirectional cross-domain layers.

BIO: Dr. Daniel Lacks is the chief scientist at Cole Engineering Services Inc. (CESI). He received a Bachelor of Science degree in computer engineering in 2001, Master of Science degree in 2002 and a doctorate in 2007 from the University of Central Florida specializing in distributed computing, software simulation and software engineering. Since 2001, Lacks has worked as a software and systems engineer in the U.S. Defense Department modeling and simulation industry on live, virtual and constructive programs including Warfighter's Simulation (WARSIM) and the One Semi-Automated Forces (OneSAF) Integration and Interoperability Support (I2S) program. He briefed the results of a prototype for embedding OneSAF and the Marine Air-Ground Task Force Tactical Warfare Simulation into SitaWare the mission command stack to provide artificial intelligence that identifies likely challenges, viable COAs and potential mission impacts at ITEC 2018.

Achieving Instant Situational Awareness in Secure Command and Control Environments

Jillian Little, Vice President, Federal Solutions, Thinklogical, A Belden Brand •

jillian.little@thinklogical.com

ABSTRACT

The proliferation of intelligence, surveillance and reconnaissance (ISR) information is radically changing the landscape of the military and intelligence community. Countries are now following a strategy of information superiority to defend against a broad range of threats, whether they be asymmetrical, nuclear or mass armies. A Herculean effort has been directed at collecting data through satellites and unmanned vehicles as well as monitoring social media and other information sources.

The processing and analysis of this information mostly happens in a secure command and control operations center, often with joint and multinational forces working together. The number and size of these centers is growing exponentially throughout the world. The current focus of the people who design and operate these command centers is instant situational awareness, that is, “How can I use the ISR information sources available to me to give me a full and instant picture of the situation?”

Typical mainstream IT and AV technologies are not designed for these types of applications and are not efficient in delivering multiple sources of information of multiple classifications. Organizations would need to invest in, maintain and manage several separate and parallel data infrastructures—one system for each classification—to attain this capability.

A next-generation command and control infrastructure solution simplifies this multiclassification architecture and allows these defense and intelligence organizations to streamline their IT needs. It provides the ability to quickly share information among teams and be more flexible to address rapidly changing mission requirements.

The solution addresses how to:

- Achieve information superiority and instant situational awareness through and immediate access to critical video and data resources via any-to-any switching
- Simplify management of multiple classifications of information through a single information assurance approved secure infrastructure
- Increase the cybersecurity profile of command and control facilities while mitigating the threat of intentional or accidental breach, hack or data loss by insiders
- Future-proof video, audio and computer signal distribution system to support advances in technology, including 4K resolution and HDR

- Enable flexible and rapid reconfiguration of command and control resources to quickly adapt to dynamic mission requirements
- Reduce up-front IT and AV infrastructure expense while lowering long-term total cost of ownership

BIO: Jillian Little is vice president of U.S. Federal Solutions for Thinklogical. Based in Virginia, Little brings more than 25 years of experience helping government and defense organizations leverage innovative technology solutions to achieve complex mission requirements.

Avoiding the Artificial Conclusion: Systems and Methods That Obtain Tactical and Strategic Clarity

Chris Mac-Stoker, Distinguished Engineer, NIKSUN • szhang@niksun.com

ABSTRACT

Cyber battlespaces can contain chaos and entropy in which are nuggets of information that only become valuable once cross-correlated across multiple technical domains, environments and, retrospectively, in time to produce a near-real-time result. Insight, clarity and appropriate levels of confidence come when multiple data sources begin to point to a similar conclusion. But how can this be done quickly across disparate theaters and mixes of different data types? The strategic and tactical danger of the artificial conclusion in which the most readily available data sources and/or too few data sources drive the military decision-making process (MDMP), producing sub-par results, can be resolved with the correct architecture. Executing an architecture of “process upon entry” that decentralizes data processing yet pools and correlates AI plus user queries enables live forensics, automated conclusions and strategic views simultaneously. Retaining sensitivity to resource usage concerns, such as bandwidth, network performance and application performance in the same footprint, lends the battlefield commander a complete picture not only of the intelligence needed for the MDMP but also predictions and measurements of what is required to reliably keep producing that result from the systems that generate it. This approach explores an executed architecture coupled with a practical exercise and past incident examples.

BIO: As the distinguished engineer, Chris “Skip” Mac-Stoker steers the technical direction of NIKSUN’s product portfolio. Prior to joining NIKSUN, Mac-Stoker was a consulting design engineer for trading infrastructures with specializations in high-availability data integrity/security issues and multidiscipline failure analysis. He brings his technical expertise to NIKSUN stemming from more than 20 years of industry experience in large-scale networking, incident response/ analytics and the high-performance infrastructure and supercomputing sectors.

Cyber Common Operating Picture Solution — MI:COP

Jamie Miller, CEO, Mission Multiplier • jmiller@missionmultiplier.com

ABSTRACT

Achieving a cyber common operating picture (COP) is an innovative, cost-effective solution to provide continuous monitoring and risk scoring and to achieve real-time security monitoring of cyber threats and vulnerabilities. Mission Innovate's COP solution (MI:COP) is founded upon mapping secure content automated protocol (SCAP) enumerations to select NIST 800-53 controls and custom cyber key effectiveness measures and designing a control database/warehouse that interfaces with a dynamic executive dashboard that reports results based on an agreed risk scoring logic. The company's approach is informed by lessons learned and best practices from its current work developing and deploying a custom solution and risk-scoring dashboard for NASA Marshall and currently being used on premises in the NASA environment.

The capabilities of the solution include the integration of real-time/automated data feeds into a database/warehouse and development of a draft risk scoring dashboard to assess risk across the numerous cyber domains, including vulnerability management, asset management (hardware/software), threat management, configuration management and incident management. Definition of key effectiveness measures drive the data needed to be collected from the existing/future tools and ultimately inform the structure of the database and dashboard that the company designs/updates. The normalization of data allows the firm to further score the data based on custom algorithms in near-real time based upon the cadence of scans to incentivize behavioral change of key stakeholders at different tiers of the organization to focus on mitigating the highest risks first. The result is that stakeholders have access to accurate, current and actionable data enterprisewide to make more informed and cost-effective risk management decisions.

BIO: Jamie Miller is the president and CEO of Mission Multiplier, a Huntsville-based, HUB-Zone-certified small business and U.S. Defense Department-recognized asset at the forefront of cybersecurity and information assurance innovation. Mission Multiplier is formally sponsored by the Missile Defense Agency as part of its Mentor-Protégé program and was recently nominated for the 2017 Small Business of the Year in the government contracting/professional services category.

Miller possesses more than 18 years experience and is a proven thought leader that has developed innovative approaches and methodologies to solve problems in the areas of cybersecurity assessment; governance; engineering; operations; critical infrastructure protection; data analytics; and continuous monitoring. His innovative cyber solutions, including ISSO-as-a-Service, MARS Box and MI:COP, are changing the game for how organizations make more informed and effective risk management decisions at a reduced cost.

Miller received the 2016 Emerging Entrepreneur of the Year Award by Innovate Huntsville and was nominated for the prestigious Russell G. Brown Award by the Huntsville Chamber in 2017. Most recently, he was a finalist as Entrepreneur of the Year as part of the 2018 Economic Development Partnership of Alabama imerge Innovation Awards. He is a regular speaker at information security industry leading conferences and has published several industry articles, most recently writing about shared risk for *Security* magazine.

Miller serves on the board of directors for Cyber Huntsville, a Tennessee Valley Initiative; CyberReach; and the Southeastern Cyber Security Foundation. He also serves as the National Cyber Summit Program co-chair. Miller holds an MBA in consulting from Thunderbird School of Global Management and a BA in international studies from American University.

Take Back Control of Your Security Operations

George Nazarey, Consulting System Engineer, FireEye • george.nazarey@fireeye.com

ABSTRACT

Cybersecurity has never been more challenging. Almost daily, new threats expose companies' vulnerabilities, forcing them to purchase more products and hire more talent. Such reactive approaches lead to escalating complexity—yet another vulnerability attackers can exploit. Security operations—big or small—require a holistic, foundational approach.

FireEye Helix helps organizations build that foundation. FireEye Helix is a security operations platform that makes it simple to deliver advanced security to any organization. It reveals unseen threats and empowers expert decisions with frontline intelligence to take back control of an organization's defenses and capture the untapped potential of its security investments. Available with any FireEye solution, FireEye Helix works as a seamless and scalable foundation to connect and enhance all security solutions, including non-FireEye products. Designed by security experts for security experts, it empowers security teams to efficiently conduct primary functions, such as alert management, search, analysis, investigations and reporting.

BIO: George Nazarey is a 2000 graduate from Youngstown State University with a Bachelor of Science in computer science. He started in the information technology field in 1995 while working at a local Internet service provider. He has worked for various companies ranging from small start-ups to *Fortune* 100 firms. He has been specializing in computer security for more than 20 years.

After graduation, Nazarey started working for Alabanza Hosting. He was in charge of more than 250,000 IP addresses and 1,000 servers. His tasks ranged from simple CGI fixes to re-architecting the IP distribution and network layout.

He then worked as a contract employee for the U.S. Department of Transportation. In this role, he was in charge of its email architecture. He re-architected the email infrastructure from a hub-and-spoke design per department to a centralized policy-based architecture.

While working at IronPort Systems, Nazarey architected, installed and optimized three of the top five largest deals in the company's history. These installations ranged from 750,000 to 4.5 million mailboxes.

When Cisco Systems purchased IronPort, Nazarey was the security consulting system engineer for the U.S. Navy and Marine Corps. During the four years with Cisco, he received the System Engineer of the Quarter Award twice for architecting the centralization of the U.S. Defense Department email and Navy 802.11x implementation.

At FireEye, Nazarey's responsibilities include both the Defense Department and Intel Community, specializing in the U.S. Army and Air Force. During his first year, he architected and installed the largest EX deal in the company's history.

Operational Analytics for the Warfighter

Andrew Ratzlaff, Business Development Director, i3solutions • andrew.ratzlaff@i3solutions.com

ABSTRACT

The Joint Collaboration Information Platform (JCIP) solution is a modular and highly customizable data fusion platform that can be used for many use cases, including visualization of the common operating picture or common intelligence picture. JCIP seeks to provide a rich analytics environment optimized for joint collaboration and effective for all echelons, from the tactical edge to the strategic core.

JCIP blends cognitive computing tools with advanced analytics and automated workflow capabilities to help enhance, scale and accelerate human expertise. By integrating distinctive capabilities and technologies into a single pane of glass, JCIP enables mission leaders, analysts and operators to have a holistic view of their environment.

Situational Understanding Through the Machine Data Fabric

Ashok Sankar, Director of Solutions Strategy, Splunk •

asankar@splunk.com

ABSTRACT

Splunk is the foundation for an organization's machine data fabric. Thousands of customers are using Splunk across a wide variety of use cases, including cybersecurity, IT operations, SCADA/ICS, Internet of Things and business analytics. Splunk natively and reliably collects, indexes, prepares and stores data from tens of thousands of sources, including network traffic or wire data, firewalls, intrusion detection and prevention systems, web and application servers, custom applications, hypervisors, GPS systems, social media, sensors and pre-existing structured databases in real time. This includes any ASCII text-based data from any location with no predefined schema, enabling the collection and indexing of petabytes of information.

Splunk has a full complement of data ingest wizards and technology add-ons that can help further reduce the time to integrate additional, more exotic, novel or Army-specific data streams. Splunk was designed to make it easy for the platform to integrate with other commercial and open source tools. With its strong focus on research and development, it continues to provide support for emerging technologies.

In today's cyberspace, corporations and the federal government alike face the challenge of securing key cyber terrain from cyberspace adversaries such as nation-state hackers, hacktivists, organized crime hackers, terrorist hackers and insiders.

It is not news that the threat environment is getting more complex. Not only are there external threats from very determined and sophisticated attackers such as nation states, cyber criminals and hacktivists but also insider threats are rising. When it comes to breaches, the new mantra is "It is not a matter of if but when." As smart devices proliferate local communities, cities and states as part the digital transformation journey, the attack surface grows, giving adversaries a larger target.

Agency systems acquired over decades are in silos managed by teams that don't necessarily interact with each other, so cyber analyst teams don't have full visibility across the organization, making it very difficult to identify and investigate threats. It can take them weeks if not months and is a very lethargic process, leading to significant costs without realizing comparable gains. Combined with an increased drive to hire additional resources, this has led to an unsustainable spending outlook with evidence lacking on enhanced security posture.

The alternative approach is a holistic solution that employs a flexible data analytics platform focused on time-series data and fast, flexible correlation searches coupled with curated machine learning techniques. This solution must be flexible enough to ingest and pivot across structured, semi-structured and unstructured data, while leveraging industry best practices to visualize, report and alert on non-compliant systems to reduce the vulnerability landscape and identify known threats. Furthermore, the solution must support curated machine learning techniques centered around unbiased treatment of anomalies to minimize event generation, reduce false positives and ascertain unknown hidden threats.

The new threats on the landscape require a fundamental shift in strategies to combat them and aid planners with cyber situational understanding.

BIO: Ashok Sankar is the director of solutions strategy focused on public sector and education markets at Splunk. In this role, he is responsible for evangelism of the company's solutions portfolio, leading thought leadership and strategic initiatives, customer engagements and content marketing strategies for the company's portfolio of data analytics solutions. He brings expertise across analytics, security, mobile, cloud and virtualization technologies and their applications in public sector and commercial industries. He holds a master's in electrical engineering from Virginia Tech and a certificate in cybersecurity strategy from Georgetown University.

Enterprise Performance Management With AIOps

Robert Schofield, Senior Solutions Architect, NetCentrics Corporation •

rschofield@netcentrics.com

ABSTRACT

Government organizations' Security Operations Centers (SOC) and Network Operations Centers (NOC) teams are drowning in tools—perhaps dozens, even hundreds—that are designed to monitor various systems, applications and other parts of the IT enterprise environment. However, these tools often fail to talk to each other to share key data in the interest of better predicting, correlating and resolving events such as cyber threats and service disruptions, events that result in data loss, user experience issues, productivity breakdowns and the failure to perform needed day-to-day tasks and/or meet long-term, strategic mission objectives. Subsequently, federal agencies employ scores of SOC/NOC specialists who stay within their silos, focused strictly on their own, individual monitoring solutions with no cross-correlating and analysis of the data produced by the tools instead of developing processes that incorporate automation, machine learning and analytics to maximize the predictive value of the tools as a collective whole to gain enterprise-wide IT visibility.

NetCentrics believes AIOps is all about enterprise performance management such as monitoring, analyzing and instantly acting on data via end-to-end situational awareness and absolute command and control of network resources. It is about establishing a single pane of glass view of the entire infrastructure so data from every tool is ingested, correlated and analyzed to generate quantitative outputs that tell how to improve. It is about launching advanced automation, machine learning and analytics that inform proactive event management while reducing response times to protect networks, systems and devices while ensuring optimal user experiences. It is about acquiring a true understanding of potential cyber attacks, help desk ticket spikes and other SOC/NOC events, so teams and machines do more than just identify root causes, they resolve events proactively.

The machine element cannot be understated. As AI innovation takes hold throughout organizations worldwide, dramatically expanding capabilities to accurately and swiftly detect incidents then respond, agencies cannot be left behind. Ultimately, NetCentrics AIOps elevates monitoring and data correlation/analytics to a level at which events are treated one in the same: Whether there is an influx of service desk tickets, an isolated incident, a service affecting an enterprise, or a critical business application that appears degraded, NetCentrics' AIOps drives toward the core using root cause analysis and actionable intelligence that tells teams what action to take based on lessons learned, mature processes and recommendations through AIOps in its entirety. Using machine learning and automation to the maximum extent practicable, the company can address an event without involving human interaction and resolve potential events before they become actual events. Its AIOps services and solutions will increasingly enable machines to make these decisions and take appropriate action, further reducing IT staffing costs for agencies.

BIO: Robert Schofield is a senior solutions architect with a BS in information technology and an MS in information systems. He has more than 15 technical certifications, including Microsoft, VMware products and ITILv3. He has 20 years experience supporting the U.S. Defense Department at an enterprise level, including eight years active duty in the armed forces. He was the technical program manager supporting several customers, including the U.S. Army NETCOM, JSP, CIA, DIA and OSD. Schofield has an active security clearance and has worked for NetCentrics Corporation since 2007, most recently supporting the management of its worldwide deployments of Enterprise Management (Microsoft System Center) capabilities to the U.S. Coast Guard.

Learning From Today's Tech Giants: Modernized Advanced Analytics at Mission- Scale — Lessons From Industry Disruptors

Brian Shealey, Enterprise Sales Manager, DoD, DataStax •

brian.shealey@datastax.com

ABSTRACT

To ensure the tactical advantage in theater during operations, a modernized approach focused on real-time, mission-oriented analytics needs to be employed in an architectural model that scales and performs with the needs of today's Army.

In today's systems, data often does not reside in a single place. The current push to allow for cloud-based computing functionality throughout the U.S. Defense Department presents an incredible opportunity to change the landscape of mission-based analytics to drive AI, machine learning and predictive modeling in ways never before seen. A big lesson can be derived from today's leading cloud application companies in understanding how to produce modernized application architectures that deliver real-time analytics across a wide variety of use cases in geodistributed business models.

The performance, flexibility and scale they have achieved with their analytics-focused applications have allowed them to disrupt industries and change the world.

This solution addresses the questions:

What can be learned from industry and how can the Defense Department (Army) take advantage of these architectures to create advanced analytics solutions?

- How are industrial IoT platforms similar to the system-of-systems architecture related to command/control and ISR systems like DCGS-A?
- How does combining multimodel analytic capabilities scale and perform across geodistributed mission environments?
- How do you build for scalability and performance in a way that matches the Army's move toward dynamic force structure successfully?

The solution touches on open technologies and ways to modernize using integrated platforms that cover Apache Spark-based analytics and search-and-graph analytics that work for companies such as Sony, Netflix and others.

BIO: Brian Shealey runs the U.S. Defense Department business for DataStax. He has extensive experience in delivering emerging technology to programs across the department with a focus on technology modernization.

Operational AI for Battlespace Mission Command

Allen Badeau, CTO, NCI • abadeau@nciinc.com

ABSTRACT

C6ISR systems are creating exponentially increasing amounts of data; however, less than 5 percent of that data is currently being leveraged for decisions within the battlespace. The current status of the suite of mission command information systems is effective at collecting, storing and displaying operational information. These capabilities are limited by their suite's inability to provide military leadership with a shared understanding of the environment by processing and turning data into knowledge automatically. To accelerate decision-making by commanders and their staffs, NCI operationalizes artificial intelligence techniques using its Scaling Humans with AI (Shai) tactical platform.

The Shai solution is capable of ingesting various types of data residing in multiple, highly distributed U.S. Defense Department environments, platforms and sensors. It provides that missing capability, which is needed to overcome limitations and improve situational awareness, especially as the number of sensors and amount of data collected continues to grow and outpace human capabilities, bandwidth and stamina. Shai can overcome these limitations by innovatively logging into each of the C6ISR systems as a human, carefully watching and learning the battlespace and providing domain knowledge, insights and intelligence fusion information to warfighters during the conduct of operations. Using benchmarks from other Shai programs, NCI expects a twentyfold improvement as compared to a human's measured ability to create actionable intelligence and produce operational information.

BIO: Dr. Allen Badeau is the chief technology officer for NCI and the director of the NCI Center for Rapid Engineering and Agile Technology Exchange (NCI CREATE) Innovation Incubator. With a 20-year history of providing innovative RDT&E solutions to the U.S. Defense Department, he is leading a team of scientists and engineers who are providing digital transformation solutions in the areas of artificial intelligence, C6ISR and the Intelligent Internet of Things (I2OT).

Combat AI with AI to Secure Your Agency

Craig Bowman, Vice President, Advanced Solutions, Verizon •

grant.obrien@verizonwireless.com

ABSTRACT

As cyber attacks continue to increase in sophistication and effectiveness, artificial intelligence is being leveraged more and more as a means of penetrating federal agency systems. The best defense against bad actor AI is to additionally employ AI to protect agency assets.

Verizon can discuss how AI can be employed to help increase situational awareness during attacks and defend critical infrastructure.

BIO: Craig Bowman is vice president of Verizon's Advanced Solutions Division. He provides strategy and engineering support for secure cloud initiatives in the public sector. Bowman speaks internationally on the subject of cybersecurity and has briefed congressional offices, senators, Olympic committees and international defense leaders.

Prior to Verizon, Bowman led the Defense and International Security Division of Adobe Systems, a *Fortune* 500 software and cloud software provider. In that capacity, Bowman helped to engineer secure content delivery systems for the most rugged security environments.

In his earlier years, Bowman was a software cybersecurity engineer for the defense and national security industry where he penetrated, tested, built and deployed secure software applications, remotely managed secure IT environments and deployed and managed secure telecommunication solutions.

Cyber Cognitive Operator

Jacob Cox, Research Scientist, Soar Technology Inc. • jacob.cox@soartech.com

ABSTRACT

The shortage of human cyber experts, vast cyber surface and speed of machines are driving the application of artificial intelligence (AI) in cyberspace. Indeed, the national strategies of the U.S. and China make it clear that future cyberspace operators will be augmented with autonomous agents. If an attacker is using AI to operate at machine speed, defense must occur at least as quickly to be effective. Research is already underway to develop more robust defensive agents that can hunt for and neutralize threats on their networks. Similar focus exists for the development of attack capabilities.

As a result of AI and the growing cyber surface, organizations can expect adversaries to use autonomous actors who can carry out attacks at varied rates against sets of potential targets. Similarly, defenders will employ cognitive agents to counter attacks on their networks at machine speed over 24/7 operations. It's possible to imagine that autonomous cyber hunt agents would select the right machine learning modules for specific times and contexts, reason over the information they provide and collaborate with their human teammates to eradicate threats.

Preparing for this eventuality, SoarTech is leading efforts to employ AI in penetration testing, cyber training and network defense. SoarTech's Cyber Cognitive Attacker (CyCog-A) is a synthetic offensive cognitive agent that emulates real attackers by modeling the complex thoughts, decision-making and contextual understanding of a human operator. Its goal-seeking behavior results in a wide range of realistic attacks, like phishing, remote exploitation and SQL injection. CyCog-A also can scan for hosts, services and vulnerabilities, perform lateral movement inside a breached network and exfiltrate files of interest.

CyCog-A is built upon the Soar cognitive architecture. The architecture is a co-symbolic production system capable of symbolic (e.g., rules, productions, etc.), episodic (e.g., temporal memory) and non-symbolic reinforcement learning. Non-symbolic machine learning contributes fast and scalable classification, pattern matching and prediction, while symbolic AI drives the integration and sense-making of the resulting information. Over multiple experiences or episodes, the agent can learn from its experiences by applying successful actions taken in previous encounters while condensing these steps into shorter and more effective and efficient chains. Alternatively, a Soar agent may learn effective policies through tuning its operator preferences over a series of decision-making steps. The CyCog agent's actions include updating its own internal mental model or executing a wide variety of command line tools to execute a specific cyber action, such as exploit or install payload. The time to execute a decision cycle is typically less than the 50 milliseconds hypothesized for a human decision cycle. This makes the agent reactive to changes in the external environment.

CyCog-A uses AI to penetration-test systems and other methods are available for AI to defend cyberspace. CyCog-A can make sense of complex information, collaborate with human teammates, emulate real attackers and perform cyber operations at machine speed. Future work for the CyCog architecture is planned.

BIO: Maj. Jacob Cox, USA (Ret.), Ph.D., is a research scientist at SoarTech, a leading research company in artificial intelligence. His fields of research include cyber operations, cyber electromagnetic activities (CEMA), software-defined radio, cyber physical systems, software-defined networking (SDN) and network simulation and modeling with an emphasis on trusted agent platforms. His recent research projects include Programming Abstraction Layers for SDNs, Security Policy Transition Framework for SDNs and Leveraging WebRTC and SDN to Detect Rogue Access Points. He has published in the areas of software-defined networking, network functions virtualization, network security, anomaly detection and policy enforcement. He holds certifications as a Certified Information System Security Professional and as a Certified Hacking Forensics Investigator. He is a member of ACM, IEEE, AFCEA and the Association of Old Crows.

Biney Dhillon, Chief Executive Officer, NexTech Solutions •

david.laughinghouse@nextechsol.com

ABSTRACT

NexTech Solutions and its partners recognize the Army's requirements as the primary need to develop and strengthen its understanding of the state of the art in AI techniques, algorithms and capabilities. For this requirement, the company recommends a solution from the NTS business partner, Veritone, called aiWARE.

aiWARE is an open platform that integrates an ecosystem of cognitive engines that can be orchestrated together to reveal multivariate insights through a suite of proprietary comparative applications. The aiWARE platform processes linear files such as radio and TV broadcasts, surveillance footage, recorded telephone calls, and other public and private content globally.

The Veritone aiWARE platform is an artificial intelligence operating system that transforms both structured and unstructured data into actionable intelligence. This result is achieved through a robust set of artificial intelligence cognitive engines and powerful applications acting in concert. aiWARE performs content ingestion, indexing, search, correlation, analytics, sharing and collaboration capabilities. The Veritone ecosystem hosts dozens of AI cognitive engines in a single platform to eliminate the need for businesses, agencies and individuals to select point solutions from the landscape of thousands of engines. This effectively future-proofs AI technology choices and ensures timely access to the latest AI advances and improvement in capabilities and accuracy.

aiWARE is an integrated yet extensible artificial intelligence technology stack. Veritone unlocks unique insights from data with a rich and multi-faceted portfolio of more than 200 cognitive engines. Clients can employ multiple engines within the same category or combine different categories of cognition. Veritone continuously researches artificial intelligence algorithms from a global network of more than 7,000 developers and works with select developers to integrate additional cognitive capabilities into aiWARE. With millions of hours of data processed, Veritone facilitates an economic exchange with proper incentives between data owners and the AI developers to foster dynamic iteration on cognitive processing with improved capabilities and results over time. aiWARE is specifically designed to enable the rapid incorporation of additional cognitive engines and applications through its APIs and container-based architecture. Veritone currently supports 15 different cognitive categories including speech-to-text, text translation, sentiment analysis, face detection, face recognition, object recognition, logo recognition, visual moderation, scene change analysis, audio fingerprinting, geolocation, optical character recognition, license plate recognition, transcoding and orchestration. The company makes efforts to integrate engines that can operate across deployment models, including network isolated, on-premises environments where security is tantamount.

BIO: Biney Dhillon assumed the role of CEO at NexTech Solutions in 2016. Dhillon has been managing large IT programs and projects for government and commercial organizations for more than two decades. With deep exposure to data center transformation, he began applying the lessons from his on-the-ground experience to the strategic side of operations in 2002, seeking opportunities for growth and innovation for clients.

AI and Moving Up the Attack Chain

Larry Gloss, Managing Director, BluVector Inc. • larry.gloss@bluvector.io

ABSTRACT

The numbers are daunting:

- 200,000 new malware threats a day; more than 30 percent of new malware threats are unknown/never seen before
- 80 percent of security environments suffer from staff shortages
- More than 40 percent of all security alerts not investigated

And the most alarming of all: The average time to detect a malware breach is 75 days.

The ideal cyber defense capability addresses these challenges and takes the current detection time down to minutes, not months. The speed of cyber demands a capability that can immediately detect and identify malware threats with high accuracy. Government environments typically require capabilities that operate completely on premises. AI and zero-day detection enables defensive cyber operations teams to move up the attack chain, remain on premises and take detection and containment to the very edge of the network.

“AI and Moving Up the Attack Chain” features a current, patented technology that detects unknown malware before a breach. By passively tapping a span port, the technology detects threats at wire speed. Its proprietary machine learning has been curated and constantly improved and consistently yields a false detection rate of under 1 percent immediately upon deployment.

To demonstrate this capability, a notional architecture that leverages commercially available products to yield a defense-in-depth capability is used. The attack chain is telescoped with AI-driven workflow automation, analyst-driven rulesets and protocols that detect both file-based and file-less zero-day malware. Case studies are referenced that attest to analyst performance improvement of 80 percent in case management, detection accuracy and alert adjudication. These same case studies document the orders of magnitude improvement in response time and the ability of analysts to seamlessly leverage AI technologies. Client references in the commercial world and among government agencies are available.

BIO: Larry Gloss leads cybersecurity solutions for public sector clients at BluVector. A published engineer, his background includes design, delivery and performance optimization of security environments for clients in civilian agencies, the U.S. Defense Department and the U.S. Intelligence Community.

Gloss enlisted in the U.S. Navy and was later commissioned from the U.S. Naval Academy. A Russian linguist, he served in operations Desert Shield and Desert Storm and earned a Navy Air Medal for combat reconnaissance. He earned graduate degrees in space systems and national security affairs.

His business experience includes executive positions in multiple start-up companies and business unit leadership in *Fortune* 100 technology firms.

Understanding the Cyber Terrain — Network Topology, Endpoint Characterization, Cybersecurity Posture – As the First Step to Active Cyber Defense

Dean Hullings, Senior Solutions Strategist, ForeScout Technologies Inc. •

dean.hullings@forescout.com

ABSTRACT

The U.S. Defense Department has numerous, complex, heterogeneous, multifunctional information technology, operational technology and platform information technology networks performing day-to-day mission-critical data sharing. These systems, for the most part, are all connected to make information sharing more efficient.

In addition, the department has adopted a layered cyber defense approach to securing and defending the “blue network” (friendly U.S. and allied forces) cyber terrain. When basic cybersecurity fails, they rely on U.S. Cyber Command’s cyber protection teams (CPT) to defend the networks.

However, what is missing in the Defense Department’s cyber warfare arsenal is an industry standards-based (NIST 800-53 and SANS Top-10) cybersecurity capability that establishes and maintains a high level of network awareness and cyber hygiene, making CPTs more effective when tasked. ForeScout Technologies offers such a capability that raises the level of compliance across the enterprise, uses automation to keep security high and, when needed, provides a source of accurate data of the key cyber terrain where CPTs are required to conduct DCO engagements to ensure the department’s networks are ready to support the mission.

BIO: With 30 years of experience in the information technology industry, Dean Hullings provides strategic recommendations and guidance to the ForeScout DoD account management team, connecting engagements and initiatives to maximize team productivity. Before joining ForeScout, Hullings spent 26 years in the U.S. Air Force as a communications and cyber officer, serving in various leadership positions for Air Force and joint commands. Hullings has a BS in computer and information science from the University of Delaware and three master’s degrees in public administration, military operations and national security and strategic studies.

Automated Secure and Optimal Cyber Configurations Using SOCCER

William Liu, Technical Director, LGS Innovations • wliu@lgsinnovations.com

ABSTRACT

Misconfigurations in cyber elements such as applications, devices, hosts, firewalls and networks could cause grave damages by exposing private data, allowing breaches and facilitating attacks. LGS Innovations and Vanderbilt University propose Secure Optimal Configurator with Cross-Component Examination and Reasoning (SOCCER) to remedy misconfigurations and improve defensive cyber operations. SOCCER uses artificial intelligence (AI)-aligned machine reasoning to automatically generate human-traceable configurations that satisfy security policies and minimize attack surfaces while achieving system functional and performance requirements.

SOCCER's approach comprises the following steps:

- 1) Build and maintain real-time situational understanding (SU) and operational contexts of the target system using machine learning.
- 2) Use domain-specific modeling languages to model the target system or network based on SU. Specify and incorporate the target's attack surfaces, configuration space—sets of all possible configurations such as the personal data access settings on a server—functional requirements, as well as security policies and metrics as logical overlays into the model.
- 3) Automatically solve the model mathematically to explore and prune the potentially large configuration space using constraints—for example, configurations that do not pass constraints are discarded or constraints are relaxed—to arrive at a manageable number of feasible target system configurations.
- 4) Evaluate the post-pruning feasible configurations using Pareto Efficiency to select optimal candidates that simultaneously minimize attack surfaces, satisfy system functional requirements and achieve security metrics defined by policies.
- 5) Use back annotation to mark up the analyzed models to explain to the operators why the configurations were chosen, thereby providing confidence and trust in the automatic solutions.
- 6) Generate and implement on the target system the secure configurations by auto-selecting the optimal configuration candidates.

Step 1 would involve scanning and surveying the target system periodically to build and track awareness including network topologies and the constituent devices and hosts. Natural language processing would be applied to continually extract knowledge on attack surfaces from external vulnerability knowledge bases, such as cyber vulnerability enumeration and common weakness enumeration, and apply it to the target

system. Additionally, machine learning, both support vector and deep learning techniques, would be used to identify and prioritize for protection, the high-value target system nodes, using labeled samples, network conditions, usage patterns and topological changes. For step 2, Vanderbilt's DARPA-proven Generic Modeling Environment tool would be used to model and analyze the target as a composed system, as well as represent operator behaviors as business process models. For step 3, automatic constraint-guided design space exploration techniques would be applied to provide computationally efficient inference without enumerating all possible configurations. For step 4, configuration selection would be treated as a multi-objective optimization problem in which satisfiability modulo theories solvers are used to reason over the post-pruning space and identify Pareto-optimal solutions that are optimized against attack surfaces, security metrics and functional requirements.

SOCGER could provide a long-needed critical capability that uses modeling and machine-based reasoning to securely configure cyber systems and enable their autonomous defense.

BIO: William Liu is a technical director at LGS Innovations in Herndon, Virginia. He has extensive experience in leading and managing cyber and systems engineering R&D programs sponsored by DARPA (DMT-PAMS, National Cyber Range Phase 1, Active Cyber Defense), the ONR and the AFRL, as well as commercial entities such as Fujitsu of Japan. Liu's technical expertise lies in the areas of cyber threat intelligence sharing and response using graph-based methods, ontology development, anomaly detection-based network security sensor, defensive cyber course of action modeling and simulation, software automation and adaptation using domain specific modeling and code generation technologies and software-defined radio development. He also has extensive solution architecting experiences where he developed large-scale managed IT service frameworks for U.S. Defense Department and IC customers using ITIL and Scaled Agile methodologies. Liu holds a bachelor of aerospace engineering degree from Georgia Tech and an MS in mechanical and aerospace engineering from Rutgers University.

Automated and Scalable Sensitive Document Classification

Malek Ben Salem, Senior R&D Manager, Accenture •

malek.ben.salem@accenture.com

ABSTRACT

Organizations use documents to communicate, perform business transactions, collaborate and innovate. These documents may carry confidential information and intellectual property. They have to be protected from unauthorized access, exfiltration or loss, but they need not be protected at the same level given that their contents are not equally sensitive, so identifying and properly labeling sensitive documents is important. Moreover, protecting sensitive data becomes even more challenging with the rapid pace of data growth, and a lot of the data comes in an unstructured format. For most organizations today, the confidentiality classification of documents remains a manual process, which makes it labor intensive, time consuming and vulnerable to intentional or inadvertent misclassification.

Accenture developed a tool called Scalable Classification through Machine Learning (SCAML) that automatically determines and labels the sensitivity level of documents to apply appropriate data protection controls. SCAML uses natural language processing and machine learning techniques to achieve high performance in terms of classification accuracy and scalability. Other security solutions, such as data loss prevention and enterprise data rights management solutions, can leverage SCAML's output to enforce the appropriate security controls.

BIO: Dr. Malek Ben Salem is a research and development senior manager at Accenture leading cybersecurity research at Accenture Labs. She has been with Accenture since 2011 and has authored several peer-reviewed publications and patents.

Her research interests include IoT security, behavioral biometrics, data protection and security analytics. She has also been a co-principal investigator on several DARPA projects, including Active Authentication and the Integrated Cyber Analysis System (ICAS). Prior to joining Accenture, Malek spent nine years working for IBM as a software engineer, controls engineer, data scientist and project manager.

Malek holds a doctorate and a master of science degree in computer science from Columbia University, New York and a Dipl.-Ing. in Electrical Engineering from the Technical University of Hanover, Germany.

Implementing Self-Healing, Self-Defending AI Systems

Nicola Whiting, CSO, Titania Ltd • nicola.whiting@titania.com

ABSTRACT

Essye Miller, the primary cyber defence advisor for the U.S. Defense Department, says cyber hygiene is what keeps her up at night. NCSC says most breaches come down to failures in the “easy stuff,” and its technical director is predicting a potentially preventable major attack.

So why hasn't AI solved this already? What's stopping AI from making sensible decisions and how can we empower the next generation of active AI-driven defense?

Titania Ltd identifies what's tipping the balance of automation in the attackers favor and how industry could join together and deliver the first truly self-healing, self-defending systems, making zero-days a hacker's last remaining option.

Discussion includes:

- Overview of current practices
- Challenges faced:
 - “junk in-junk out” - bad data, poor AI decisions, disastrous actions
 - “data bloat” - choosing the right information source for the right job and multiple efficiency gains
 - “cutting the cyber shackles”- what's needed to build trust in AI decision making to free experts to concentrate on strategic and offensive operations
- The mental shift needed by industry: Would streamlined data and AI systems mean fewer data storage and contracting profits?
- The BIG vision: As transformative as the Wright brothers' first flight or Kennedy's moon landing challenge?
- The step process needed to achieve self-healing, self-defending systems.

Titania software provides one of the key cornerstones for successful AI implementation. It provides accurate granular data on defined risks and their severity, their likelihood of exploitation and the command-line-specific mitigation needed to remove them. This capability was further developed in consultation with multiple military clients to provide fully autonomous and accurate STIG validation and analysis.

The company's tools have been assessed by independent labs, including the C.I.S. benchmark authority and certified as 100 percent accurate. Titania has a reputation for honesty and integrity. Titania produced some of the world's first software capable of virtualizing multiple manufacturers' network infrastructure devices and intelligently auditing them against known security issues.

BIO: Nicola Whiting has written for multiple defense magazines on this topic. She is an experienced chief strategy officer specializing in enterprise security automation software (self-healing systems) and neuropsychology. An Amazon bestselling author, she's written for magazines such as the *Huffington Post*, *Defence Contracts Bulletin*, *Defence News Online* and *SIGNAL Magazine*. *SC Magazine* named Whiting as one of the top 20 most influential women working in cybersecurity.

Portable Fiber Optics on the Battlefield

Larry Widgeon, Ground Tactical Product SME, KITCO Fiber Optics •

lwidgeon@gmail.com

ABSTRACT

WIN-T Increment 2, Big Army Network on-the-move, needs a more secure network by adding more single mode and multimode fiber reels to the network. KITCO has solved the portability problem by designing a portable KITCO Sustainment Enclosure (KSE) and placed a powerful quad fusion splicer in a backpack. A simple procedure allows set-up, breakdown and the fusion process to make the network more secure and less susceptible to hacking and simultaneously increases bandwidth.

BIO: Founder and former CEO and president of KITCO Fiber Optics, Larry Widgeon is now dedicated to the ground tactical arena and invention of products to help the warfighter sustain WIN-T and TOC systems in theater quickly and safely by fusion splicing of pigtailed. He is a leader and innovator of "Operation Pigtail" via Lt. Gen. Paul Ostrowski, USA, at the Pentagon.

AI and Machine Learning

Jeff Winterich, DoD Account Chief Technologist, Hewlett Packard Enterprise •

jeff.winterich@hpe.com

ABSTRACT

Artificial intelligence and machine learning in today's world as well as the U.S. Defense Department can be transformed from an art to a science.

BIO: Jeff Winterich is an account chief technologist for the HPE Department of Defense team. Winterich is responsible for providing strategic technology design and architecture expertise to HPE's federal government customers, partners and systems integrators, focusing on the U.S. Army, U.S. Air Force and combatant commands. He also serves as a Machine Evangelist for HPE Labs where he is responsible for providing insight into HPE Labs' activities around the next-generation data center to HPE federal customers.

In Depth Security From a Hacker's Point of View

Craig Bowman, Vice President, Advanced Solutions, Verizon •

grant.obrien@verizonwireless.com

ABSTRACT

SCADA, IoT, wireless and firewalls. Look at how threats are branching out across a wider spectrum of attack vectors and what you can do to get ahead of hackers' efforts.

Take a look at what Verizon is seeing on the network and how, from a hacker's point of view, you should implement technology, policies and procedures to help prevent the risk of future attacks.

BIO: Craig Bowman is vice president of Verizon's Advanced Solutions Division. He provides strategy and engineering support for secure cloud initiatives in the public sector. Bowman speaks internationally on the subject of cybersecurity and has briefed congressional offices, senators, Olympic committees and international defense leaders.

Prior to Verizon, Bowman led the Defense and International Security Division of Adobe Systems, a *Fortune* 500 software and cloud software provider. In that capacity, Bowman helped to engineer secure content delivery systems for the most rugged security environments.

In his earlier years, Bowman was a software cybersecurity engineer for the defense and national security industry where he penetrated, tested, built and deployed secure software applications, remotely managed secure IT environments and deployed and managed secure telecommunication solutions.

Cyber Integration with Warfighter Training Platforms

Kevin Hofstra, Chief Technology Officer, Metova CyberCENTS •

kevin.hofstra@metova.com

ABSTRACT

Metova CyberCENTS provides advanced cyber modeling and simulation (M&S) training environments for multidomain operations that integrate with kinetic and synthetic warfighter training systems. The company does this through the integration of a high-fidelity emulated, realistic and risk-free cyber M&S environments for training, TTP development, experimentation and exercising. Warfighters learn best through doing rather than observing, which is why it is so critical that cyber operations training includes a hands-on mission rehearsal capability that is connected into a multidomain operations environment training system. Metova's cyber environments are capable of recreating the dynamic network protocols and events necessary to accurately reflect the indicators of compromise associated with the advanced persistent threats representing the evolving adversary and insider threats cyber warriors face. The company combines this with machine learning, application programming interfaces and software brokers that integrate high-fidelity the cyber domain with live, virtual and constructive (LVC) warfighting domains, such as Army OneSAF, JLCCTC or hardware in the loop, to allow interconnection with communication systems and weapons platforms.

Metova CyberCENTS was one of four vendors selected to the DoD Persistent Cyber Training Environment (PCTE) Cyber Innovation Challenge (CIC) #1 under PEO-STRI. More specifically, the company was selected for Cyber Integration with Warfighter Training Platforms. This includes:

- Data exchanges, software brokers and application programming interfaces between the PCTE cyber range and other warfighting training platforms
- Integration of M&S platforms, industrial control systems electronic warfare, intelligence, kinetic (air, land, sea, space) domains and hardware in the loop

This review will focus on Metova CyberCENTS research and development in four areas:

1. Cyber integration with warfighter training platforms for the U.S. Defense Department PCTE CIC #1 under PEO-STRI
2. Cyber battlefield operating system simulation tools for LVC simulations (CyberBOSS) under Army Research Labs
3. Simulated cyber opposing force (OPFOR) for live, virtual, constructive & gaming (LVC&G) training simulations - Intelligent Cyber Adversaries Tool Suite (ICATS) under Army Research Labs
4. Multidomain operations cyber integration for Cyber Quest and Unified Challenge experiments under the Army Cyber Battle Lab

BIO: Kevin Hofstra has more than a decade of experience within Defense Department cyber operations, including the Air Force Network Integration Center, 38th Cyberspace Readiness Squadron, 835th Cyber Operations Squadron and the Air Force Cyber Protection Teams (AF CPTs). Prior to joining Metova, he led the development of the SCOPE Genesis component of the AF Cyber Vulnerability Assessment/Hunter Weapon System and helped build the first AF CPTs at Scott AFB. In his current role, Hofstra leads the development of the Metova Cyberoperations Enhanced Network and Training Simulators (CENTS) product portfolio used for cyber training for the Defense Department, federal and commercial customers. He led the Metova delivery of the Air National Guard's Virtual Interconnected Training Environment, Navy Cyber Operations Training Simulator and multiple Small Business Innovation Research (SBIR) projects. He currently is leading the Metova efforts on the PCTE CIC #1. His background includes a Bachelor of Science degree in computer science from Yale and two Master of Engineering degrees, one in telecommunications and one in engineering management, from the University of Colorado. Hofstra also serves as the communications sector chief for the Denver FBI InfraGard, a founding board member on the Florida Cyber Range and a strong advocate for public/private/academic partnerships and information sharing.

High Fidelity Modeling and Simulation for Commercial Mobile Networks and Mobile Apps Using an Innovative Live, Virtual and Constructive (LVC) Testbed

Steven Kropac, Chief Technology Officer - Cyber, LGS Innovations •

kropac@lgsinnovations.com

ABSTRACT

This solution is a new and innovative cyberspace modeling and simulation (M&S) solution to support cyber mission planning, proficiency training, cyber situational understanding (SU) and exercise support. The company has developed unique enhancements that improve the state of the art for commercial mobile network testbeds and training environments. Specific enhancements include: 1) an integrated high fidelity, flexible and cost-effective LVC environment that supports commercial mobile network equipment; 2) the capability for full 3GPP network protocol stack analysis with the ability to create customized message sets; and 3) a unique capability for live and virtualized mobile app traffic generation seamlessly integrated with the commercial modeling and simulation platform. This environment allows live 4G LTE technology to be integrated with a mix of live, virtualized and simulated handsets to support rapid course of action analysis.

The technical approach is based on using a commercial modeling and simulation software package to minimize technical risk. The platform has been enhanced with new Hardware in the Loop modules that support seamless integration with live commercial 4G radio access networks and access points. These can then be connected to live handsets using 4G radio frequency (RF) spectrum. This cost-effective integrated solution provides a previously unavailable level of fidelity for mobile network interfaces and endpoint devices in an M&S environment. The operator and analyst can utilize live handsets interacting with a simulated network yet have the ability to perform full 3GPP protocol traffic analysis to explore the effect of adversary cyberspace effects. In addition, the operator can substitute specific simulated network elements (NEs) with live NEs to support mission requirements. The operator can also install mobile apps onto live handsets as well as virtualized handsets in the simulated domain and have them interact with each other.

The solution allows NEs and handsets to be placed at specific latitude/longitude/altitude coordinates and mapped onto simulated terrain. As needed, specific NEs can be selected to be live. Mobility allows live and simulated handsets to move from one location to another, affected by RF propagation characteristics. It supports commercial handsets for the live domain Android virtual device handsets for the emulated domain and simulated handsets for the simulated domain. Interoperability between all handsets mapped to simulated terrain includes interoperability up through mobile applications for live and emulated handsets and

the ability to install commercially available mobile apps for high-fidelity traffic. The simulation system feeds GPS coordinates to apps and can collect analysis results from NEs, network traffic and mobile handsets.

The system provides unique cyber SU to support mission planning, course of action analysis and proficiency training for mobile networks and support the emerging needs of both Cross-Functional Teams pursuing the Army's network modernization goals.

BIO: Steven Kropac is chief technology officer and vice president of the Internet and Cybersecurity Research Department at LGS Innovations. His team is primarily focused on network assurance for commercial and military networks. He has more than 20 years experience as a subject matter expert on global carrier class network architecture, design and implementation. This includes several network and network element technologies, including optical transport, IP routing and switching, traditional and next-generation mobile network technology (3G, 4G, 5G) as well as traditional and next-generation public switched telephone networks.

Over the past 15 years, Kropac has been building a team of cybersecurity and network assurance experts primarily focused on security analysis of networks and network elements. His team has developed several innovative security solutions and has strong backgrounds in carrier class network technology, modeling and simulation, reverse engineering, vulnerability research, software development, protocol analysis and system engineering.

Kropac holds a Master of Science degree in computer engineering from Stevens Institute of Technology with a concentration in image and signal processing.

CyberSAF Simulator

Daniel Lacks, Chief Scientist, Cole Engineering Services Inc. •

daniel.lacks@cesicorp.com

ABSTRACT

The Army requires cyberspace modeling and simulation (M&S) in support of cyber mission planning, proficiency training, cyber situational understanding (SU) and exercise support. This demands that M&S tools perform cyber actions and cyber effects because the kinetic and cyber domains are becoming increasingly integrated and dependent upon one another. The CyberSAF Simulator focuses on cyber effects simulation as a partial solution provided by CyberSAF that interoperates with cyber action tools.

CyberSAF is a One Semi-Automated Forces (OneSAF) system configuration, a U.S. government-owned open source M&S framework designed to provide automation for planning, training, SU, exercise support, testing, experimentation, acquisition and analysis capabilities in an array of mission-specific kinetic, nonkinetic and cyber land, sea, air and space environments. CyberSAF addresses interactions between cyber effects and cyber and kinetic domains by responding to signals that, for example, may take control and crash a simulated unmanned vehicle; passively watch video feeds generated by the simulation; and activate or deactivate simulated Supervisory Control and Data Acquisition (SCADA) devices. These signals are exchanged with CyberSAF that can either act as a gateway between cyber action simulators or can act as a MSEL or test tool to stimulate CyberSAF on demand without requiring external systems. CyberSAF also can generate manual, reactive and automated outputs.

OneSAF interoperates with a variety of mission command systems, including the future SitaWare system currently in development. SitaWare provides a potential platform to host CyberSU capabilities with its open architecture. Integrating with SitaWare will provide an intuitive and familiar platform for cyberspace mission and support personnel at all levels. For example, Cole Engineering Services Inc. built a prototype course of action (COA) analysis SitaWare plugin that embeds OneSAF and Marine Air-Ground Task Force Tactical Warfare Simulation into the mission command stack to provide artificial intelligence that identifies likely challenges, viable COAs and potential mission impacts.

OneSAF provides a low-fidelity emulation of realistic mission-specific logical environments such as cell towers, IP networks and satellite links. It has been used as a tactical traffic generator for testing and security accreditation activities, pairing well with other commercial and military generators. OneSAF includes a variety of cyber capabilities such as Cyber Operations Battlefield Web Services (COBWebS) that create an adversary's cyberspace effects, anomalous network activities and insider threats without changing the configuration or software of mission command systems.

Integration with SitaWare hides the details of the simulation from the commander, enabling seamless imports of existing SitaWare plans, equipment and scenarios for expedient cloud-based COA analysis outputting a variety of information, charts and graphs aiding the military decision-making process.

As a component of WARSIM and LVC-IA, OneSAF participates in exercises at different classification levels separated by a guard interface. Higher classified capabilities are exercised in a domain synchronized and fed with conventional warfare information from lower classification domains. In the case of the PCTE, this approach may provide a solution as the cyber effects are exchanged between domains as opposed to the cyber actions and techniques that stimulated those effects.

BIO: Dr. Daniel Lacks is the chief scientist at Cole Engineering Services Inc. (CESI). He received a Bachelor of Science degree in computer engineering in 2001, Master of Science degree in 2002 and a doctorate in 2007 from the University of Central Florida specializing in distributed computing, software simulation and software engineering. Since 2001, Lacks has worked as a software and systems engineer in the U.S. Defense Department, modeling and simulation industry on live, virtual and constructive programs including Warfighter's Simulation (WARSIM) and the One Semi-Automated Forces (OneSAF) Integration and Interoperability Support (I2S) program. He briefed the results of a prototype for embedding OneSAF and the Marine Air-Ground Task Force Tactical Warfare Simulation into SitaWare the mission command stack to provide artificial intelligence that identifies likely challenges, viable COAs and potential mission impacts at ITEC 2018.

Muddler

**Accenture Federal Services Adversary Research and Recon Team,
AFS ARRT, Accenture Federal Services • greg.wells@accenturefederal.com**

ABSTRACT

Accenture Federal Service presents Muddler, an essential product for any computer network operations (CNO) code compilation tool chain. Built by the Adversary Research and Reconnaissance Team (ARRT), Muddler provides binary obfuscation and binary diversity and increases the time and effort required to reverse engineer, correlate and attribute a binary without requiring changes in source code. The company recognizes the challenges faced by today's cyber operators when deploying tools to hostile environments and the necessity to minimize mission impact if discovered. Muddler mitigates that risk by providing a simple way to compile variations of a tool without modifying source code or disrupting functionality.

Muddler is a suite of transform plug-ins that enhance the LLVM compiler by applying specific obfuscation techniques. Plug-ins can be chained together in any order, configuration or iteration to provide multiple layers of obfuscation and compound the effect of each plugin. This essentially results in the ability to produce an infinite number of unique tool binaries. Operating as LLVM modules, the plug-ins inherently benefit from the wide variety of architectures and operating systems supported by LLVM, including x86, x64, ARM, macOS, Linux, Windows, iOS and Android. Muddler integrates into established toolchains without disrupting developer workflow, augmenting ongoing cyber operations with all the obfuscation power the system offers.

Muddler, as with all ARRT CNO offerings, is a mature product that undergoes continual and automated testing in the company's development operations environment. During nightly tests, ARRT implant agents are compiled with Muddler and then tested end-to-end, from deployment to a target to tasking through its command and control platform to verify functionality. Beyond functional testing, ARRT performed several internal research campaigns to validate the effectiveness of Muddler against the leading binary comparison tools, analyze the risk of introducing Muddler-related signatures and implement machine learning models to identify the best mix of Muddler plug-ins and their configurations. Because of these efforts and iterative improvements based on the results, Accenture Federal Service stands behind Muddler as a capability necessary for today's cyber operations.

BIO: Accenture Federal Services' Adversary Research and Reconnaissance Team provides software solutions to the U.S. Intelligence Community and Defense Department that enable and enhance offensive cyber operations. Since 2008, the team has been researching and exploiting vulnerabilities in software and embedded systems and developing complementary implants and C2 software to enable advanced offensive cyber operations.

On-Demand, Secure and Traceless Cloud Networks

Jason Crowley, Business Development, Dexter Edward • jcrowley@dexteredward.com

ABSTRACT

Dexter Edward is a leading integrator of secure, traceless and anonymous cloud-based mission partner networks (MPN) utilizing commercial cloud infrastructure. Its immediately available software solutions aid in institutional adherence to the Federal Acquisition Streamlining Act (FASA) of 1994 by providing readily available commercial items and limiting unnecessary government research and development costs.

The core of this capability is the proprietary, patented Fognigma enterprise software engine that administers the automated deployment of polymorphic, on-demand ephemeral infrastructures over seven commercial cloud providers, which encompass more than 100 data centers in more than 50 regions over five continents. The virtual nature of the Fognigma environment allows for global scalability and adaptability per mission requirements.

All data transmitted over the Fognigma MPN is secured using cascading, dual-wrapped AES-256 symmetric encryption with 4096-bit RSA for initial key exchange, guaranteeing full user control over the fidelity of their data. Integrated collaboration components include encrypted and obfuscated telephony, voice and video-conferencing, chat messaging, file transfer and storage and Virtual Desktop Infrastructure (VDI) enabling the secure, traceless exchange of information at all levels.

Unlike other software-defined network (SDN) providers, Fognigma allows for multiple implementation configurations to fit each organization's varying needs:

1. Traditional cloud-based integration affording access to the MPN by way of the NigmaClient or reverse proxy—perfect for remote and/or mobile users.
2. The on-premises Fognigma Gateway, which enhances existing networks regardless of topology by ensuring all data transferred from the network is routed through a Fognigma MPN.
3. The Fognigma Wicket provides a portable gateway-like device that provides MPN functionality for small office/home office environments.

MPN hybrid cloud environments facilitate interagency and multilateral collaboration between organizations without sacrificing security. Furthermore, Fognigma and its associated components are device agnostic working on any desktop, laptop or mobile device, alleviating the need for additional organizational implementation costs.

Fognigma's secure MPNs offer variety, anonymity, scalability and availability of resources through any civilian infrastructure capable of data transmission, trusted or untrusted, allowing users unparalleled freedom of movement in the accomplishment of their mission.

Fognigma's globally available virtual point-of-presence provides for the inherent obfuscation of activities while mitigating an adversary's ability to detect and attack the network. Organizations define the MPN, selecting the preferred cloud providers and entry and exit points, ensuring that each SDN instance is specific to the unit's needs and mission.

Fognigma component VDIs provide sandboxed Linux or Windows environments capable of incorporating organizationally specific programs. This integration ability facilitates continuity of operations while mitigating risk to the user's core network, while still applying Fognigma's intrinsic managed attribution capabilities. Sandboxed VDIs offer full USB compatibility, including CAC readers, printers and keyboards, allowing users to import and export data as required.

All MPN instances are created in real time, as needed, ensuring they have no previous target profile associated with them and, when they are no longer of use, are destroyed and remain forensically undetectable. Using Fognigma's cyber stealth technology, the U.S. Defense Department can greatly enhance its offensive and defensive cyberspace missions worldwide.

BIO: Jason Crowley is a U.S. Army veteran and former federal civilian employee with more than 23 years of experience in intelligence collection within the Defense Department. His experience focuses on HUMINT, MASINT, OSINT and technical collection in support of U.S. tactical and strategic goals and provides him with a unique insight into the mind of military users and the challenges they face.

Establishment of Secure Networks on Untrusted or Hostile Infrastructure

Jonathan Roy, Principal Security Architect, Unisys Corporation •

jonathan.roy@unisys.com

ABSTRACT

The technological capability exists to deploy endpoints on a untrusted or hostile network, while keeping the trusted endpoints cloaked and their network traffic secure. This technique is based on a microsegmentation overlay software that uses distributed point-to-point IPSec, coupled within built-in network filtering capabilities of participating endpoints. While a derivative of this can be accomplished manually with static elements found in some operating systems, the Stealth Solution accomplishes this dynamically and in real-time by not relying on IP address, network policy enforcement chokepoint, or trust level of the network.

Stealth is a software security overlay that protects data-in-motion with encrypted microsegmentation, while cloaking network assets with role/identity/attribute-based access controls. Additionally, Stealth provides streamlined change control and provisioning operations, threat mitigation with near-real time quarantining, resulting in the establishment of trusted boundaries that can traverse any infrastructure, to include legacy and end-of-life equipment, on-premise (virtual or physical) platforms and forward-deployed tactical edge assets or can extend out to the cloud. The Unisys Stealth Solution can dynamically configure endpoints to only accept traffic from other endpoints equipped with the Stealth Solution thus cloaking them from non-stealth enabled endpoints. All network communications are fully encrypted using IPSec thus denying access to the information contained in the network communication and also ensuring the integrity and authenticity of the communication. Stealth dynamically manages the endpoints network filtering platform and will only respond to or accept network traffic from another Stealth-enabled endpoint so the adversary will not receive any response from a Stealth-protected endpoint.

Coordinating firewall changes across a global enterprise is complex and time consuming. When applications need to be segmented from other systems to control administrative access, enforce data classification segmentation or meet a mission/business need and sensitivity, most other solutions require creating separate network space, VLANs and layering physical or virtual firewalls. In contrast, Stealth segments without the need to fragment the network or adding layers of firewalls. This streamlines infrastructure by displacing the need for layers of firewalls, VLANs and thousands of firewall objects.

Stealth is accredited by the National Information Assurance Partnership (NIAP) and is an approved component on NSA's Commercial Solutions for Classified (CSfC). This capability can be used to create latent command and control networks that remain turned off until the need arises. When the need arises, the endpoints can be switched on and the Stealth Solution will dynamically create, configure and secure an out-of-band command and control network. This technique also can be applied to covert offensive operations. This could give the offensive force a foothold on a hostile network, while keeping the endpoint cloaked on the hostile network.

The Stealth Solution can create small, secure and out-of-band networks from larger unknown/untrusted networks while cloaking the endpoints into trusted software-defined boundaries thus giving the users the ability to operate securely anywhere on any network regardless of who owns or manages the underlying infrastructure.

BIO: Jonathan Roy is a principal security architect for Unisys Corporation with a focus on software-defined enterprise. Roy is an expert in enterprise security architecture and has led the design and implementation of more than 50 agencies transforming into a consolidated Software-Defined Enterprise. He has planned and executed numerous enterprise-scale security solutions leveraging his subject matter expertise in cross-domain technologies, microsegmentation, identity and access management, cloud transformation and secure multitenancy integrating into multiple defense-in-depth security tools with the objective to address security requirements in NIST/DOD RMF and NSA CSFC frameworks.

Roy served in the U.S. Army from January 2003 to 2009 providing tactical network and satellite communications, while stationed in Mannheim, Germany, and at MacDill Air Force Base in Tampa, Florida, with the Joint Communication Support Element. Roy served in multiple deployments to support operations Iraqi Freedom and Enduring Freedom.

Roy received an Master of Science and Master's of Business Administration from the University of Maryland.

Operation Pigtail

Larry Widgeon, National Sales and Marketing Manager, KITCO Fiber Optics •

lwidgeon@gmail.com

ABSTRACT

There are more than 20,000 reels of tactical fiber optic cable in theater utilized by the WIN-T and TOC programs. These reels offer high bandwidth and a secure network as they are impervious to cyber intrusion and EMI. However, they are impossible to re-terminate in the field in harsh environments. A unique product has been invented that enables the warfighter to carry a KITCO Sustainment Enclosure (KSE) in the battlefield and set it up even at night. Two warfighters can enter this enclosure with the WidgCo BackPack, spread out the BackPack and fusion splice a “pigtail” in place of the broken connector. Inline fusion splicing can be accomplished if the problem is only fiber related.

At the present time, the Army and Marine Corps are replacing the entire reel if there is a problem; this is very costly. They are also hesitant to place fiber, even with all of its advantages, in WIN-T Increment 2 because of the difficulty in sustainment. The advent of the WidgCo BackPack and KSE could reap enormous technical enhancements and economic windfalls for the ground tactical warfighter.

BIO: Larry Widgeon is the co-founder of KITCO Fiber Optics and a pioneer in sustainment of shipboard and tactical fiber systems throughout the armed forces and all aspects of the U.S. Defense Department. He has been instrumental in developing MIL-STD-2042 and the design of cleaning, inspection, termination and test equipment for all branches of Defense Department for the past 25 years. Widgeon recently invented a method for sustainment of TFOCA reels of fiber for WIN-T on the move.

SWaP Improvements in RF High Power Amplifiers

Steve Richeson, Vice President, Sales and Marketing, Mission Microwave •

steve.richeson@missionmicrowave.com

ABSTRACT

Mission Microwave RF solid-state amplifiers and frequency converters are becoming widely deployed in SATCOM communications ground terminals for MILSATCOM application. These amplifiers use gallium nitride semiconductors and unique design and linearization techniques to provide a drastic increase in performance at roughly 25 percent of the weight of traditional RF amplifiers.

These same amplifier construction and weight/power reduction techniques can be applied to EW applications that also require a high degree of linearity, performance and reliability. Examples of compelling weight reduction for mobile, airborne and ground portable applications will be covered highlighting the potential for application of these same technologies to the EW domain.

The primary frequency ranges covered by these COTS products are X, Ku and Ka bands with power densities exemplified by a 10 pounds, 100 watt Ka band amplifier and up converter that takes the place of amplifiers that weigh well over 60 pounds. Examples in X-band for ground or airborne scenarios also are available. The goal is to create awareness of this new capability and begin to understand EW requirements where these low SWaP amplifiers may provide a benefit.

BIO: Steve Richeson is the vice president, sales and marketing, at Mission Microwave Technologies LLC. Richeson joined Mission Microwave in 2017. He has 30 years of satellite and radio frequency experience in engineering and sales leadership roles at Advantech Wireless, Exelis Inc., Harris Corporation, EchoStar, Scientific-Atlanta, GTE Spacenet International, SATCOM Technologies and Schlumberger. Richeson is a senior member of the IEEE and a Registered Professional Engineer. He earned his engineering degree at Georgia Tech and an MBA at Georgia State University.

Unified Heterogeneous Network (HetNet) Transport

Denis Couillard, Director, Government Strategy, Ultra Electronics TCS •

denis.couillard@ultra-tcs.com

ABSTRACT

The Ultra ORION radio offers a unified heterogeneous network (HetNet) transport solution that provides seamless broadband connectivity from brigade-to-mobile edge and solves several of the Army's tactical network design challenges. By simultaneously activating different waveforms in different frequency bands, ORION-based networks can adapt to solve various interoperability, range, throughput, latency, mobility and EA challenges as environments and missions change. All the waveforms required by the various echelons and missions are available in one, multichannel, multiband radio system: the ORION "One Radio In One Network" system.

ORION enables overlapping network layers to ensure nodes can be connected through a diversity of waveforms, including ECCM/AJ, channel bandwidths, network topologies, frequency bands, routes, antenna types and polarization, MIMO paths and radio channels. The result is a multitransport tactical network that provides multiple layers of diversity, multiple data paths to network nodes, significant scalability and band flexibility.

This approach is optimal to efficiently transmit different types of tactical data traffic, permanent or bursty, unicast or multicast, multi-priority. The waveform selection, combination and redundancy are entirely managed at layer 2—redundant VLANs are automatically created, routed and managed by ORION network processors—and transparent to upper network layers that ensure the expected ease-of-use to the end user.

The ORION radio system provides a unified HetNet that enables joint interoperability and has been selected by PM Tactical Network for the TRILOS program of record under the nomenclature AN/GRC-262(V)1.

BIO: Denis Couillard has received his B. Eng. in electrical engineering and his Master in Technology Management from École Polytechnique de Montreal, Canada. He has more than 30 years experience in the telecom industry where he helped launch several new radio communication technologies and products, working on products innovation for several years. Couillard authored a book on strategic technology management and holds two U.S. patents on electronic attack and protection. He is currently director of government strategy at Ultra Electronics TCS in Montreal. Ultra has designed and deployed thousands of early cognitive radios in South Korea and is known in North America as the designer of the GRC-245 HCLOS and GRC-262 TRILOS radios, the terrestrial backbone of U.S. and Canadian Forces in the field.

The NTS Tactical Edge

Biney Dhillon, Chief Executive Officer, NexTech Solutions •

david.laughinghouse@nextechsol.com

ABSTRACT

The company's mission in supporting the tactical community across the U.S. Defense Department has been to build As-a-Service (AaS) solutions for remote/tactical users and provide full automation capabilities to enable true tactical communication.

One of the major challenges in creating this solution has been addressing the disconnected, intermittent and limited conditions concerns of the forward-operating environment. This has traditionally been a limiting factor in the types of services and functions that can be deployed to the operator. NTS seeks to provide insight to the Army on how it has addressed these concerns for other forward-deployed units and how it uses next-generation, small-form factor hardware to greatly enhance the capabilities provided to the Army.

The company works with leading tactical organizations in the Defense Department and federal government including USSOCOM, JCSE, USN PMW 790, USAF 844 CG, USAF 5CCG, and USA WIN-T. It has also designed, tested and is implementing the NTS Tactical Edge, which is built upon the Klas Voyager Tactical Data Center (TDC), an enterprise-grade tactical data center in a single airline carry-on size rollaway case with 32 physical Intel Xeon cores, 512 GB RAM and an integrated 10 Gbps switch to provide the highest performance and smallest footprint on the market today. The hypervisor-agnostic TDC is certified and tested for use with Rubrik, VMware, Nutanix, Red Hat, Microsoft and other on-premise Hyperconverged Infrastructure (HCI) solutions. The NTS Tactical Edge meets a broad set of certification requirements, including NIST, FIPS 140-2, Suite B and CSfC. This solution is built on modular, line replaceable units, field sustainable with minimal training. The small form factor modules run efficiently on low power requirements, and the component case provides environmentally sealed protection for the equipment. No external environmental support is required, and the unit can run on battery power for up to an hour before being connected to a small generator or a vehicle to recharge the internal batteries. The solution for compute and storage can fit in the overhead bin of airliner, providing complete flexibility to the deploying forces.

To meet the Army's requirements, the company would recommend a Klas Telecom TDC and Voyager VMm for the physical HCI and Rubrik for the Software and build/management. Leveraging Rubrik revolutionizes how warfighters can quickly move services between primary, fixed-site data centers and the TDC. Rubrik allows the company to ingest, de-duplicate and then replicate entire enterprise server stacks to the KLAS TDC. When the deployed mission stands down, administrators in the fixed site can instantly resume those services. This also dramatically minimizes deployment, re-deployment and disaster recovery times and reduces manpower.

BIO: Biney Dhillon assumed the role of CEO at NexTech Solutions in 2016. Dhillon has been managing large IT programs and projects for government and commercial organizations for more than two decades. With deep exposure to data center transformation, he began applying the lessons from his on-the-ground experience to the strategic side of operations in 2002, seeking opportunities for growth and innovation for clients.

Do You Want Good Network Resiliency Today or to Wait for Unknown Routing Tomorrow? COTS Multipath Is Here Today

David Howgill, President, Huckworthy • dhowgill@huckworthy.com

ABSTRACT

Cellular networks, broadcast networks and even home networks have options for spectrum resiliency/diversity today and all are COTS. These same users have access to spectrum sensors and multiband automatically switching/synchronizing radios and data circuits. So why doesn't the Army have this access?

Systems integrators can deliver COTS technology today that will beat the EW and spectrum congestion threats of today, or the Army can wait for tomorrow's technology and tomorrow's evolved threat.

The risk to the Army is whether products are rugged enough and hardened enough to operate in harsh environments. The security layers are NOT difficult to implement in COTS as the risks are similar and many of the COTS solutions are designed with IP67/IP67 in mind. Milspec? No. Going to last a year at a fraction of the price of the Milspec one designed for three years and deliverable in two years? Yes.

To stay ahead, the Army has to leverage COTS. Its systems integrators already know how, and it's using U.S. technology available today.

BIO: David Howgill is founder and president of Huckworthy LLC, a Washington, DC-based integrator, consultancy and distributor of specialized advanced wireless telecommunications, specialist audio and video, energy and security solutions.

Howgill also serves as chairman of the Global VSAT Forum Wireless Backhaul Group and co-chairman of the British American Business Association's Small Business Group.

Huckworthy provides private, emergency responder and tactical LTE and hybrid wireless networks, encrypted communications, wireless intelligence solutions, hearing protection and HD audio solutions. Huckworthy is a certified HUBZone Small Business and a protégé of The Boeing Company under the Department of Defense's Mentor-Protégé Program.

Increase Integrated Resilience at the Tactical Edge with Software-Defined WAN (SD-WAN)

Martin Isaksen, Senior Architect, Cisco • marisaks@cisco.com

ABSTRACT

The need for transport, network and application path resilience is paramount for increasing automatic path diversity at the tactical edge. SD-WAN provides a software capability to increase intelligent network resiliency at the tactical edge by seamlessly integrating existing wired/wireless transports, future transports and even older legacy transports to increase communication availability under DIL conditions. SD-WAN can enhance end-to-end assured voice and data services at the tactical edge by leveraging multiple transport paths with continuous monitoring QoS, plug-and-play setup, SBU encryption, analytics and intelligent application routing.

BIO: Martin Isaksen has more than 30 years of U.S. Defense Department experience in applications, networking and software solutions. He is currently the senior architect for Cisco's federal defense business. In his prior role as Microsoft Federal DoD CTO, he led the Microsoft technology strategy for unified communications, hybrid cloud, business productivity and mobility. Prior to that role, Isaksen worked at Nortel for 10 years as DoD chief architect supporting several mission-critical systems for the federal government, including the NASA Space Shuttle IP Multicast Network and the first DoD-certified VoIP solution at Fort Huachuca, Arizona. Prior to that, Isaksen worked in the federal government for 11 years across Defense Department and civilian agencies as a branch chief and architect where he helped publish the first Defense Department websites at the Defense Technical Information Center. He holds a Bachelor of Science degree in computer science from the University of Maryland University College.

Core Level Security Extended to the Tactical Edge

SafeNet AT • mary.shiflett@safenetat.com

ABSTRACT

Core data center functionality is moving to the field as part of battlefield multidomain transformation. It is becoming commonplace for command posts, mobile command centers and even mobile platforms—vehicles, ships and planes—to contain micro data centers that provide new capabilities and services at the cyber edge to the warfighter. What still needs to be addressed is how to effectively transition existing core cybersecurity controls so data is protected in the field when faced with conditions such as:

- Harsh environments
- Bandwidth-limited and disconnected environments
- Overrun or hostile scenarios
- SWaP constraints

Core cybersecurity controls can be transitioned to the tactical field to safely provide highly sensitive data for command and warfighters at the cyber edge.

Network Automation – Rapid Response to Enterprise Threats

Chuck Swan, Solutions Architect, Force 3 • cswan@force3.com

ABSTRACT

Today's technologies demand a network that constantly learns, constantly adapts and constantly protects so users can work faster, more efficiently and more securely. Mission requirements are always changing, which puts network operators into a reactive posture that requires participation from multiple teams: network, security and endpoint management are just a few. Even with the most responsive and talented teams, timing and accuracy are still a challenge and threat detection is usually an afterthought or a bolt-on solution. Network automation can address these issues by automating provisioning and configuration with predefined and approved rules and policies that provision the network itself and deploys the appropriate security tools without human error or the inefficiency of coordinating multiple teams.

Network automation by itself is a powerful concept, but when it can be leveraged by the network acting as a sensor to take action based on security threats with or without operator assistance, the network can now defend itself. Analyzing traffic behavior, the network can identify threats and dynamically restrict access permissions or remove it as its threat potential worsens. Once the threat is contained, focus can be placed on remediating the endpoint.

Unfortunately, many organizations look to automation as a point solution to a specific need such as network provisioning or security and find little value compared to the conceived complexity and learning curve of automation. To enjoy the benefits, organizations should look for automation to solve interdependent requirements and solve broader workflow challenges. Open source tools should be evaluated with the understanding they will require a higher degree of operator expertise. Commercial tools have cost concerns and require less demand from the operators. Vendor-specific software-defined network tools demand even less from operators but may have vendor-specific hardware requirements. Larger organizations will find a mix of tools will solve more challenges.

BIO: Chuck Swan is a network solutions architect with Force 3 who helps federal and specifically DOD customers rethink their network solutions to simplify management and improve their security posture. Swan has more than 20 years of experience in the networking industry with expertise in wired and wireless networks.

Enabling IoT at the Edge

Jeff Winterich, DoD Account Chief Technologist, Hewlett Packard Enterprise •

jeff.winterich@hpe.com

ABSTRACT

As the computing world moves to a software-defined state, COTS Internet of Things (IoT) devices are enabling an improvement in services and capabilities at the edge all with an improved SWaP (size, weight and power) footprint. IoT edge devices can help the Army moving forward as network agility and other improvements are being considered.

BIO: Jeff Winterich is an account chief technologist for the HPE Department of Defense team. Winterich is responsible for providing strategic technology design and architecture expertise to HPE's federal government customers, partners and systems integrators, focusing on the U.S. Army, U.S. Air Force and combatant commands. Winterich also serves as a Machine Evangelist for HPE Labs where he is responsible for providing insight into HPE Labs' activities around the next-generation data center to HPE federal customers.

A “Future Tactical Waveform” Process for Accurate Position, Navigation and Timing

Timothy Allen, Senior Principal Software Engineer, CERDEC S&TCD •

timothy.j.allen7.ctr@mail.mil

ABSTRACT

To reduce radio frequency signatures in contested electronic warfare (EW) environments, a modern terrestrial tactical radio waveform relies on accurate position, navigation and timing (PNT) to control, inter alia, time of transmission (TX) and reception (RX) as well as pointing of directional antennas. A process exists whereby a future tactical waveform (FTW), when deployed in a network, can provide accurate PNT without use of a Global Navigation Satellite System (GNSS) signals, such as the Global Positioning System.

In the first step of the FTW process, each radio establishes its authorization-to-participate (ATP) and identity. This paper compares and contrasts the FTW process to the Highband Networked Waveform (HNW) because HNW is an existing fielded technology whose radios already are designed to maintain accurate timing for control of TX/RX time slots, integrate with their host platform’s inertial navigation system and inherently exchange geographic position among radios. In short, this paper posits HNW as a conceptual engineering line of departure for the development and demonstration of a real physical FTW radio network.

The next several steps of the FTW process advance FTW radios individually through progressively refined stages of PNT. In an expeditionary setting completely devoid of GNSS signals, FTW radios can start with crude map-spotted positions and estimated timing that is off the cuff. Even so, FTW radios among themselves will be able to expeditiously refine PNT accuracies to a sufficient degree that supports basic tactical maneuver and fire support. Then, as FTW radios join the network with better PNT accuracies, for example when collocated with a survey control point established by a topographical engineer unit, the FTW process will propagate the more accurate PNT to other FTW radios throughout the network and allow them to refine their PNT accuracies to the mathematical limits imposed by terrain, location and radio frequency environment. Operators and applications that require knowledge of both PNT values and accuracies will be able to obtain them from the FTW radio on the same platform.

With progressively more accurate PNT and when augmented with additional data, FTW radios will be able to support advanced functionalities, such as networking on-the-move, intermittent link connectivity, network fragmentation and recombination, and PNT support for disadvantaged and exo-networked nodes. In one example of an advanced function, suitably equipped FTW radio import terrain data—such as digital elevation, foliage and structures—and a scheme of maneuver, wargame the operation and advise the communications-electronics staff on the network’s capabilities to support the operation’s requirements for link connectivity and PNT accuracy. In another example, the civil-military operations staff determines it advantages to accommodate the large number of nonmilitary people who have GNSS equipment and thereby recommend having some FTW radios export PNT to pseudolites.

BIO: Timothy Allen is a software engineer with more than 40 years in airborne EW, radar, telephony and military communications modeling and simulation. He is a retired Army officer with 30 years commissioned service in Signal Corps and Field Artillery.

Adaptive and Efficient Frequency Band Reuse for Reduced RF Signatures

Ronald Connelly, Program Manager, Alion Science and Technology •

rconnelly@alionscience.com

ABSTRACT

The Army is seeking technologies to reduce the RF signatures of its radios and make them less susceptible to electronic attack. To achieve this goal, Alion proposes using multiple input/multiple output (MIMO) technology and orthogonal frequency division multiplexing (OFDM). The method allows radios to simultaneously reuse frequency channels, thereby decreasing the spectrum footprint by minimizing bandwidth, which also makes the radio transmissions harder to detect. Alion applies this technique to a frequency-hopping system to further decrease the probability of detection, while increasing communication throughput speed.

Traditional wireless communication systems use a single antenna for transmission and a single antenna for reception. Such systems are known as single input/single output systems. In recent years, significant progress has been made in developing systems that use multiple antennas at the transmitter and the receiver to achieve better performance. Such systems are known as multiple input/multiple output systems.

In a contested or congested electromagnetic environment (EME), RF systems do not have the available spectrum to use multiple frequency channels when necessary. To minimize the number of channels required to operate, Alion uses a form of frequency division duplexing OFDM. The Alion solution will allow systems to transmit and receive multiple OFDM frequency bands simultaneously in the same frequency bands, a design achieved by changing the phase modulation of the OFDM signals. While each carrier frequency is phase modulated and amplitude modulated within an OFDM signal, the solution remodulates the OFDM signal phases by 90 degrees. For example, the first OFDM signal is modulated at 0 degrees, the second OFDM signal will be modulated at 90 degrees, the third OFDM signal will be modulated at 180 degrees and the fourth OFDM signal will be modulated at 270 degrees. Therefore, on the receiver side, Alion demodulates the phase modulation to separate the OFDM signals before demodulating each OFDM packet. Using this process, about 6-10dB signal-to-noise ratio is lost but the gain is much higher communication speed on the order of four.

The solution allows simultaneous use of four OFDM channels in the same frequency band and achieves close to four times greater throughput speed. Reuse of the same frequency bands reduces the spectrum footprint by a magnitude of four because four times less spectrum is used to send four times more data in a given time period.

This type of MIMO technology is just starting to make its way into the commercial sector; however, most arrangements only use two to three OFDM channels, while Alion proposes using four OFDM channels.

BIO: Ronald Connelly has 20 years of experience in the field of spectrum engineering, electromagnetic compatibility analysis and program management. Connelly has performed electromagnetic compatibility analysis, RF propagation analysis and signal-to-noise and interference-to-noise analysis for numerous communication systems. He has managed programs that involved the development and design of new RF systems to operate in the electromagnetic environment for agencies such as DARPA, U.S. Army CERDEC, AFRL and NASA. Connelly has a Bachelor of Science degree in mathematics from Stony Brook University, Master of Science degree in electrical engineering from New York Institute of Technology and Master of Business Administration degree from Johns Hopkins University.

Charles Abraham, a member of this team, has more than 20 years of experience in the field of RF design. Abraham has designed and developed numerous RF systems and has expertise in developing OFDM modulations, digital signal processing and other modulation techniques. He has designed new radar systems to enable them to gain higher signal-to-noise ratios and track small fast-moving targets like bullets. Abraham has a Bachelor of Science degree in electrical engineering from the University of Pennsylvania.

Multilayer Network Diversity and Adaptation

Denis Couillard, Director, Government Strategy, Ultra Electronics TCS •

denis.couillard@ultra-tcs.com

ABSTRACT

By offering a unified heterogeneous network (HetNet) transport solution, Ultra ORION provides frequency agility, multilayer network diversity, multiple data paths and significant scalability. In contested environments and in addition to multilayer diversity, ORION offers 1000hops/s frequency hopping ECCM MIMO waveforms in both PTP and PMP topologies and automatic frequency change (AFC) features in all its backhaul waveforms. By using two polarizations and two antennas for both transmission and reception on all links, ORION benefits from advantages not previously available in electronic protection schemes. Beam switching antenna technology is also leveraged to improve both LPD, link robustness, resistance to jamming and increased ease of use.

ORION HetNet radios provide significant spectrum agility by allowing operation in Band 3, Band 3+, Band 4, ISM 2.4GHz and/or 5.8GHz and/or LTE bands. The radio offers unmatched flexibility with more than 30 waveforms supporting 15 RF channel profiles from 0.75MHz up to 38MHz allowing the Army to leverage a wide range of available spectrum allocations. ORION networks maximize spectral efficiencies in all circumstances by using:

- 2x2 MIMO space-time multiplexing that doubles spectral efficiencies
- Adaptive modulation and coding
- Automatic power control to lower spectral power density and improve LPD
- A choice a medium access control layers to improve spectrum sharing as link density per square mile increases, allowing more nodes to share the same RF channel
- Beam-switching antennas to further improve frequency reuse
- An embedded wide band cooperative spectrum scan to confirm spectrum availability in the field.

Ultra TCS has pioneered cognitive radio design, creating the first full-production spectrum-aware and adaptive military radio in 1992 (the AN/GRC-512, widely used in South Korea). The company is now adapting artificial intelligence and machine learning techniques and integrating them with its innovative HetNet technology to deliver high-value capabilities, including self-configuring, self-organizing, self-optimizing and self-healing communications systems that autonomously adapt and optimize network connectivity and resilience in harsh and contested tactical environments with minimal network planning and user expertise.

The ORION HetNet radio has been selected by PM Tactical Network (TN) for the TRILOS program of record under the nomenclature AN/GRC-262(V)1.

BIO: Denis Couillard has received his B. Eng. in electrical engineering and his Master in Technology Management from École Polytechnique de Montreal, Canada. He has more than 30 years experience in the telecom industry where he helped launch several new radio communication technologies and products, working on products innovation for several years. Couillard authored a book on strategic technology management and holds two U.S. patents on electronic attack and protection. He is currently director of government strategy at Ultra Electronics TCS in Montreal. Ultra has designed and deployed thousands of early cognitive radios in South Korea and is known in North America as the designer of the GRC-245 HCLOS and GRC-262 TRILOS radios, the terrestrial backbone of U.S. and Canadian Forces in the field.

Leveraging COTS Wireless for Secure Spectrum Agile Multipath Communications Today

David Howgill, President, Huckworthy • dhowgill@huckworthy.com

ABSTRACT

The commercial market has software-defined and spectrum agile radios available today that can use commercial spectrum to achieve the security, spectrum agility and automated interference resolution the Army needs. The radios are further valued as they can be programmed and controlled both in the field and through the network using APIs that bring the system into DOD control with full security and interoperability ensured.

These technologies can be married to commercially available wideband bodypatch antennas to allow lower profile antennas on the new systems and the ability to take advantage of spectrum agility without the antenna nightmares of constant changes or CONOP compromises.

All these technologies are deployable simply and immediately in the field, demonstrable today and available through better systems integrators. The problem is not technology. It is the willingness to try what is already available in paid proof-of-concept demonstrations, which is the best way to integrate COTS technology into the field.

COTS technology can immediately help in tough terrain, contested spectrum and even daily ease of use if it is given the chance to do so and, if you like it, it can be toughened up for the field!

BIO: David Howgill is founder and president of Huckworthy LLC, a Washington, DC-based integrator, consultancy and distributor of specialized advanced wireless telecommunications, specialist audio and video, energy and security solutions.

Howgill also serves as chairman of the Global VSAT Forum Wireless Backhaul Group and co-chairman of the British American Business Association's Small Business Group.

Huckworthy provides private, emergency responder and tactical LTE and hybrid wireless networks, encrypted communications, wireless intelligence solutions, hearing protection and HD audio solutions. Huckworthy is a certified HUBZone Small Business and a protégé of The Boeing Company under the Department of Defense's Mentor-Protégé Program.

WHAT IS AFCEA?

AFCEA is a member-based, non-profit 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 31,070 individual members, 139 chapters and 1,625 corporate members. For more information, visit www.afcea.org

